جامعة مولود معمري – تيزي وزو

كلية الحقوق والعلوم السياسية

قسم الحقوق

الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)

أطروحة لنيل شهادة دكتوراه علوم

تخصص: قانون

إعداد الطالبة

بن طالب ليندا

إشراف الأستاذ:

أ. د. تاجر محمد

لجنة المناقشة

. **يسعد حورية، أستاذة، جامعة مولود معمري، تيزي وزو .....رئيسة.**

. **تاجر محمد، أستاذ، جامعة مولود معمري، تيزي وزو..... مشرفا ومقررًا.**

. **عمارة عبد الحميد، أستاذ محاضر "أ"، جامعة الجزائر.....ممتحنا.**

. **خليفي عبد الرحمان، أستاذ، جامعة بجاية .....ممتحنا.**

. **كسال سامية، أستاذة محاضرة "أ"، جامعة مولود معمري، تيزي وزو .....ممتحنة.**

. **كتاب ناصر، أستاذ محاضر "أ"، جامعة الجزائر.....ممتحنا.**

تاريخ المناقشة 2019/01/23

إهداء

إلى روح والدي الطاهر طيب الله ثراه

إلى أغلى إنسان أمي الحبيبة حفظها الله وأطال في عمرها

إلى زوجي العزيز وقرت عيني أولادي أسأل الله أن يجعلهم من حفظة كتابه الكريم

إلى كل من أحبني وأحببته من عائلتي وأصدقائي

اليهم جميعا أهدي ثمرة جهدي ونتاج بحثي المتواضع.

كلمة شكر وتقدير

الحمد لله رب العالمين الخالق العزيز الكريم الذي بفضله تم إنجاز هذا البحث، والصلاة والسلام على أشرف الأنبياء والمرسلين سيدنا محمد وعلى اله وصحبه ومن تبعهم بإحسان إلى يوم الدين، وبعد...

أقدم شكري الجزيل بأجمل عبارات التقدير لأستاذي الفضيل الأستاذ الدكتور تاجر محمد، الذي لم يبخل علي بتوجيهه الرشيد، وتقويمه السديد إلى أن خرج هذا البحث إلى النور بصورته الحالية، جزاه الله عني وعن كافة طلاب العلم خيرا ان شاء الله.

كما أتقدم بكامل الشكر والتقدير للأساتذة الكرام الأعضاء في لجنة المناقشة، حيث أتقدم لهم بكامل الشكر على قبول مناقشة هذه الأطروحة لسد خللها والابانة على مواطن القصور فيها، فلهم مني فائق الاحترام والتقدير.

كما أشكر كل من ساعدني وأعانني وسهل عليا إنجاز هذا البحث.

قائمة المختصرات

أولا: *باللغة الفرنسية*

- **Anssi** : Agence nationale de la sécurité des systèmes d'information.
- **CA** : Cour d'Appel.
- **Cass** : cour de cassation
- **CE** : conseil d'Europe.
- **CEEAC** *:* Communauté économique des Etats de l'Afrique Centrale.
- CNEJITA : Compagnie Nationale des experts de justice en Informatique et Techniques Associées
- **Hadopi** : Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet.
- **IP** : Internet Protocol.
- **ISPEC** *:* Institut de Sciences *Pénales* et de Criminologie.
- **LRC** : Lois et règlements cités.
- **ONDRP** : Observatoire National de la Délinquance et des Réponses Pénales.
- **OPSI** : Orientation de Programmation pour la performance de la Sécurité Intérieure.
- **PUAM :** Presses Universitaires d'Aix-Marseille
- **PUF** : Presses universitaires de France.
- **RDPC** : Revue droit pénal et de criminologie.
- **RIDC** : Revue internationale de droit comparé.
- **RIDP** : Revue Internationale de Droit Pénal.
- **ROP** : Réseau de recherche sur les Opération de Paix.
- **RSC** : Revue de science criminelle et de droit pénal comparé.
- **STAD** : systèmes de traitement automatisé de données.
- **TCP** : Transmission Control Protocol.
- **TIC** : Technologies de l'Information et de la Communication.

ثانيا: باللغة الإنجليزية

- **ARK Code** : Arkansas Code.
- **BYOD** : Bring Your Own Device .
- **CCCA** : Comprehensive Crime Control Act.
- **CFAA** :Computer Frond and Abuse Act.
- **CMA** : Computer Misuse Act .
- **CRS** : Congressional Research Service.
- **ECPA** : The Electronic Communications Privacy Act .
- **FBI** : Federal Bureau of Investigation.
- **GPEA** : Governement Paperwork Elimination Act .
- **ICITAP** *:* International Criminal Investigative Training Assistance Program .
- **ICPO** : International Criminal Police Commission .
- **INTERPOL** : International Criminal Police Organization .
- **IOCE** : Internation Organization on Digital Evidence.
- **LAN** : Local area network .
- **MISC** :Multi-System & Internet Security Cookbook
- **PDA** : Personal Digital Assistant.
- **PEM** : Privacdy enhanced mail .
- **RCS** : Remote Control System .
- **SEC** : SECTION.
- **SWGDE** : Scientific Working Group on Digital Evidence.
- **UNODC :** United Nations Office on Drugs and Crime.
- **US** : United States .
- **WAN** : Wide Area-Net werh.

مقدمة:

منذ وقت قريب كان كم المعلومات المتولدة عن التفاعلات البشرية محدودا إلى حد كبير ولم يشكل حجمها أي مشكلة أمام عمليات تجميعها وتخزينها وإعادة استرجاعها، إلا أنه مع تقدم العلوم بدأ كم المعلومات يتزايد ويتكاثر، وصارت الطرق التقليدية لتجميع وتنظيم هذه المعلومات عاجزة عن تلبية احتياجات المستفيدين منها بكفاءة وفعالية، فأصبح من الضروري اللجوء إلى استخدام أساليب علمية وتقنية متطورة لمواجهة هذه الظاهرة، مثل الحاسبات الإلكترونية، والمستحدثات التقنية الأخرى كأقراص الفيديو الرقمية وأقراص الليزر ووسائط الاتصال.

إن عصر ثورة المعلومات التي يشهدها عالمنا اليوم يعتمد إعتماداً أساسياً على الحاسب بما له من قدرات هائلة للتخزين والاسترجاع وطرح الحلول لأعقد المشكلات. فالحاسب، جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال بيانات، أو إخراج معلومات، أو إجراء عمليات حسابية أو منطقية، وهو يقوم بالكتابة على أجهزة الإخراج، أو التخزين. يتكون الحاسب الالي من مجموعة من المكونات المادية، والمكونات المنطقية (البرامج) وهي الأوامر المرتبطة منطقياً والموجهة إلى الحاسب بعد ترجمتها إلى اللغة الوحيدة التي يفهمها وهي لغة الأرقام الثنائية

لم يكن من المتصور أن الحياة سوف تعتمد بصفة أساسية ومطلقة على جهاز الحاسب الآلي وملحقاته، إلا أن ذلك أصبح واقعا وحقيقة، فمؤسسات الدولة والشركات العامة والخاصة تعتمد على الحاسب الآلي، بل أن الأفراد في معاملاتهم اليومية باتوا حريصين على التعامل به واعتماده بصورة تكاد تكون أساسية، يمكن معها القول أن جهاز الحاسب الآلي أصبح يقاسم الإنسان حياته، خاصة بعد أن تم الربط بين أجهزة الإعلام الآلي ووسائل الاتصال، فتعززت منظومة الحاسب الآلي بالكمال بظهور شبكة المعلومات الدولية – الأنترنت – التي ساعدت على عولمة المعلومات وجعلها في متناول الجميع، حيث أصبح العالم بذلك مزدحما بكم هائل من المعلومات، حيث فتحت شبكة الأنترنت أفاقا رحبة أمام الأفراد، وسمحت لهم على إختلاف ثقافاتهم ولغاتهم بالدخول اليها، وتبادل المعلومات بحرية دون ادنى إعتبار للحدود الجغرافية بين الدول.

إن التطور الذي نحن بصدده وهو ثورة المعلومات والاتصالا ت كان على جانبين، الأول لخير البشرية والثاني لشر البشرية، فعلى صعيد الجانب الاول نرى أن هذه الثورة ساعدت على عولمة المعلومات وسهلت الكثير من الخدمات والاعمال، فقد توصلت البشرية من خلال هذا التطور الى السيطرة على المعلومات وإستخدامها في عمليات التصميم والتصنيع والتعليم والادارة، ناهيك عن تطوير تطبيقاتها لتشمل أداء خدمات عديدة، بذلك بزغت شمس ثورة المعلوماتية، أو الثورة الصناعية الثالثة التي دفعت وستدفع المجتمع لعصر جديد هو عصر مجتمع المعلومات. أما على صعيد الجانب الثاني فإن الإنسان يبقى حبيس نزواته وشهواته ونواقصه، لأنه يسيء إستخدام معالم هذه الثورة، بالتالي نجد جملة من الانعكاسات السلبية الخطيرة صاحبت التطور الهائل للتكنولوجية المتنامية جراء سوء استخدامها، حيث سهّلت ارتكاب بعض الجرائم التقليدية، ناهيك عن ظهور جرائم جديدة مرتبطة أساسا بالفضاء الافتراضي[1]– الأنترنت – لم تكن معهودة من قبل، كالجرائم المعلوماتية، التي يتخطى مداها حدود الدول والقارات، فإن كانت المصارف مثلا تستخدم الحاسب الإلكتروني في أعمالها، فإنه من خلاله أيضا ترتكب الكثير من الجرائم كالسحب الإلكتروني من الرصيد بواسطة الكارت الممغنط المزور، كذلك يمكن تصور جرائم التجسس عن بعد وسرقة المعلومات، ومن الممكن أيضا أن يترتب على الإصابة بالفيروس المعلوماتي تدمير برامج في غاية الأهمية[2].

[1] – الفضاء الإلكتروني هو مصطلح صاغه وليام جيبسون لوصف مكان خالٍ من الأبعاد الفيزيائية، ليتم تنظيم البيانات العالمية في شكل دعم بصري. راجع :

Arnaud NIKIEMA KOULIKA, La preuve dans le contentieux du cyberespace, mémoire de recherche droit du cyberespace africain, université Berger de saint Louis, Sénégal, 2010/2011, p 18 .

[2] – سجلت أول حالة اعتداء أمني على شبكة الأنترنت بعد مضي 20 سنة على إنشاءها، وهو اعتداء **دودة موريس** التي تعد من أولى ديدان المعلومات التي انتشرت عبر الأنترنت، أطلقت في 2 نوفمبر 1988، وسميت على اسم صانعها روبرت تابان موريس، كانت مهمة دودة موريس هى معرفة عدد الأجهزة المتصلة بالأنترنت ونسخ نفسها على الحاسبات الآلية. مما تسبب إلى إجمالى الخسائر لما يقرب من 100 مليون دولار. حكمت المحكمة على موريس بالمراقبة لمدة ثلاث سنوات و400 ساعة لخدمة المجتمع و10000 دولار غرامة، وكان موريس أول شخص يحاكم بموجب قانون الاحتيال الإلكتروني الأمريكي. محمد فؤاد الصاوي، جرائم الأنترنت،ص 10، محمول من الموقع الإلكتروني التالي: http://www.startimes.com/?=33677893، تم الاطلاع عليه يوم: 2012/10/22

بات هذا التطور يثير تحديات قانونية وعملية أمام الأجهزة المعنية بمكافحة هذه الجريمة، وآلية مباشرة إجراءات التحقيق –التي تتم عبر البيئة الافتراضية– لتعقّب المجرمين وتقديمهم للعدالة؛ كما أن ملاحقة الجناة وكشف جرائمهم قد يقتضي من الناحية العملية أن يتم في نطاق إقليم دول أخرى، وهو ما يصطدم بمبدأ السيادة الإقليمية للدول عملاً بمبدأ إقليمية القانون الجنائي.

تعد الجوانب الإجرائية مسألة أكثر حساسية في إطار البحث عن كافة الجرائم ذات العلاقة بالأنترنت بصفة خاصة، ذلك أن القاعدة الموضوعية وحدها لن تكون كافية في التفاعل مع الوقائع ما لم يكن هناك تتبع إجرائي من السلطات، فان كشف ستر هذا النوع من الجرائم يحتاج إلى طرق رقمية إلكترونية تتناسب مع طبيعتها، بحيث يمكن فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة، تصلح لأن تكون أدلة إثبات، التي يطلق عليها مصطلح الأدلة الإلكترونية[1]. بذلك ان التتبع الإجرائي يلزم أن يكون دستوريا بمعنى أن يكون ذات طبيعة مشروعة ليحافظ على مشروعية الأدلة المتولدة منه، والالتزام بمسألة الحقوق والحريات التي تحفظها الدولة لمواطنيها.

---

[1]– استعمل لفظ الدليل الإلكتروني من طرف المشرع الأوربي والأمريكي، راجع كل من:

–Conseil de l'Europe ,recommandation n° R (95) 13 du comité des ministres aux états membre relative aux problèmes de procédure pénale liés à la technologie de l'information, adoptée le 11 septembre 1995 ,in ;
https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1900873. Consulté le :06/11/2011.

اتفاقية بودابست المنعقدة في 23 نوفمبر 2001 وهي اتفاقية تمت تحت إشراف المجلس الأوربي، ووقعت عليها 30 دولة بما في ذلك دول أربعة من غير أعضاء المجلس الأوربي المشاركة في إعداد هذه الاتفاقية وهي كندا، اليابان، جنوب إفريقيا، والولايات المتحدة الأمريكية، حيث صادقت عليها هذه الأخيرة في 22 ديسمبر 2006، ودخلت بالفعل حيز النفاذ في 01 جانفي 2007، وهي مفتوحة لانضمام دول أخرى حتى يتمكن أن تساهم في ضبط وتنظيم مجتمع المعلومات والاتصالات بشكل أفضل.

- Convention sur la cybercriminalité, Conseil de l'Europe, signée à Budapest le 23 novembre 2001,in ; http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf consulté le: 21/12/2016.

-JARRETT H. Marshall , BAILIE Michael W, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, third edition, 2002 ,Published by Office of Legal Education Executive Office for United States Attorneys, p01.

إن الدليل الإلكتروني مثل أي واقعة تحدث من خلال النظام المعلوماتي، غالبا يأخذ طابع القرص المرن أو الفلاشة، فهو إذن عبارة عن برنامج **او** برمجية للحاسوب . لذلك فان التحفظ على قطع صلبة لحاسوب مسروق لا يعني على الإطلاق إننا بصدد دليل إلكتروني، وإنما نكون في مواجهة دليل مادي عادي ناجم عن جريمة سرقة .كذلك الحال يسري حين التحفظ على مسروقات من بينها أقراص مرنة او ليزرية مثل، فهذه الاخيرة لا تعد من قبيل الأدلة الإلكترونية وإنما أدلة مادية بالطبيعة. والحال غير ذلك إذا كان التحفظ قد تم على إسطوانة تحتوي على ملفات تتضمن أرقام كروت إئتمان مصرفية أو أرقام دخول سرية لمواقع أو صفحات او بريد الالكتروني أو كود دخول الى برمجيات في التداول سواء ماديا أوعبر الانترنت، فكل من هذه وتلك أدلة إلكترونية. والطبيعة التي عليه الدليل الإلكتروني تجعل من البيئة التي يحيا فيها أمرا لازما، فإذا لم تتوافر هذه البيئة فإن الدليل الإلكتروني لا يصلح لكي يعول عليه، إذ من غير المقبول بناء الحكم على التقرير بوجود قرص محرز في الأوراق يحوي ملفات ذات موضوع إجرامي، بل يجب أن يرد في ذات الحكم أنه قد تم فتح القرص والإطلاع على فحوى الملفات المحرزة ثم بعد ذلك التقرير بأن هذا الدليل ليس من قبل مخرجات حركة البرامج في الحاسوب أو الأنترنت وإنما دليلا مخزنا وضعه فرد ما.

إنّ موضوع الدليل الإلكتروني ودوره في الإثبات الجنائي، من الموضوعات الجديدة في إطار القسم الإجرائي من القانون الجزائي، له أهمية بالغة، فكان الدافع لاختياره راجع لإرتباطه الوثيق والمباشر بظاهرة الجريمة المعلوماتية، التي لا تزال جديدة ولم تنل حظها الكافي من البحث والتمحيص على مستوى الفقه الجنائي، إذ إقتصرت أغلب الدراسات المنشورة في مجال الجريمة المعلوماتية على البحث في الجوانب الموضوعية دون محاولة الغوص في مسألة إثباتها ومدى تأثير خصائصها على إجراءات التحقيق المتبعة في ذلك.

كما أثارت الجريمة المعلوماتية العديد من المشكلات في نطاق قانون الإجراءات الجزائية، الذي وضعت نصوصه لتنظم الإجراءات المتعلقة بالجرائم التقليدية، التي لا تتضمن صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي

الجزائي في الاقتناع وصولا إلى الحقيقة الموضوعية بشأن الجريمة والمجرم، أما بالنسبة للجرائم المعلوماتية فيتسم التحقيق فيها بالعديد من المعوقات والصعوبات، لذلك كان لابد من خلق قواعد إجرائية تنظم مسألة استخلاص الدليل الإلكتروني لإثباتها، والا كانت نتائج التحقيق سلبية، تنعكس على نفسية المحقق بفقدانه الثقة في أجهزة التحقيق، وعلى المجرم نفسه، حيث يشعر أن الجهات الأمنية غير قادرة على اكتشاف أمره وأن خبرة القائمين على مكافحة الجريمة والتحقيق فيها لا تجاري خبرته، الأمر الذي يعطيه ثقة أكبر في ارتكاب المزيد من هذه الجرائم، فضلا عن ذلك فإن المجرم المعلوماتي غالبا ما يضرب سياجا أمنيا على أفعاله غير المشروعة قبل ارتكابه لها، فيزيد بذلك من صعوبة تطبيق القواعد الإجرائية التي يتوقع تتبعها للبحث عن الأدلة الإلكترونية التي تدينه، وذلك بالعمل على ترميز أو تشفير المعلومات المخزنة إلكترونيا والمنقولة عبر شبكات الاتصال، بحيث يستحيل على غيره الاطلاع عليها، ويصبح بذلك الدليل الإلكتروني مشفرا.

تتعلق المشكلات الإجرائية في مجال البحث عن الدليل الإلكتروني بسرعة ودقة تنفيذ الجرائم المعلوماتية وإمكانية محو آثارها عقب التنفيذ مباشرة، كما قد تكون البيانات المراد تفتيشها وضبطها مخزنة في أنظمة وشبكات إلكترونية موجودة بالخارج، فتثير مسألة الدخول إليها– لمحاولة جمعها وتحويلها إلى الدولة التي يجرى فيها التحقيق– مشكلات تتعلق بسيادة الدولة أو الدول الأخرى التي توجد لديها هذه البيانات، وفي هذه الحالة يحتاج الأمر إلى تعاون دولي في مجالات البحث والتفتيش والتحقيق وجمع الأدلة، وتسليم المجرمين، بل وتنفيذ الأحكام الأجنبية الصادرة في هذا المجال.

ينبع الهدف الأساسي من هذه الدراسة في المساهمة في وضع الخطوط العريضة للتعرف على الدليل الإلكتروني وطرق التحقيق التي يستخلص بها، ذلك أن جدية وحداثة الجرائم المعلوماتية–وما تتسم به من خصائص–تجعل المحقق في حيرة أمام كيفية التعامل معها وأسلوب التحقيق فيها، إذ لاشك أن إجراءات التحقيق وجمع الأدلة بخصوص هذه الجرائم يختلف عما هو الحال عليه في الجرائم التقليدية، وحاليا أصبح القاضي الجزائي يستند على

الدليل الإلكتروني باعتباره تطبيقا من تطبيقات الدليل العلمي، فوجب إظهار دوره في قبوله وتقديره للدليل الإلكتروني، والأسس التي يرتكز عليها من اجل الوصول إلى الحقيقة.

بناء على ما تقدم، إن محور الإشكالية التي يثيرها هذا البحث، تتعلق ب :

كيفية ضمان مصداقية الدليل الإلكتروني كي يعبر عن الحقيقة التي تهدف إليها الدعوى الجزائية.

للاجابة على هذه الاشكالية اعتمدت ذهه الدراسة ثلاثة مناهج علمية تساير التسلسل المنطقي التدريجي للأفكار حرصا على تحقيق الغاية من البحث، من خلال المنهج التفسيري تم شرح موضوعات البحث المختلفة، بحمل بعضها على بعضٍ، تخصيصاً وتعميماً، حتى تتّضح مشكلاتها، وتتكشف مبهماتُها، لتبدوَ بصورةٍ واضحة متكاملة، بالمنهج الإستقرائي تم رد النقاط التفصيلية إلى أصولها وهي النظرية العامة للإثبات. أما المنهج المقارن فلا يستهدف منه في هذه الدراسة الجرد لأوجه التشابه والاختلاف، وإنما لإثراء الفهم وادراك المعنى الذي يجب استخلاصه، وذلك من اجل الوقوف عند التوجهات التي يجب أخذها بعين الاعتبار للتيقن من منطق الدليل الإلكتروني والمنظور القانوني والعلمي له، وذلك بدراسة أهم القوانين المقارنة، والتطرق للأنظمة القانونية المتأثرة بها.

على هذا الأساس قسمت الدراسة إلى بابين:

محور الباب الأول هو الإطار العام للدليل الإلكتروني، قسم الى فصلين:

الفصل الأول يعرض فيه ذاتية الدليل الإلكتروني، بالوقوف أمام محله وهي الجريمة المعلوماتية بصفة خاصة.

الفصل الثاني يعرض فيه إجراءات جمع الدليل الألكتروني التقليدية والحديثة.

محور الباب الثاني هو حجية الدليل الإلكتروني في الإثبات الجنائي، قسم الى فصلين:

الفصل الأول أظهرنا فيه المبادئ التي يجب على القاضي الجزائي إحترامها لقبول الدليل الإلكتروني.

الفصل الثاني أظهرنا فيه أهمية دور القاضي الجزائي في الإقتناع بالدليل الإلكتروني، كما أبرزنا فيه فعالية التعاون الدولي في هذا المجال.

الباب الأول

الإطار العام للدليل الإلكتروني

كان للدور البارز الذي حققته تكنولوجيا المعلومات والإتصال في تسهيل الحياة اليومية للفرد أثار سلبية تتمثل في استخدام نظم المعالجة الآلية على نحو غير مشروع، أدى إلى ظهور مجموعة جديدة من الجرائم، ونوعية جديدة من الجنّاة الذين يرتكبون هذه الجرائم، كما أثرت تأثيرا كبيرا على الإثبات الجزائي بظهور نوع خاص من الأدلة وهي الأدلة الإلكترونية، التي جعلت طرق التحقيق التقليدية المتبعة لاستخلاصها تقريبا عقيمة نتائجها سلبية.

ان الطبيعة الخاصة للدليل الإلكتروني التي اكتسبها من محله – الجريمة المعلوماتية– أثرت على الإجراءات التقليدية لجمع الأدلة، فاستحدثت إجراءات أخرى قادرة على استنتاج هذا النوع من الأدلة، حيث أضحى الأمر في غاية الضرورة والأهمية لمواجهة هذا الأجرام المستحدث.

انطلاقا من ذلك سيتم دراسة الإطار العام لمفهوم الدليل الإلكتروني(الفصل الأول)، إجراءات جمع الدليل الإلكتروني(الفصل الثاني).

الفصل الأول

مفهوم الدليل الإلكتروني

يقصد بالاطار العام لمفهوم الدليل الإلكتروني، دراسة ذاتية هذا الدليل في مجمله، بالتطرق إلى تعريفه طبيعته خصائصه وأقسامه، مع دراسة المحل الذي يولد وينبعث منه، حيث أن الأدلة بطبيعتها تتشكل من طبيعة الجريمة التي ارتكبت، وفي نطاق الدليل الإلكتروني، فإن الجريمة التي يولد وينبعث منها هذا الدليل هي "الجريمة المعلوماتية".

إن أوّل ما ينبغي دراسته في مستهل هذا الفصل هو تحديد محل الدليل الإلكتروني بمعنى الجريمة المعلوماتية (المبحث الأوّل)، ثم دراسة موضوع الدليل الإلكتروني (المبحث الثاني).

المبحث الأوّل

محل الدليل الإلكتروني

يقصد بمحل الدليل الإلكتروني، تلك الجريمة التي يولد منها وهي الجريمة المعلوماتية المدعى حدوثها من قبل سلطة الإتهام.

إذ لا يستقيم الخوض في دراسة الدليل الإلكتروني إلاّ بعد دراسة هذه الجريمة، وذلك من خلال التطرق لموضوعها (المطلب الأول)، والوقوف عند أساليب ارتكابها، وطرق اكتشافها (المطلب الثاني).

المطلب الأوّل

الجريمة المعلوماتية

إن ظاهرة الإجرام المعلوماتي الناشئ في بيئة الفضاء الإلكتروني، كأي ظاهرة جديدة احتاجت في البداية إلى تعريفها وتحديد مفهومها ولن نخوض في مختلف التسميات للدلالة على هذه الظاهرة الإجرامية، ولا إلى تطوّرها التاريخي، فالمتفق عليه دوليا ووطنيا أنها تشكل أنشطة

منظمة، ذات خطورة على أمن واستقرار الدول المتقدمة والنامية، على ذلك يدرج فيما يلي تعريف الجريمة المعلوماتية (الفرع الأول)، وصورها (الفرع الثاني).

الفرع الأوّل

تعريف الجريمة المعلوماتية

ان اهم التعريفات التي حاولت الإحاطة قدر الإمكان بجميع الأشكال الإجرامية للجريمة المعلوماتية[1] سواء تقع بواسطة النظام المعلوماتي–المزدوج بين تقنيات الحوسبة والاتصال بما في ذلك شبكة الأنترنت – أو داخل هذا النظام أي على المعطيات والبرامج، هو التعريف المقدم من طرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين، بأن الجريمة المعلوماتية هي :"أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، وتشمل هذه الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الإلكترونية"، حيث أن هذا التعريف جدير بالتأييد[(2)] كونه يعبر عن الطابع التقني لهذه الجرائم، ويوفر فرصة إمكانية التعامل مع المستجدات العلمية التقنية فشمل جميع الجرائم التي من الممكن ان تقع في البيئة الإلكترونية، كما لم يركز على فاعل الجريمة ومقدرته الفنية، ولا على وسيلة ارتكابه للجريمة، بل حاول عدم حصر هذه الجريمة في نطاق ضيق يفتح باب لإفلات العديد من النشاطات قد تدخل في دائرة التجريم[3].

سعت الدول للتصدي لهذا النوع من الإجرام، بوضع قوانين موضوعية للوقاية منه ومحاربته ومن ثم القضاء عليه، ومن اهم التطبيقات التشريعية يوجد تشريع الولايات المتحدة الأمريكية، التشريع البريطاني، التشريع الألماني، التشريع الفرنسي والتشريع الجزائري.

---

[1]– ان تباين التعاريف راجع لتباين ميل الباحث ووجهته فقد يكون تقنيًا وقد يكون قانونيًا، أن التعريفات تتباين أيضًا تبعًا لموضوع الدراسة القانونية ذاته، فقد تكون متعلقة بالقانون الجنائي، وقد تكون متعلقة بحقوق الملكية الفكرية، يفضل استخدام مصطلح جرائم المعلوماتية لأسباب متعددة منها كون المصطلح القانوني ذو دلالة واسعة مراعيا كل مستجدات الاختراعات الإلكترونية ووسائل الاتصال أي كل ما يخدم المعلومة.

[2]– نجد نفس التأييد عند : **أسامة أحمد المنعاسة، جلال محمد الزغبي، فاضل الهواوشة**، جرائم الحاسب الآلي والأنترنت، دار وائل للنشر، عمان، 2001، ص 78.

[3] - عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دراسة مقارنة، رسالة ماجستير، كلية الحقوق الإسكندرية، 2009، ص 18.

أولا : التشريع الأمريكي

شرعت الولايات المتحدة الأمريكية قانونا يشمل حماية أنظمة الحاسب الآلي وهو القانون الشامل لمكافحة الجريمة لعام 1984(CCCA) [1]، وفي عام 1986 أصدرت قانون مكافحة الاحتيال وإساءة استخدام الكمبيوتر (CFAA) [2]،عرّف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى اثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم[3] بما يتناسب مع هذا القانون.

أما القانون الجزائي الفدرالي للولايات المتحدة الأمريكية[4] ينظم الجريمة المعلوماتية بجمع أحكام القانونين، القانون الشامل لمكافحة الجريمة لعام 1984(CCCA)، وقانون مكافحة الاحتيال وإساءة استعمال الكمبيوتر لعام 1986(CFAA)، بذلك أجمل "الجرائم المعلوماتية" في ثلاث فئات[5]:

---

[1] – **Public law** 98-473—OCT. 12, 1984 Chapiter XXI—Access devices and computers , in ; https://www.gpo.gov/fdsys/pkg/STATUTE-98/pdf/STATUTE-98-Pg1837.pdf.

[2]-**Computer Fraud and Abuse Act** ,section 1 short title of 1986, in ; https://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1213.pdf.

تم تعديله عدة مرات في 2008،1996،1994،1989، في جانفي 2015، اقترح الرئيس باراك اوباما توسيع قانون (CFAA) بتحديث سلطات انفاذ القانون لمكافحة الجريمة المعلوماتية، الا انه لاقى المعارضة من الكونجرس على اساس ان هذا التعديل سوف يجعل العديد من انشطة الأنترنت العادية غير قانونية .

[3]– تعاقب المواد Subsection 1030 (b)(c) من قانون CFAA السالف الذكر على:

الحصول على معلومات تتعلق بالأمن الوطني، الوصول إلى الحاسوب والحصول على المعلومات دون إذن،

الوصول غير القانوني إلى جهاز كمبيوتر حكومي،الوصول إلى الحاسوب لغرض ارتكاب الغش والحصول على المعلومات، إلحاق الضرر عمدا بجهاز كمبيوتر عن طريق نقل البيانات، الضرر بسبب الإهمال أو التهور بعد الوصول عن عمد إلى جهاز كمبيوتر، وإهمال تسبب الأضرار والخسائر بعد الوصول عمدا إلى جهاز كمبيوتر، العبث مع كلمات السر، والابتزاز من خلال جهاز كمبيوتر، وكل من يحاول او يتامر على ارتكاب الجرائم السالفة الذكر.

[4]–**United States Code**, Title 18 , Crimes and criminal procedure, in ; https://www.unodc.org/res/cld/document/usa/1948/u_s__code_-_title_18_html/US_Code_Title_18.pdf .

[5] –• accessing a computer to commit espionage, 18 U.S.C. 1030(a)(1).

– computer trespassing (e.g., hacking) in a government computer, 18 U.S.C. 1030(a)(3)

• computer trespassing (e.g., hacking) resulting in exposure to certain governmental, credit, financial, or computer-housed information, 18 U.S.C. 1030(a)(2)

damaging a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce (e.g., a worm, computer virus, Trojan horse, time bomb, a denial of service attack, and other forms of cyber attack, cyber crime, or cyber terrorism), 18 U.S.C. 1030(a)(5);

– الجرائم التي تستهدف شبكة الأجهزة والحواسيب "hacking" أو القرصنة[1]، والبرمجيات الخبيثة أو التخريب، الحرمان من الخدمة Denial of Service (DoS)، والتي تتطابق مع الهجمات المتزامنة متعددة أجهزة الكمبيوتر.

–الجرائم التي تشكل الأجهزة أو شبكة الكمبيوتر أداة لارتكابها، هذه الفئة تجمع الجرائم ضد الأشخاص: الاستمالة « grooming »[2] أو انتهاك الخصوصية[3]، الإيذاء النفسي، والتحرش والتهديد والتحريض على الانتحار والجرائم ضد الممتلكات: الابتزاز على الأنترنت [4].

– جرائم المحتوى المعلوماتي، تضم هذه الفئة النشر الطوعي للمحتوى غير القانوني المواد الإباحية المتعلقة بالأطفال[5] والتوزيع الطوعي للمحتوى غير المرغوب فيه أو الرسائل غير المرغوب فيها spam [6].

أما بالنسبة للدليل الإلكتروني، فالقوانين الأمريكية التي تحكم الأدلة الإلكترونية في التحقيقات الجزائية هي: التعديل الرابع للدستور الأمريكي، وقوانين الخصوصية القانونية مقننة في

.18 U.S.C. §§ 2510-22, 18 U.S.C. §§ 2701-12, and 18 U.S.C. §§ 3121-27

ثانيا : التشريع البريطاني

يعرف قانون إساءة استخدام الحاسوب لعام 1990(CMA) [7]، الجريمة المعلوماتية على أنها "الوصول غير المصرح به إلى الحاسوب أو ملفات البيانات الإلكترونية لغرض ارتكاب جرائم"

---

[1]– بعض تشريعات في الولايات الامريكية تميز "القرصنة من الخارج" من "القرصنة من الداخل، أنظر:

LegiGlobe, Cybercriminalité (br, cn, es, us, nl, uk), p 05, in ; http://legiglobe.rf2d.org/cybercriminalite-2/2013/09/05/. Consulté le :25/09/2016.

[2]– يعتبر الاستمالة الجنسية جريمة خاصة، تنطوي على تحريض شخص على ممارسة الجنس مع الآخرين، تستوجب استخدام شبكات الاتصالات تحديدا.

[3]– انتهاك الخصوصية الذي يقصد به هنا هو التقاط الصور أو الأفلام من الحياة خاصة للضحية دون علمه.

[4]- **Tiffany CURTISS**, Computer fraud and abuse act enforcemen : cruel, unusual and due for reform, p 6, in ; https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1643/91wlr1813.pdf?sequence=3&isAllowed=y. consulté le 23/10/216.

[5]– يعاقب عليها بموجب المادة 2256 من الباب الثامن عشر من القانون العقوبات الأمريكي (code5).

[6]– تتطابق هذه الفئة مع إرسال رسائل البريد الإلكتروني غير المرغوب فيها المحددة في القانون الامريكي the Canspam act of 2003.

The Canspam Act of 2003, Section.4 §1037,in ; https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf

[7] **Computer Misuse Act 1990** ,in ; http://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf.consulter le 20/12/2017.

مثل الاحتيال وسرقة الهوية، التزييف، جميع انتهاكات الملكية الفكرية، كما يجرم على وجه التحديد اقتحام نظام حاسوبي لارتكاب جرائم القرصنة، التسلل، الرسائل غير المرغوب فيها أو البرامج الضارة كالفيروسات.

يحتوي هذا القانون على 18 مادة جاءت موزعة على أربعة أبواب1 و2 و3 وA3، ترد فيها أربع جرائم معلوماتية، وهي:

-الوصول غير مصرح به إلى ملفات الكمبيوتر الخاصة من نظام آخر

-الوصول غير المصرح به بنية ارتكاب أو تسهيل ارتكاب أي نوع من الجرائم والذي يضم الجرائم المالية والاحتيال والسرقة والجرائم الجنسية وغير الأخلاقية والجرائم التي تهدد حرمة الحياة الشخصية والتزوير والمقامرة والإتجار بالمخدرات.

-أعمال غير مصرح بها بقصد الإيذاء أو التهور المتعمد في تشغيل الكمبيوتر.

-إنشاء أو توفير أو الحصول على معلومات لاستخدامها في ارتكاب الجرائم المشار إليها في المواد من 1 إلى 3 أعلاه.

ثالثا: التشريع الألماني

ان التشريع الألماني لا يحتوي على تعريف قانوني مباشر للجريمة المعلوماتية[1]، لكنه يحتوي على العديد من الأشكال التي قد تتخذها، خاصة بعد إضافة المادتين 303 (أ)، 303 (ب) إلى قانون العقوبات« Strafgesetzbuch, StGB » [2] في الجزء السابع والعشرون- حيث جرم كل تغيير للبيانات، تخريب الكومبيوتر، الحاق اضرار بنظام تشغيل البيانات -لمؤسسة أو مشروع

[1]- ولكن المكتب الاتحادي للشرطة القضائية(BKA) بناءا على دلائل قانونية وإحصائية يستخدم تعريفيين لهذه الظاهرة، تعريف ضيق يقتصر على عدد قليل من الجرائم المحددة وتعريف أوسع يمتد إلى جميع الجرائم التي تستعمل الأنترنت أهمها الاحتيالphishing، الهجمات على المواقع الإلكترونية، الابتزاز، التجارة غير المشروعة، تصنيع ونشر أدوات البرمجيات غير القانونية. وتنشر شركة Le BKA، ومقرها في فيسبادنWiesbaden ، تقريرا سنويا عن الجريمة المعلوماتية تأتي من خلاله هذه التعاريف انظر كل من :

https://Office_fédéral_de_police_criminelle. Consulté le 26/09/2016.

Peter HUNERFELD, "Le Droit Allemend La preuve en procédure pénale", V 63, 1er et 2ème trim, RIDP, 1992, p57.

[2] - **Strafgesetzbuch, StGB** 15/05/1871, in ; https://www.gesetze-im-internet.de/stgb/StGB.pdf.

تابع للغير أو لسلطة عامة – متى كان لهذا النظام أهمية جوهرية، كما حدد المشرع الألماني محل الجريمة التي تنصب عليها أفعال التخريب بأنه جهاز معالجة البيانات أو وحدة تخزين هذه البيانات، كما حدد صور هذا الإضرار بأنها تأخذ صور: التعطيل، عدم القابلية للاستعمال، المحو والتغيير.

كما جرم بموجب المادة 202 (أ)، فعل التجسس على المعلومات المخزنة، وردت هذه المادة في الباب الخاص بجرائم الاعتداء على الحياة الخاصة والسرية، الذي أدرجت فيه المواد المتعلقة بحماية سرية المحادثات، وسرية المراسلات، والأسرار الخاصة للأفراد.

أما المادة 270 من قانون العقوبات الألماني فهي تجرم كل من توصل بطريق الخداع إلى إحداث تأثير يؤدي إلى الإخلال بعمل نظام البيانات الإلكترونية.

أدرج الشارع الألماني حماية بالغة للمعلومات في قانون المعلومات وخدمات الاتصالات[1]، ويتضح من هذا أن المشرع الألماني أراد الإحاطة بكافة صور المساس بنظام معالجة البيانات، حيث جمعها كلها تحت اسم "التخريب"، كما أنه ساوى بين وقوع الجريمة على شخص خاص أو عام، ووجهته بذلك جديرة بالتأييد لأن علم التجريم هي كفالة نظم معالجة البيانات لأداء دورها أيا كانت الجهة المجني عليها.

رابعا: التشريع الفرنسي

شرعت فرنسا عدة قوانين في هذا المجال، وكان من أهمها :

– قانون حماية البيانات والحريات 1978 [2] الذي كرس حماية لأجهزة الكمبيوتر والملفات التي يتضمنها، يعتبر هذا القانون أول قانون ينظم الجوانب القانونية المتصلة بالمعلوماتية وأثرها على الخصوصية خاصة بعد ان أثيرت قضية القرصنة في المعلومات، حيث تنص المادة 14منه على حماية البيانات الخاصة سواء كانت ملك للدولة أو الأشخاص.

[1] – وهو القانون الذي ينظم الشروط الإطارية لخدمات المعلومات والاتصال اعتمد في 22 جويلية 1997 والذي دخل حيز النفاذ في أول جانفي 1998.

Informations- und KommunikationsdiensteGesetz, in ;
http://www.bibliotheksverband.de/fileadmin/user_upload/Kommissionen/Kom_Recht/Publikationen_Allgemeines/1997_09_Informations-und_KommunikationsdiensteGesetz.pdf .

[2] - Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460.

– قانون 1988 المتعلق بالاحتيال المعلوماتي[1]، الذي جرم معظم الهجمات ضد أنظمة الكمبيوتر، وبموجبه تم إنشاء فرع تجاوزات نظم معالجة البيانات الآلية (STAD).

– قانون رقم 90–1170 [2] أكد على ضمان سرية المعلومات وعدم الاستيلاء عليها بطريق اختراق التشفير، فعرفت المادة 28 منه التشفير بان" كل التسهيلات أو الخدمات التي تهدف إلى النقل أو التحويل وذلك عن طريق ترتيب سرية المعلومات أو الإشارات الواضحة إلى معلومات أو إشارات مفهومة لأطراف ثالثة من خلال أجهزة أو برامج تصوره لهذا الغرض وهو الدفاع الوطني والحفاظ على المصالح الداخلية والخارجية وامن الدولة".

بعده مرسوم رقم 92–1358[3] المتعلق بالبلاغات والالتماسات للحصول على إذن الترميز المتعلق بالوسائل والتسهيلات، تضمنت مواده تفاصيل تقديم وتصدير واستخدام خدمات أي نوع من أنواع المرافق المشفرة، وبموجبه لا تعتبر وسيلة من وسائل الترميز إذا كانت تتعلق بأجهزة أو برامجيات خاصة لحماية البرامج من النسخ غير المشروع استخدامها والتي تستفيد من وسائل أو أجهزة سرية شريطة أن لا يسمح التقييد بشكل مباشر أو غير مباشر من خلال البرنامج المعني.

– قانون العقوبات الفرنسي[4] عالج بدوره تنظيم المعالجة الآلية للبيانات في المادة 323 فقراتها الأربعة فالفقرة الأولى ذهبت لتجريم الوصول أو البقاء بطريقة مخادعة في كل جزء من نظام المعالجة الآلية للمعطيات، كما عاقبت على حذف أو تعطيل أو تعديل المعطيات الموجودة في النظام أو تحريض لمجريات النظام، الفقرة الثانية جرمت إعاقة النظام وتزوير المعطيات والمعالجة، أما الفقرة الثالثة جرمت فعل كل من يدخل بطريقة مخادعة إلى معطيات داخل نظام المعالجة الآلية أو من يحذف أو يعدل بطريقة مخادعة معطيات موجودة في النظام، والفقرة الرابعة فقد تضمنت موضوع الاشتراك والمساهمة في هذه الأفعال حيث يعاقب الشريك بذات عقوبة الفاعل الأصلي.

---

[1] -Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000875419 .

[2] - Loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000533747.

[3] −Décret n°92-1358 du 28 décembre 1992 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000543201&dateTexte=19980224

[4] - **Code pénal Français**, in ; https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 .

– قانون 2001[1] بشأن السلامة اليومية، تضمن موضوع حفظ بيانات الاتصالات، ومكافحة الغش على آلات الصرف وتعزيز جهاز القمع ضد أولئك الذين يستخدمون موارد تكنولوجيا المعلومات لتحقيق هذا الاحتيال.

– قانون 2003[2] للأمن الداخلي التزم بتعزيز فعالية الإجراءات الجزائية التي تنظم آليات الاستيلاء والتفتيش المعلوماتي.

– قانون 2004[3] المتضمن تكييف نظام العدالة للتطورات في الجريمة، ثم عززت الأجهزة في مكافحة المواد الإباحية المتعلقة بالأطفال، ونشر الأنترنت العنصري والتزوير على وجه الخصوص.

– قانون 2004[4] المتضمن الثقة في الاقتصاد الرقمي، اهتم بمكافحة الجرائم المعلوماتية في كثير من النواحي، رفع من العقوبات، كما نص على بمعاقبة الأفعال التحضيرية لارتكاب هذه الجرائم الواردة في المادة 323–3–1قانون العقوبات.

– القانون 2006 [5] بشأن مكافحة الإرهاب، وسع نطاق الأشخاص الخاضعين لالتزام الاحتفاظ بالبيانات الاتصالات كما مكن المحققون التفتيش دون إذن قضائي.

– قانون 2007 [6]بشأن قمع الجريمة، جاء لتعزيز فعالية عمل المحققين باستخدام الإجراءات السرية، التي تتيح لهم المشاركة تحت اسم مستعار في التبادلات الإلكترونية، والاتصال بالجناة المحتملين واكتساب محتوى غير قانوني، كما نص هذا القانون على جرائم جديدة تستهدف بوجه خاص حماية القاصرين من الاستغلال الجنسي الإلكتروني ومكافحة التحميل الإلكتروني غير القانوني للأفلام المتعلقة بذلك على شبكة الأنترنت.

– قانون 12 جوان2009 مواده تعزز نشر وحماية الخلق على شبكة الأنترنت.

---

[1]- Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052.

[2]-Loi n° 2003-329 du 18 mars 2003 pour la sécurité intérieure in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000412199.

[3] - Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000249995.

[4] - Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164.

[5]- Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000454124.

[6]- Loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000615568&dateTexte=20070307.

– قانون 28 أكتوبر 2009[1] بشأن الحماية الجزائية للملكية الأدبية والفنية على شبكة الأنترنت.

خامسا : التشريع الجزائري

تبنى المشرع الجزائري في القانون رقم 15/04[2] المعدل لقانون العقوبات – للدلالة على الجريمة المعلوماتية– مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة وافرد القسم السابع مكرر منه تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، والذي تضمن 08 مواد من المادة 394 مكرر وحتى المادة 394 مكرر 7، حيث جرم فيها الأفعال الماسة بأنظمة الحاسب الآلي .

أما في عام 2006 ادخل المشرع تعديل على قانون العقوبات بموجب قانون رقم 06–23[3] مس القسم السابع مكرر، حيث تم تشديد عقوبة الحبس والغرامة المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم.

لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت استراتيجية لمكافحة الجريمة المعلوماتية، حيث تم في مرحلة لاحقة اختيار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بموجب القانون رقم09–04[4]، تطرق فيه إلى تعريف الجريمة المعلوماتية ونظام المعلومات في المادة 2 منه، مسميا إياه": المنظومة المعلوماتية " بأنها أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع

---

[1] Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet, dite (HADOPI II), in ;
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021208046&categorieLien=id

[2]– قانون رقم 04–15 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، يعدل ويتمم الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية عدد 71بتاريخ 10 نوفمبر 2004.

[3]– قانون رقم 06– 23 مؤرخ في 2 9 ذي القعدة عام 1427الموافق 20 ديسمبر سنة 2006،يعدل ويتمم الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية عدد 84 بتاريخ 24 ديسمبر 2006.

[4]– قانون رقم 09– 04 مؤرّخ في 14 شعبان عام 1430 هـ الموافق 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ووكافحتها، الجريدة الرسمية للجمهورية الجزائرية عدد 47 بتاريخ 16 غشت 2009.

بعضها البعض أو مترابطة، يقوم واحد منها أو أكثر بالمعالجة الآلية للمعطيات تنفيذا لبرنامج معين .

وفقا للمشرع الجزائري في تعريفه لنظام المعالجة الآلية للمعطيات ومقارنة مع التشريعات الأخرى اشترط ضرورة الترابط بين مكونات أو أجهزة النظام وبين الأنظمة فيما بينها، وركز على وظيفة المعالجة الآلية للمعطيات موسعا بذلك مجالها، فلم يركز على وسائل ارتكابها بل حصرها فقط في صور الأفعال التي تشكل اعتداء على النظام المعلوماتي، أي الجرائم التي يكون النظام المعلوماتي محلا لها وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحولها إلى معلومات بعد معالجتها وتخزينها، حيث قام بحماية هذه المعطيات من أوجه عدة.

يؤخذ على المشرع الجزائري من ناحية المصطلحات أنه إستعمل مصطلح ضيق للتعبير عن الجرائم المعلوماتية وهو مصطلح المساس بأنظمة المعالجة الألية للمعطيات جرائم الحاسب الآلي حيث أنه يعبر عن جرائم التي يستعمل في إرتكابها الكمبيوتر دون الأنترنت، إلا ان مضمون النصوص التجريمية الواردة تشمل في نفس الوقت جرائم الأنترنت، لان أنشطة الأنترنت تتطلب أجهزة كمبيوتر ترتكب بواسطتها وهي تستهدف أيضا معلومات مخزنة أو معالجة ضمن أجهزة كمبيوتر وهي الخوادم التي تستضيفها مواقع الأنترنت أو تديرها، وإذا فصلت وسائل تقنية المعلومات، فان هذا لن يتحقق لأن الشبكات ذاتها عبارة عن برمجيات وبروتوكولات مدمجة في نظام الحوسبة بذاته، إلا إذا تم حصر فكرة الشبكات بالأسلاك، وهذا يخرج من نطاق الجرائم المعلوماتية إلى جرائم الاتصالات التي تستهدف ماديات الشبكة.

الراجح أن الغاية من التجريم هي حماية النظام المعلوماتي في حد ذاته ومنتجاته لان هذا الأخير يضمن برامج المعلومات المخزنة في الذاكرة.

الفرع الثاني

صور الجريمة المعلوماتية

ترتكب الجريمة المعلوماتية لدوافع تختلف تبعا لطبيعة المجرم ومدى خبرته في مجال الحاسب الآلي، وهي غالبا تدور ما بين تحقيق الكسب المادي- كالمساومة على البرامج أو المعلومات المتحصلة بطريقة الغش – أو المتعة والتحدي والرغبة في الانتقام، كما يعد التسابق العسكري والفضائي دافعا لهذه الجريمة.

تقع هذه الجريمة في بيئة المعالجة الآلية للبيانات يستلزم على مرتكبها التعامل مع البيانات مجمعة ومجهزة بغرض معالجتها إلكترونيا بما يمكنه من العبث بتعديلها ومحوها وتخزينها واسترجاعها وطباعتها.

تتميز هذه الجرائم بطبيعة خاصة كونها تتم في البيئة الإلكترونية، فهي إما تأخذ شكل اعتداء واقع على الأموال أو على الأشخاص.

أولا: الاعتداء الواقع على الأموال

تعد الأموال المادية في البيئة الإلكترونية الرقمية عبارة عن معلومات ذات قيمة اقتصادية عالية[1]متجسدة في نبضات إلكترونية- يمكن سرقتها عبر الأنترنت - أضفت عليها معظم التشريعات حماية خاصة بتجريم جميع صور العدوان الواقعة عليها.

يستهدف هذا الاعتداء بصفة أساسية المؤسسات المالية، حيث يسعى عمالقة مجتمع الأعمال إلى الحصول علي المعلومات سواء كانت الطرق مشروعة أو غير مشروعة.

كذلك يمكن أن يصيب هذا النوع من الاعتداء المعلومات المخزنة في ذاكرة الحاسبات الموجودة لدى المحامين والأطباء ومراكز البوليس والنقابات المهنية والأحزاب السياسية، كما يمكن أن يتحقق هذا الاعتداء كذلك بالنسبة للمعلومات العسكرية وهي معلومات تكثر الطلب عليها خاصة الدول الأجنبية[2].

ثانيا: الاعتداء الواقع على الأشخاص

يمكن أن يقع ضحية هذه الجرائم جميع الأشخاص سواء الطبيعية أو المعنوية – العامة والخاصة – طالما كان استخدام الحاسب الإلكتروني في ممارسة أنشطة اقتصادية، الاجتماعية والسياسية وحتى العسكرية. من الصعب تحديد نطاق ضحايا هذه الجرائم على وجه الدقة لأن

---

[1] – « أن المعلومات قوة اقتصادية، والقدرة على تخزين أنواع معينة من البيانات ومعالجتها يمكن أن يعطي بلدا مميزات أساسية وتكنولوجية على البلدان الأخرى، وهو ما قد يؤدي إلى فقدان السيادة الوطنية من خلال انتقال البيانات فيما بين الدول ». **هشام محمد فريد رستم**، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، اسيوط، 1992، ص 16.

[2] – **محمد سامي الشوا**، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة،1998، ص 28.

الضحايا غالبا لا تعلم شيئا عنها وان علمت فنادرا من تقوم بالإبلاغ عنها حتى لا يعلن عن انتهاك نظامه[1]. يأخذ الاعتداء الواقع على الأموال احدى الصور التالية:

أ- انتشار الشائعات والأخبار الكاذبة التي تحمل رموز الشعوب سواء أكانت تلك الرموز فكرية سياسية أو دينية، ظهرت في شبكة الأنترنت بعض المواقع المشبوهة والتي جندت نفسها لهدف واحد هو خدمت تلك الشائعات والأخبار الكاذبة تركز هجومها في الغالب على إبراز سلبيات الشخص المستهدف ونشر بعض أسراره التي تم الحصول عليها بطريقة غير مشروعة بعد الدخول على جهازه والعبث فيه أو بتلفيق تهم كاذبة عنه، جرم قانون ولاية أركانساس -أحد الولايات المتحدة الأمريكية- ARK Code amn. §5-41-108 (2000) جريمة التخويف أو الترهيب أو التهديد أو الإساءة ضد أي شخص باستخدام البريد الإلكتروني أو أية وسيلة اتصال أخرى[2]

ب- تدمير الشباب بدفعهم للانتحار، ففي أقل من شهر، سجلت لعبة "الحوت الأزرق" الإلكترونية ثاني ضحية لها في الجزائر، حيث أقدم طفل في التاسعة من عمره على الانتحار، بعد أن تجاوز كل مراحل اللعبة ووصل إلى تحدّي الموت، فلف حبلا حول عنقه داخل حمام المنزل وشنق نفسه بطريقة مثيرة[3].

ج- السب والتشهير عبر البريد الإلكتروني فالسب يكون باستخدام خاصية الإرسال الفردي المتوافرة في البريد الإلكتروني، أما التشهير يكون باستخدام خاصية الإرسال الجماعية، بحيث يتم السب عبر قائمة المراسلات وتصل المراسلة إلى الفرد المقصود بالسب ويطلع على المراسلة مجموعة الإفراد المشتركين في قائمة المراسلات.

---

[1]- **عفيفي كامل عفيفي**، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، الطبعة الثانية، منشورات الحلبي الحقوقية، بيروت، 2007، ص 28.

[2] - ***Arkansas* Code** AMN. §5-41-108 (2000) ,in ; https://law.justia.com/codes/arkansas/2010/title-5/subtitle-4/chapter-41/subchapter-1/5-41-108/

[3]- **منية غانمي**، الجزائر.. هكذا يقود "الحوت الأزرق" الأطفال إلى الانتحار، العربية. نت، 11ديسمبر 2017 محمول من الموقع الإلكتروني التالي:https://www.alarabiya.net/ar/north-africa/2017/12/1/، تم الاطلاع عليه يوم: 2017/12/20.

د- جرائم ارتياد المواقع الإباحية، الشراء منها أو إنشائها، أما القوائم البريدية فهي تخصص لتبادل الصور والأفلام الجنسية وغالبا تكون مجانية ويشترك فيها آلاف الأشخاص[1]، واستفادة هذه المواقع والقوائم من الانتشار الواسع لشبكة الأنترنت والمزايا الأخرى التي تقدمها حيث تتيح أفضل الوسائل لتوزيع الصور الفاضحة والأفلام الخليعة بشكل علني فاضح يقتحم البيوت والمكاتب، دون حدود دولية أو جغرافية[2].

يحظر القانون تبادل الصور التي تُظهر القصر –الأطفال- في أوضاع منافية للآداب، ومن التشريعات التي تحظر هذا النوع من التعاملات التشريع الكندي، حيث تنص المادة 163-1 من قانون العقوبات الكندي[3] على عقاب كل شخص يحوز صورا جنسية خاصة بالقصر، كذلك القانون الفرنسي[4] والتشريع الأمريكي في قانون آداب الاتصالات عام 1996.

حتى المشرع الجزائري جرم في المادة 10 من القانون رقم 14-01 المعدلة للمادة 333 مكرر 1 من قانون العقوبات الجزائري [5] كل من صور قاصرا لم يكتمل سن 18 سنة بأي 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 بيعا وحيازة مواد إباحية متعلقة بالقصر.

---

[1] – قررت إحدى المحاكم في اسكتلندا وضع المتهم نيل روس الذي يبلغ من العمر 61 سنة، على قائمة مقترفي الاعتداءات الجنسية ضد الأطفال، بعدما تبين لها أن علاقة مع فتاة التي لم تبلغ السن القانونية قد استمرت خمس أشهر على شبكة الأنترنت، كان يطلب منها التجرد من ملابسها بالكامل أثناء دردشتها عبر كاميرا الويب، اعترف روس بارتكابه أفعالا وسلوكيات غير مهذبة تجاه الفتاة أدانته المحكمة بممارسة الجنس عبر الأنترنت مع فتاة قاصر، بعد تعرفهما في غرفة الدردشة على الأنترنت، كما أدانته بتهمة التقاط صور فاضحة للفتاة، وقضت بمعاقبه بالسجن لمدة خمس سنوات.
John Wilson RANDRIAMAHAFALY, De l'evolution de la cybercriminalité, mémoire de maitrise, université de Toliara, Madagascar, 2010, p29

[2]- **Pascal VERGUCHT**, La répression des délits informatique dans une perspective internationale, Thèse de doctorat, Montpellier, 1996, p 37.

[3] –Loi concernant le droit criminel, L.R.C ,1985,ch.c-46, in ;law-loi.justice.g.c.ca/pdf/c-46.pdf.

[4] - Article 227-23 du code pénale Français, in ;
https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 .

[5]– قانون رقم 14-01 مؤرخ في 4 ربيع الثاني عام 1435 الموافق 4 فبراير 2014، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو 1966 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية عدد 07 بتاريخ 16 فبراير 2014.

المطلب الثاني

أساليب إرتكاب الجريمة المعلوماتية

إن الهدف الأساسي لارتكاب الجرائم المعلوماتية هو الحصول على معلومات إلكترونية، مما تشمله من بيانات ومعطيات وبرامج بكافة أنواعها، والتي قد تكون إمّا مخزنة في نظم المعالجة الآلية، أو تلك المنقولة عبر شبكة الأنترنت [1]. تتشابه الجرائم المعلوماتية مع الجرائم التقليدية من حيث استخدام المجرم لوسائل وأساليب غير مشروعة في سبيل ارتكابه لجريمته، بالتالي قد تقع على النظام المعلوماتي المزدوج بين الحوسبة والإتصال بشبكة الأنترنت، كما قد تقع داخل هذا النظام أي على المعلومات والبرامج. ومع ذلك فإن جرائم المعلوماتية تتميز بارتكابها من طرف مجرمين يستعملون كل ما من شأنه خداع الحاسب الآلي والتحايل على أنظمته المعلوماتية، وتتنوع أساليب ارتكاب الجريمة المعلوماتية التي يستعمل من خلالها المجرمون تقنيات مختلفة لتنفيذ جرائمهم وحتى وإن أمكن حصرها في الوضع الراهن إلا أنه لا يمكن التنبؤ بالوسائل الفنية التي قد تستحدث في مجال تكنولوجيا المعلومات.

الفرع الأول

بالنسبة الجريمة المرتكبة بواسطةالنظام المعلوماتي

يتم السلوك الإجرامي للجريمة المعلوماتية بطرق متعدد ومتنوع، فمن أهم أساليب ارتكاب الجرائم المعلوماتيةيذكر:

أولا: استغلال البيانات المخزنة بشكل غير قانوني

يتمثل هذا الأسلوب في الغش في أنظمة معالجة البيانات الآلية مثل التحايل أو انتهاك لسلامة الجهاز، إدراج تسجيل ملف، تجسس عن رموز المشتركين، تدخل في نظام لعرض أو تنفيذ عمليات واحدة أو أكثر سرقة البيانات، التجسس الإلكتروني، أو جرائم الاعتداء على حرمة الحياة الخاصة، سواء حرمة المعلومات الشخصية المخزنة في قواعد ونظم المعلومات كالدخول

[1] - **Marie BAREL**, Fraude informatique et preuve : la quadrature du cercle ? ,p2, in ; http://sondage.sstic.org/SSTIC05/Delits_informatiques_et_preuve/SSTIC05-article-Barel-Delits_informatiques_et_preuve.pdf. consulté le 02/01/2016.

والتداول غير المرخص للمعلومات واستخدامها لغير الغرض الذي أعدّت من أجله، أو حرمة الإنسان في المراسلات والأحاديث الخاصة والموجودة في الملفات الشخصية للبريد الإلكتروني[1].

ثانيا: استخدام الحاسب الآلي بشكل غير قانوني من قبل الأفراد المرخص لهم باستغلاله

يتمثل هذا الأسلوب في إفشاء الأسرار، تسريب المعلومات، اختلاس المعلومات، اختلاس أموال معلوماتية التزوير المعلوماتي، جرائم الأموال حيث أن الحاسب أصبح أداة سلبية للاعتداء على أموال الغير لاسيما في نطاق شبكة الأنترنت مما أدى إلى خلق صور مستحدثة من الجرائم كجريمة غسل الأموال عبر الأنترنت، الجرائم المتعلقة بالتجارة الإلكترونية كالتصريح عمدا لمعطيات خاطئة، جرائم التهرب الضريبي[2].

يوجد تمييز ينبغي مراعاته يتعلق بفصل هذه الجريمة عن جريمة الحيازة غير المشروعة لكلمة المرور لمواقع أو صفحات عبر الأنترنت ذاتها، ففي هذه الحالة الأخيرة يكون المعتدي موجودا على الأنترنت بشكل مشروع، إلا أنه يقوم بارتكاب دخول غير مشروع على مواقع وصفحات عبر الأنترنت يستلزم للولوج إليها الحصول على كلمة المرور[3].

ثالثا: استخدام الحاسب الآلي للتخطيط أو تنفيذ جرائم تقليدية

مثل استخدامه في جريمة تزوير المحررات الرسمية أو العرفية، تزييف العملة، جرائم الأخلاق كالقذف والسب والتشهير عبر الأنترنت وغيرها من وسائل الاتصال الحديثة كالهاتف المحمول عن طريق تقنية الرسائل، سواء كانت رسائل نصية SMS، أو عن طريق وسائل MMS، جرائم الاستغلال الجنسي للأطفال، جرائم القتل عن طريق استخدام التقنية

---

[1] – **فتحي محمد أنور عزت**، الحماية الجنائية الموضوعية والإجرامية على المصنفات والحق في الخصوصية في الكمبيوتر والأنترنت في نطاق التشريعات الوطنية والتعاون الدولي، دار النهضة العربية، القاهرة، 2007 ص 161.

[2] – راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، ورقة عمل مقدمة إلى المؤتمر الدولي الأوّل حول "حماية أمن المعلومات والخصوصية في قانون الأنترنت برعاية الجمعية الدولية لمكافحة الإجرام السيبري بفرنسا، القاهرة 2–4 يونيو 2008، ص 5.

[3] – **فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، دار النهضة العربية، القاهرة، 2010، ص297.

الحديثة ببرمجة جهاز التفجير أو إطلاق أشعة قاتلة يتم التحكم فيها آليا أو الدخول إلى قواعد البيانات الصحية والعلاجية وتحويرها عبر التلاعب ببرمجياتها، الجرائم الإرهابية وذلك عن طريق الاتصال بعناصر التنظيم الإرهابي لتنفيذ الجريمة[1].

الفرع الثاني:

بالنسبة للجرائم المرتكبة داخل النظام المعلوماتي

أولا : استغلال نظم المعلومات كمحور أساسي في الجريمة المعلوماتية

يتمثل أسلوب الجريمة في تدمير نظام المعلومات –أو البرامج التي تحتوي عليها– من خلال التسلل إلى المواقع وبث الفيروسات أو البرامج المخربة التي تمحو البيانات وتعرقل سير العمل بل ترسل معلومات مظللة غير حقيقة تؤدي إلى خسائر اقتصادية فاضحة[2]، ومن أهم هذه تقنيات الاختراق واستعمال البرامج الخبيثة (Virus) يشرح فيما يلي:

أ– **الاختراق phishing**[3]: تقوم معظم جرائم المعلوماتية على تقنية الاختراق وذلك بغرض الدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات، والاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف أو الوصول إلى البيانات الموجودة على الأجهزة الشخصية بوسائل غير مشروعة.

لا يحتاج التسلل إلى جهاز الضحية علمه، فقد يتم الاختراق عن طريق:

1. استخدام نظم التشغيل لكونها مليئة بالثغرات من خلال البروتوكولات IP التي يستخدمها نظام التعامل مع شبكة الأنترنت.
2. استخدام البرامج، ويشترط في هذه الطريقة وجود برنامجين أحدهما بجهاز الضحية

---

[1]– **أيمن عبد الله فكري**، جرائم نظم المعلومات، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2006، ص 87.

[2]– راجع كل عن: **عبد الفتاح بيومي حجازي**، الجريمة في عصر العولمة دراسة في الظاهرة الإجرامية المعلوماتي، دار الفكر الجامعي، الاسكندرية، 2010، ص 76. **حاتم عبد الرحمن منصور الشحات**، الإجرام المعلوماتي، دار النهضة العربية، القاهرة 2002، ص 32، 55.

[3] – **مسعود كبها**، اختراق hackingteam، محمول من الموقع الإلكتروني التالي:

http://www.arageek.com/tech/2015/07/11/hacking-team-hack.htm تم الاطلاع عليه يوم.: 2016/08/29.

ويسمى بالبرنامج الخادم لأنه ينفذ المهام الموكلة إليه داخل جهاز الضحية وبرنامج آخر يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد[1].

3. أسلوب التفتيش في مخلفات التقنية وذلك بالبحث في مخلفات الحواسيب من القمامات والمواد المتروكة على مستوى الجهاز عن أي شيء يساعد على اختراق النظام.

4. انتحال شخصية الموقع، يقوم هذا الأسلوب على قيام المخترق بوضع في موقع بيني بين البرنامج المستعرض للحاسب الخاص بأحد مستخدمي الأنترنت وبين الموقع (WEB) ومن هذا الموقع البيني يستطيع المجرم المعلوماتي من خلال جهاز حاسوبه مراقبة أي معلومة متبادلة بين الضحية الذي يزور الموقع وبين الموقع نفسه، كما له أن يقوم بسرقة هذه المعلومات أو تغييرها[2].

ب- البرامج الخبيثة (Les Virus): تعد الفيروسات بمثابة المرض المعدي الذي يصيب المعطيات فيقضي عليها أو يشوهها فتذهب في كلتا الحالتين بفائدتها، وفيروس الحاسب الآلي يشبه إلى حد كبير الفيروس الذي يصيب الإنسان لقدرته على الانتقال من حاسب إلى آخر، فهو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي يصمم

---

[1]- أخطر هذه البرامج برنامج "حصان طروادة"، وتتجلى خطورته لتميزه بالقدرة على الاختراق دون أمكانية كشفه وتتبعه والقضاء عليه واحتلال هذا البرنامج مكانا داخل النظام المخترق حتى ولو قام الضحية بحذفه فلا فائدة من ذلك، كما أنه يكفي أن يعمل البرنامج هذا لمرة واحدة فقط حتى يقوم بمهام، ويمكن إرساله للضحية عن طريق رسائل إلكترونية أو عن طريق استخدام برامج الدردشة، وبواسطته يتمكن المخترق أن يحصل على كلمة سر الدخول على الجهاز ويدخل بطريقة لا تثير أي شك، وهذا ما يزيد من خطورة هذا البرنامج. **John Wilson RANDRIAMAHAFALY**, op.cit, p20-22.

[2]- وكل ما يحتاجه من يقوم بهذه العملية هو السيطرة على أحد المواقع التي تتم زيارتها بكثرة وتحويله ليعمل كموقع بيني ثم يقوم المخترق بتركيب البرنامج الخاص به هناك، وبمجرد أن يكتب مستخدم الأنترنت اسم هذا الموقع فإنه يدخل في هذا الموقع المشبوه الذي أعده المخترق. يمكن أن يكون الاختراق هنا باستخدام البروكسي للدخول على المواقع المحجوبة: والبروكسي هو برنامج يقوم بحصر ارتباط جميع مستخدمي الأنترنت في جهة واحدة ضمن جهاز موحد، والمعنى المتعارف عليه لدى مستخدمي الأنترنت للبروكسي هو ما يستخدم لتجاوز المواقع المحجوبة والتي عادة ما تكون هذه المواقع المحجوبة أما مواقع جنسية أو سياسية معادية للدولة أو مواقع علمية خاصة أو حتى بعض المواقع العادية، لذلك من يستخدم البروكسي للدخول إلى هذه المواقع خطأ يستوجب المسؤولية.

John Wilson RANDRIAMAHAFALY, op.cit, p25. **Pascal VERGUCHI**, op.cit, p 125.

بشكل يجعل منه قادرا على نسخ نفسه إلى نسخ كثيرة[1] والانتشار من نظام لآخر عبر شبكات الاتصال والقدرة على الاختفاء داخل برنامج سليم بحيث يصعب اكتشافه، كما أنه قد يكون مصمما لتدمير برامج أخرى أو تغيير معلومات ثم يقوم بتدمير نفسه ذاتيا دون أن يترك أي أثر يدل عليه[2] فبمجرد فتح البرنامج الحامل للفيروس أو الرسائل البريدية المرسل معها الفيروس يصابة الجهاز به ومن ثم يبدأ الفيروس بالعمل طبقا للأسلوب الذي صممت من أجله .ومن أمثلة الفيروسات يذكر: Le cheval de Troie، La porte dérobée[3]، Le logiciel espion، Le key logger

ثانيا : جرائم تضخم البريد الإلكتروني (E-Mail)

يعد البريد الإلكتروني باختصار أحد أهم الخدمات التي توفرها شبكة الأنترنت وأكثر أدواتها، بالإضافة إلى كونه أحد أهم خدمات الاتصال الشخصي، تقوم فكرة البريد الإلكتروني على تخصيص مزود البريد الإلكتروني مساحة على الحاسوب الخادم، فيكون لكل مشترك في هذا المزود مساحة فرعية خاصة به وعنوانا خاصا به[4]، يمكن من خلاله تبادل الرسائل الإلكترونية والملفات، والرسوم والصور... الخ، عن طريق إرساله من المرسل إلى شخص أو أكثر، والبريد الإلكتروني في الوقت ذاته شبيه بصندوق البريد العادي، مع فارق وجود الرسائل الواردة والصادرة

---

[1] – للبرامج الخبيثة ستة مستويات للاختراق بحسب درجة الخطورة:

- المستوى الأول: يعرف أنها هجوم قنبلة صندوق البريد ويؤدي إلى إعاقة النظام عن تقديم الخدمة.
- المستوى الثاني: الدخول غير مرخص به لنظام المعلومات والحسابات بما يتيح قراءة الملفات أو نسخها للمخترق غير مرخص له.
- المستوى الثالث: يتمكن المخترق فيه من الدخول إلى مواقع غير مرخص له بالدخول إليها.
- المستوى الرابع: يتمكن المخترق فيه من قراءة ملفات سرية.
- المستوى الخامس: يتمكن المخترق من نقل ونسخ الملفات السرية
- المستوى السادس: يتمكن المخترق من إيجاد قناة مفتوحة للدخول إلى سائر أرجاء النظام والعبث بمحتوياته.

فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص 343.

[2] – **سعيداني نعيم**، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة باتنة، 2013، ص 60، 62.

[3] – حول التعريفات المختلفة للفيروسات راجع:

- **Dominique LALOUX**, Les virus informatiques, Morabout Alleur, Belgique 1989, p 261.
- **Jan HRUSKA** ,Virus informatiques et lutte anti-virus, Paris, 1992, p20.

[4] – أنواع عناوين البريد الإلكتروني: العنوان الإلكتروني يتخذ أحد صورتين، إما أن يكون عنوانا إلكتروني دولي تشير الى انشطة دولية عامة مثل (com.) أو عنوان إلكتروني وطني تشير الى اسم الدولة التي ينتمي اليها العنوان مثل(dz.) **شريف محمد غنام**، حماية العلامات التجارية عبر الأنترنت في علاقتها بالعنوان الإلكتروني، دار النهضة العربية، القاهرة، 2003، ص96.

André BERTRANT , **Thierry PIETTE-COUDOL** , Que sais-je ? Internet et le droit ?p.u.f , 2000, p 53.

وكذا الرسائل التي ألغيت ولا يشترط أن يتم إرسال رسالة البريد الإلكتروني من كمبيوتر المرسل الخاص به أو باستخدام اشتراكه الخاص بخدمة البريد الإلكتروني، بمعنى أنها قد ترسل من أي جهاز إلى أي خادم وبأي اشتراك[1]، كما يمكن أن يضمنها المرسل اسمه الحقيقي واسم مستعار أو اسم لشخص آخر أو يستخدم عنوان البريد الإلكتروني لشخص آخر فيرسل الرسالة باسمه، وهي في صورها الأولية رسالة غير موقعة، لكن التطور التقني أوجد العديد من وسائل توقيعها وربطها بشخص مرسلها ومن ذلك استخدام التوقيع الإلكتروني في نسبة الرسائل إلى مصدرها[2].

•يعد العدوان بتضخيم البريد الإلكترونيSpam أكثر صور العدوان على قواعد البيانات تداولا، بل أشهرها يتم بتوجيه بريد إلكتروني مجهول المصدر يسبب مشاكل ضخمة للمتعاملين به يأخذ العدوان بالإثقال شكل وصول الرسائل إلى حساب البريد الإلكتروني للمستسلم النهائي مجهولا للمصدر، ويستخدم في إرسالها برمجيات معدة خصيصا لذلك، وهي برمجيات محظورة لكونها تهدد قواعد البيانات بتضخيم قاعدة عمل البريد الإلكتروني، بحيث إذا امتلأ لم يعد بالإمكان فتحه والتعامل به، فالتضخم الحادث فيه أدى إلى الامتناع عن تأدية الخدمة المنوطة إليه[3]، وعادة ما تتضمن الرسائل موضوعات فاضحة أو مواد دعائية لمشروعات وهمية،... الخ.

ثالثا : جرائم استعمال الأنترنت الخفي

بدأ ظهور بجانب شبكة الأنترنت العادي التقليدي، نوع آخر من الأنترنت الخفي الذي يطلق عليه اسم Darknet، الذي لا يعرف فيه عن المتعامل به سواء المرسل أو المرسل إليه أي معلومة من المعلومات الشخصية سواء الاسم، الجنسية، محل الإقامة إلى غيرها من المعلومات الشخصية[4].

---

[1] - **Adam C ENGST**, Internet starter Kit for Macintosh, 4th Edition, Hayden Books, U.S.A, 1996, in; http://vintageapple.org/macbooks/pdf/Internet_Starter_Kit_for_the_Macintosh_4th_Edition_1996.pdf . consulté le 22/10/2016.

[2] – خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الاسكندرية، 2010، مرجع سابق، ص 55.

[3] -« Le spam peut bien étre présenter comme : spam couriel, spam SMS, spam vocal », **Emmanuelle MATIGNON**, la cybercriminalité : un focus dans le monde du télécom, mémoire master droit du numérique admistrations, école de droit de la sorbonne, université paris1,paris , 2011−2012 , p 27-28.

[4]– إن هذا النوع من الأنترنت في البداية صنعته القوات العسكرية الأمريكية وذلك بهدف حماية المعلومات العسكرية السرية وكل ما يتعلق بسيادة الدولة، ثم بدأ استعمال Darknet من أجل التصدي للأنظمة الدولية العربية الديكتاتورية والإطاحة بها، قد استعمل لتحريض الشعوب للنهوض بالدفاع عن حقوقهم وحرياتهم التي لطالما عاشوا بدونها، وبالتالي تم إسقاط النظام العراقي، التونسي، المصري وفي سوريا.

بدأت الجهات الإرهابية[1] ومرتكبي الإجرام المنظم العابر للحدود خاصة تجار المخدرات غير المشروعة وتجار الأسلحة غير المشروعة وتجار الأفلام الإباحية للأطفال باستعمال Darknet لترويج بضاعتهم، وقد نجحوا في ذلك دون أن تتمكن الجهات الأمنية المختصة من التوصل إليهم.

يوجد في شبكة Darknet موقع يطلق عليه اسم TOR تستعمله الجهات الإجرامية في بيع أو شراء كل ما تريده من مواد غير مشروعة دون ترك أي معلومة شخصية ولا موقع محدد متعلق به، حيث يمكن أن يكون عند إجراءه العملية في فرنسا ثم بعد بضع ثوان يسجل مكانه في أي بلد آخر من العالم مثلا رومانيا، وبالتالي لا يمكن التوصل إلى مكان وجوده.

كيف تتم عملية البيع والشراء عبر شبكة Darknet؟

البائع صاحب البضاعة غير المشروعة يعرض كل بضاعته في جدول، المشتري يحدد نوع من هذه البضاعة والكمية التي يريدها، دون أن يحدد موقعه، بل يقوم بذلك عبر رموز من الصعب جدا فكُّها أو فهمها، **البائع** يحضر البضاعة المطلوبة ويغلفها في شكل بلاستيكي متطوّر لا يسمح للرائحة بالخروج –إذا كانت البضاعة مخدرات– ويبعثها في شكل رسالة، أو طرد بريدي عادي، أمّا بالنسبة للأسلحة غير المشروعة والأفلام الإباحية الخاصة بالأطفال، فقد يتم إدخالها بهدف إخفاءها في تلفزيون أو شاشة الحاسوب أو أي شيء لا يثير الشك، ثم يبعث في صورة طرد عن طريق البريد، أما المشتري فعندما يستلم الرسالة أو الطرد البريدي وذلك بكل سهولة، فعليه دفع مقابل البضاعة (الثمن).

فكيف يتم ذلك؟

يفتح المشتري حساب بنكي يدخل فيه أموال أو نقود ملموسة ثم يطلب تحويلها إلى نقود غير ملموسة يتعامل بها عبر الأنترنت ويطلق على هذا النوع من النقود اسم bitcoin "البيتكوين" العملة الإلكترونية، يتم سحبها من حساب إلى آخر دون استعمال نقود مادية[1]، فيقوم بشراء عدة أشياء عبر الأنترنت ويدفع مقابلها بـ bitcoin وليس بالطريقة التقليدية التي تستعمل في الأنترنت

[1]– جرم المشرع استخدام تكنولوجيا الإعلام والاتصال لارتكاب أفعال إرهابية، أو تجنيد الأشخاص لصالح إرهابي، في المادة 87 مكرر 11 فقرة 4 و5 المعدلة بموجب المادة 2 من قانون رقم 16–02 مؤرخ في 14 رمضان عام 1437هـ الموافق ل19 يونيو سنة 2016 يتمم الأمر رقم 156-66المؤرخ في 18 صفر عام 1386هـ الموافق 8 يونيو سنة 1966 تضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية عدد 37 بتاريخ 22 يونيو 2016.

العادي وهو إمّا بطاقات الائتمان أو بتقديم رموز للبطاقات البنكية... الخ

البائع عندما يحصل على bitcoin داخل حسابه البنكي، يمكنه عندئذ أن يجسدها على شكل أوراق نقدية ملموسة وهكذا يجد المجرمون حريتهم في عمليات البيع والشراء ما دامت الجهات الأمنية الدولية لم تجد حلا نهائيا لغلق هذا الأنترنت الخفي وضبط المجرمين المتعاملين به، حيث تمكنت قوات FBI الأمريكية من غلق أحد مواقع Darknet وذلك في أكتوبر 2014 الذي تمت من خلاله عدّة جرائم، لكن في اليوم التالي من ذلك تمكن المجرمون من إعادة تشغيله مرّة أخرى[2].

رابعا: نظام التشفير

يجعل نظام التشفير إقامة الدليل على ارتكاب الجريمة أمرا مستحيلا، وهذا ما حدث في قضية السيد Fowrisson، حيث نشرت رسائل عنصرية ومضادة لليهودية تحمل اسم Robert Fowrisson وتم اكتشافها على أحد المواقع بعنوان Arargh والذي تم إيوائه في أمريكا، إلا أن المحكمة لم تستطع إقامة الدليل على أن هذا المتهم هو صاحب الرسالة المجرمة، الأمر الذي يقتضي إلزام معهد الوصول بتحديد شخصية المشترك وعدم توصيل الأسماء المجهولة بشبكة الأنترنت [3].

لعل من مظاهر أهمية التشفير هو أن المعلومة حين الشروع بإرسالها إلى المستقبل النهائي إما عن طريق بريد إلكتروني أو التراسل المباشر(الصوتي أو المرئية) قبل أن تصل إليه تكون عرضة لاطلاع الغير عليها[4]، وهذا أمر وارد دائما إزاء التطورات القوية في نشاط الهكرة عبر الأنترنت. إن لتقنية إخفاء المعلومات بتشفيرها جانب سلبي، فالمنظمات الإرهابية عبر الأنترنت لا تتوانى عن إعداد مواقع مشفرة لتعاملاتها والتعامل فيما بينها، فالتشفير يعد من المشكلات التي تواجه المشرع المقارن[5].

---

[1] – **جميل عبد الباقي الصغير**، الأنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2002، ص 6.

[2]-Envoyé spécial 2014, le côté obscur du Net Darknet- Reportage complet, –in ; https://www.youtube.com/watch?v=AERRgC-GIuM. Consulté le : 17/11/2014.

[3] – **فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص 322، 234.

[4] -**Myriam QUEMENER**, Cybercriminalité défi mondial et réponses, Economica, Paris, 2007, p 240.

[5]– يعاقب عليه قانون العقوبات الفرنسي في المادة 392–3.

الفرع الثالث

أهم طرق كشف الجريمة المعلوماتية

يصعب حصر مجموعة الجرائم التي ترتكب عبر الأنترنت، حيث أن أشكالها والطرق المتبعة فيها متنوعة وتزداد تنوعا وتعدادا كلما زاد التوغل في استخدام الحاسب الآلي وشبكة الأنترنت.

يمكن اكتشاف الجرائم المعلوماتية بشكل عام بإحدى هذه الطرق:

- يمكن اكتشافها من قبل احد المستخدمين الذي قد يشتبه في ولوج شخص آخر إلى حاسوبه بشكل غير مشروع وذلك بواسطة برامج خاصة أعدت لذلك الغرض.
- ضبط المجرم بالجرم المشهود وهو يحاول اقتحام غرفة الحاسوب أو المبنى الخاص به، أو أن يلاحظ مدير النظام الحاسوب أثناء ولوجه إلى النظام أن هناك شخص آخر متصل بالنظام من خارج المنظمة بواسطة نوع من أنواع النظام الشبكي وباستخدام نفس اسم المستخدم وكلمة المرور الخاصة بمدير النظام، وكذلك قد تكون برمجيات متطورة خاصة بالحماية باكتشاف الخطر مثلا فور حدوثه وبطريقة آلية، وذلك بتوجيه إنذار فور تحسسها لأي نشاطات مشبوهة على الشبكة لمدير النظام أو للمستخدم للحاسوب أو الشبكة.
- اكتشاف الجريمة المعلوماتية من خلال الأدلة المتحصل عليها.

إلا انه وبالرغم من التوصل إلى اكتشاف بعض الجرائم المعلوماتية بالطرق سالفة الذكر إلا انه تبقى النسب ضئيلة جدا مقارنة بالعدد الجرائم التي ترتكب دون التمكن من كشفها، ويرجع ذلك إلى صعوبات عديدة.

هناك الكثير من الأسباب تصعب عملية إكتشاف الجرائم المعلوماتية توجز في الآتي:

- إن الجرائم المعلوماتية لا تقتصر على مكان وزمان معين، فأجهزة الحاسوب والمحمول وشبكات المعلومات أصبحت في متناول الجميع، بذلك يمكن ارتكاب الجريمة في داخل المنزل، أو في أماكن العمل، أو في السيارة، أو على ظهر سفينة، أو حتى على متن طائرة.
- إن أشكال هذه الجريمة تتغير بسرعة فائقة تتجاوز أحيانا سرعة التوعية بأخطارها والتعامل معها والتقليل من مخاطرها.

– صعوبة تعقب تلك الجرائم وتداخل أكثر من وسيلة في وقوعها، فعلى سبيل المثال يمكن التواصل بأجهزة محمولة في اليد مع أجهزة الحاسب الآلي مع شبكات المعلومات، مما ييسر ارتكاب هذه الجريمة ويؤدي إلى صعوبة الوصول إلى مرتكبيها.

– يشترك في الجرائم المعلوماتية، أفراد ذو أعمار وهويات مختلفة، فمنهم الأطفال، ومنهم مبرمجو الكمبيوتر، ومنهم الموجودين في دول مختلفة عن تلك التي يقع فيها الاعتداء على نظم المعلومات، وكل ذلك يؤدي إلى صعوبة القبض والمحاكمة في الكثير من الأحوال، ومما يزيد هذه الصعوبات ما يتسم به المجرم الإلكتروني من سمات الذكاء والمهارة والمعرفة أو التورط في مؤامرات التجسس الصناعي[1].

– لا تزال التشريعات الحالية في مختلف بلاد العالم قاصرة عن التعامل مع أنواع الجريمة المعلوماتية، مما يحتاج أحيانا إلى كثير من التعديل لمتابعة ما يطرأ من أشكال جديدة للإجرام الإلكتروني.

– يتجنب المجني عليه الإبلاغ عن هذه الجرائم، لعدة أسباب منها: عدم قدرته الفنية التي تمكنه من اكتشاف الجريمة أو خوفا من الإضرار بمصالحه، لاسيما إذا وقعت الجريمة على مؤسسات مالية ومصرفية أو تجارية كبيرة فربما يؤدي الإبلاغ عن الجريمة إلى تأثر المؤسسة أو مركزها المالي إلى خسائر[2]، وهو ما يعبر عنه بالرقم الأسود، فقد يحجمون عن تقديم الدليل الذي قد يكون بحوزتهم عن هذه الجرائم، وقد يكون مقصدهم من ذلك استقرار حركة التعامل الاقتصادي بالنسبة لهم، أو رغبتهم في إخفاء الأسلوب الذي ارتكبت به الجريمة لكي لا يتم تقليدها من الآخرين[3].

---

[1] – هناك عدة خصائص يتميز بها المجرم المعلوماتي تميزه عن غيره من المجرمين العاديين، ويمكن حصرها ضمن الطوائف التالية: فئة صغار مجرمي المعلوماتية، فئة القراصنة أو المخترقون، ويمكن تصنيفهم إلى صنفين: الهاكرز Les Hakers) و الكراكر ،Les crakers، فئة المحترفين، فئة الحاقدين. **فاضل نصر الله عوض**، "الطبيعة القانونية للاستيلاء على الأموال من البنك الآلي"، مجلة كلية الحقوق الكويتية، تصدر عن كلية الحقوق جامعة الكويت، العدد 122، مارس 1988، ص 283.

[2] – **محمد أحمد عياينة**، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، 2006، ص 37.

[3] – **علي محمود علي حموده**، "الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي"، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث والدراسات، أكاديمية شرطة دبي، الإمارات العربية المتحدة، المنعقد في الفترة 26، 28 أفريل 2003، ص 11.

عادة المؤسسات المالية كالبنوك والمؤسسات الإدخارية وشركات الإقراض والسمسرة هي التي تلجأ لهذا الأمر، حيث يخشى القائمون على إدارتها من شيوع أمر الجرائم التي تقع داخلها على الثقة فيها من العملاء المتعاملين معها، مما قد يؤدي إلى انصرافهم عنها، وهو ما قد يصيبهم بأضرار قد تزيد بكثير عن كشف ستر هذه الجرائم وتقديم مرتكبيها إلى العدالة.

وإذا نظرنا إلى هذا الإحجام عند الإبلاغ عن مثل هذه الجرائم الفنية نجد أنه قد ترتب عليه نتائجتكونلمكافحتها[1].

. سهولة إزالة أدلة إدانة الجاني خلال فترة بسيطة وبالتالي اختفاء الأدلة بسهولة[2].

. قلة الخبرة الفنية وذلك لأن هذا النوع من الجرائم يتطلب خبرة فنية عالية وإلماما واسعا باستخدام الحاسوب[3].لا

المبحث الثاني

موضوع الدليل الإلكتروني

إنّ طبيعة الجرائم المعلوماتية بعناصرها ووسائل ارتكابها قد تدفع المشرع الجزائي إلى أن يعيد النظر في كثير من المسائل الإجرائية، خاصة فيما يتعلق بمسألة الإثبات باعتبارها أهم موضوعات هذا القانون –ذلك أن الدليل الذي قد يقوى على إثبات هذا النوع من الجرائم لابد أن يكون من ذات طبيعته التقنية– وهو الأمر الذي لا تكون فيه القواعد الإجرائية التقليدية قادرة على استخلاص الدليل منه، مما يستوجب تدخل المشرع لتكريس قواعد إجرائية يمكن للجهات المكلفة بالبحث والتحري عن الجريمة المعلوماتية الاعتماد عليها في الوصول إلى الدليل المناسب في إثبات الجريمة المعلوماتية.

---

[1] – **هشام محمد فريد رستم**، "الجرائم المعلوماتية أصول التحقيق الجنائي الفني والية التدريب التخصصي للمحققين"، مجلة الأمن والقانون، تصدر عن أكاديمية شرطة دبي، دولة الامارات العربية المتحدة، السنة الرابعة، العدد الثاني، يوليو 1999، ص 26.

[2] – **محمد حماد مرهج الهيتي**، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، عمان، 2004، ص 166.

[3] – **سعيد عبد اللطيف حسن**، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الأنترنت، دار النهضة العربية، القاهرة، 1999، ص95.

بمعنى آخر ترتكز عملية الإثبات الجزائي للجرائم المعلوماتية على الدليل الإلكتروني باعتباره أهم الوسائل لإثبات وقوعها.

لذا سيتم العمل في هذا المبحث على إبراز ذاتية الدليل الإلكتروني (المطلب الأول)، ثم دراسة أهم تقسيماته (المطلب الثاني).

المطلب الأول

ذاتية الدليل الإلكتروني

ان الدليل هو البرهان المتحصل عليه بالطرق المشروعة لتقديمه للقاضي لتحقيق حالة اليقين لديه والحكم بموجبه، يخلط البعض أحيانا بين الدليل والإثبات لما بينهما من علاقة[1].

ترتكب الجريمة المعلوماتية في وسط معنوي أو ما يعرف بالوسط الافتراضي، فإن التحقيق بواسطة أدلة الإثبات التقليدية أصبح دون معنى إذا لم يكن مدعما بتوفيق من قبل التقنية ذاتها، ظهور طائفة خاصة من الأدلة الجزائية يمكن الاعتماد عليها في إثبات هذه الجرائم ومن ثمة نسبتها إلى فاعلها، بحيث تكون من ذات الطبيعة التقنية للنظم المعلوماتية التي تم الاعتداء عليها، وتتفق مع طبيعة الوسط الذي ارتكبت فيه الجريمة وهي الأدلة الإلكترونية.

يقسم هذا الطلب إلى فرعين، يدرج في الأول تعريف الدليل الإلكتروني وطبيعته، والفرع الثاني يدرس فيه اهم خصائص الدليل الإلكتروني.

الفرع الأول

تعريف الدليل الإلكتروني وطبيعته

إن الدليل الإلكتروني له أهمية كبرى ودور أساسي في معرفة كيفية ارتكاب الجريمة المعلوماتية، بهدف إثباتها ونسبها إلى مرتكبيها، وتقييم أي نظام إلكتروني من الناحية القانونية لا

---

[1]– كلمة الإثبات تجمع كل عناصر التحقيق، وبالتالي يصدق القول بأن الإثبات هو التنقيب عن الدليل وتقديمه وتقديره لاستخلاص السند القانوني للفصل في الدعوى، أمّا الدليل فهو النتيجة النهائية المتحصلة من مراحل الإثبات المختلفة، بمعنى هو ثمرة الإثبات، من ذلك يظهر أن مفهوم الإثبات أوسع من أن ينحصر في كلمة الدليل.
أحمد أبو القاسم، "المفهوم العلمي والتطبيقي للدليل الجنائي المادي"، مجلة مركز بحوث الشرطة، تصدر عن أكاديمية مبارك للأمن، القاهرة، العدد السابع والعشرين، يناير 2005، ص 152.

يمكن أن يصل إلى نتائج صحيحة إلا إذا توافر لدى المقوم تصورا واضحا لذلك النظام، وعليه فانه ومن الواجب ليتسنى فهم طبيعة هذا النوع من الأدلة لا بد من تناول تعريفه.

أولا: تعريف الدليل الإلكتروني

قدم الباحثين في المجال القانوني[1] عدة تعاريف مختلفة للدليل الإلكتروني، ويرجع ذلك لموضوع العلم الذي ينتمي إليه هذا الدليل، فيعرفه البعض بأنه « كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من أنجاز مهمة ما »[2] وهناك من يعرفه بأنه "الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم وذلك من اجل اعتماده أمام أجهزة تطبيق القانون".

حاولت مجمل التعريفات التي جاءت بشان الدليل الإلكتروني إستيعاب هذا النوع المستحدث من الدليل على الرغم من ارتباطه بالعالم الافتراضي إلا أن هناك بعض الإشارات، والتي تتمثل في:

- إنّ بعض التعريفات السابقة مزجت مفهوم البرنامج بمفهوم الدليل الإلكتروني[3]، فقد عد الدليل لإلكتروني بأنه كل معلومة يتم إعدادها أو تخزينها بشكل رقمي كما لو كانت محملة على

---

[1] – **Compagnie Nationale des experts de justice en Informatique et Techniques Associées CNEJITA**, La preuve numérique à l'épreuve du litige, colloque du 13 Avril 2010 à la première chambre de la cour d'appel de Paris, p 9.

[2] – عائشة بن قارة مصطفى، مرجع سابق، ص 29. **خالد ممدوح ابراهيم**، الدليل الإلكتروني في جرائم المعلوماتية، ص 01، محمول من الموقع الإلكتروني التالي:http://kenanaonline.com/users/khaledMamdouh/posts/79345 . تم الاطلاع عليه يوم 2016/05/14.

[3] – إلا انه على الرغم من أن كلا المكونين يتفقان في خصوصية الاتصاق بمفهوم تقني المعلومات من حيث تكوينهما، لأنهما عبارة عن آثار معلوماتية رقمية تستخدم الشبكة المعلوماتية أو الأنترنت ويظهران في الشكل الرقمي. لان المعلومات داخل نظام المعالجة الآلية سواء كانت نصوص أو أحرف أو أرقام أو أصوات أو صور أو فيديو أو برامج تتحول إلى طبيعة رقمية حيث ترتكز تكنولوجيا المعلوماتية على تقنية الترقيم التي تقوم بترجمة أي مستند معلوماتي وتحويله إلى نظام ثنائي في تمثيل الإعداد قوامه الرقمان الصفر والواحد، إلا أن الفرق بين الدليل الإلكتروني وبرنامج الحاسب الآلي يكمن في الوظيفة التي يؤديها كل واحد منهما، فهذا الأخير له دور في القيام بمختلف العمليات التي يحتويها نظام المعالجة الآلية، عن طريق مجموعة من الأوامر بذلك، أما الدليل الجزائي الإلكتروني فله أهمية كبرى ودور أساسي في معرفة كيفية حدوث جرائم تقنية المعلومات بهدف إثباتها ونسبتها إلى مرتكبيها. **ممدوح عبد الحميد عبد المطلب**، استخدام بروتوكول tcp/ip في بحث وتحقيق الجرائم على الحاسوب، ورقة عمل مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الإمارات العربية المتحدة، المنعقد في الفترة 26 –28 نيسان 2003، ص 7.

وسيط معين يمكن قراءته عن طريق الآلة والتي تؤدي عند تنفيذها في النظام المعالجة الآلية إلى إنجاز وظيفة ما، ومثل هذا التعريف يتفق مع مفهوم البرنامج المعلوماتي[1].إلا أنه لا ننفي وجود برامج خاصة تساهم استخلاص الدليل الإلكتروني مثل: برنامج معالجة الملفات مثل: (X tree pro gold)، وبرنامج النسخ مثل (lap link[2])، بل أكثر من ذلك قد تعد بعض البرامج لوحدها دليلا إلكترونيا مثل برنامج الاختراق (asylum).

– كما حصرت بعض التعريفات السابقة الأدلة الإلكترونية في تلك التي يتم استخراجها من الحاسوب الآلي، ولا شك أن ذلك فيه إضافة إلى دائرة الأدلة الإلكترونية، فهي كما يمكن أن تستمد من الحاسب الآلي، فمن الممكن أن يحصل عليها من أية وسيلة تقنية أخرى[3].

ان الدليل الإلكتروني تشير مقدمات التعامل معه بكونه يعبر عن تجاوب متكامل يتطور بسرعة كبيرة جدا، فبعد أن كان الدليل الصامت يشير إلى ما يمكن الحصول عليه بطريق الطابعة، وهو ما يسمى بمخرجات الحاسوب مثال الوثائق والصور... الخ، فإن التطور اقتضى أن يكون له منطق آخر يعبر عنه المظهر التقني المعلوماتي المتسم بالحركة والذكاء[4]، فهو المعلومات ذات القيمة المحتملة أو المخزنة أو المنقولة في صورة رقمية، ويمكن الاعتماد عليها أمام المحكمة.

إنّ الدليل الإلكتروني في المسائل الجزائية لا يقتصر دوره في إثبات الجرائم المعلوماتية فحسب، كسرقة الملكية الفكرية، واستغلال الأطفال في المواد الإباحة، والتحرش الجنسي بل يتعداه إلى الجرائم التقليدية كالإتجار بالمخدرات،جرائم القتل،الاختطاف التي تستخدم فيها التكنولوجيا

رشيدة بوكر، "الدليل الإلكتروني ومدى حجيته في الإثبات الجزائي في القانون الجزائري"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، تصدر عن كلية الحقوق جامعة دمشق، المجلد 27، العدد الثاني، 2011، ص305،307.

[1] – **فاروق علي الحفناوي**، موسوعة قانون الكمبيوتر ونظم المعلومات قانون البرنامجيات دراسة متعمقة في الأحكام القانونية ببرمجيات الكمبيوتر، الكتاب الأول، دار الكتاب الحديث، القاهرة، 2003، ص79.

[2] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 31، 32.

[3] – كالهاتف المحمول والبطاقات الذكية والمساعد الرقمي الشخصي وغيرها من الأجهزة التي تعتمد المعالجة الآلية للمعلومات يمكن أن تكون مصدرا للدليل الإلكتروني.

[4] – **فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص635.

الرقمية كأداة لتسهيل التنفيذ بغرض التستر عن أعين الأمن والمحققين[1]، حيث يعتقد المجرمون أن هذه البيئة منفصلة تماما عن العالم المادي، مما يجعلهم يشعرون بالأمان.

بعد الملاحظات التي تم عرضها يمكن إستنتاج أن الدليل الإلكتروني ليس على صورة واحدة وإنما له خصوصية التنوع نظرا إلى ما تتنوع به طبيعته من ضرورة توافقه مع الواقعة الإجرامية، وبطبيعة الحال فإن أي محاولة لتقسيم الدليل الإلكتروني من جهة الفقهاء، يمكن أن يكون محل جدل فقهي، وذلك سببه التطور المستمر الذي يطرأ على البيئة الرقمية التي يعيش فيها الدليل، وهو ما يجعله من الأدلة المتطورة بطبيعتها، ولاسيما أن العالم الافتراضي لا يزال في بدايته ولم يصل بعد إلى منتهاه.

ثانيا: طبيعة الدليل الإلكتروني

يعرض فيما يلي أهم المواقف الفقهية بخصوص تحديد طبيعة الأدلة الإلكترونية مقارنة بالأدلة الجزائية بصفة عامة:

الاتجاه الأول – يرى أنصار هذا الاتجاه أن الأدلة الإلكترونية ما هي إلا مرحلة متقدمة من الأدلة المادية الملموسة يمكن إدراكها بإحدى الحواس الطبيعية للإنسان إذا ما كانت على شكل مطبوعات مستخرجة من الحاسوب، باعتباره مصدر الدليل الإلكتروني، فالأدلة الإلكترونية في منظور هذا الاتجاه لا تختلف من حيث المفهوم والقيمة عن الآثار الأسلحة وبصمات الأصابع والبصمة الوراثية (DNA) وغيرها من الأدلة العلمية[2].

الاتجاه الثاني– يذهب أنصار هذا الاتجاه، إلى القول بأن الأدلة الإلكترونية نوع متميز من وسائل الإثبات ولها من المواصفات ما يؤهلها لتقوم كإضافة جديدة لأنواع الأدلة الجزائية القانونية، الفنية، القولية، والمادية. يميل هذا الاتجاه اكثر إلى الصواب لأن الأدلة الإلكترونية تتمتع بخصائص جعلتها متميزة عن غيرها من الأدلة الجزائية الأخرى سواء من حيث البيئة التي تنبعث

[1] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 32.

[2] - **عائشة بن قارة مصطفى**، مرجع سابق، ص 39.

منها أو من حيث الشخص القائم على جمعه حيث يشترط فيه على الأقل أن يكون ملما بتقنية المعلومات [1].

الفرع الثاني

أقسام الدليل الإلكتروني

نظرا لحداثة الدليل الإلكتروني والتطور السريع الطارئ عليه مما يزيد من صعوبة جمعه، نجد الفقه الجنائي لم يدرس تقسيماته دراسة متعمقة. ان أساس المقارنة بين الدليل الإلكتروني والدليل المادي، هو شكل وتقسيم الدليل الإلكتروني من حيث نسبته إلى مصدره.

أولا: تقسيمات الدليل الالكتروني

اختلفت المحاولات الفقهية في تقسيم الدليل الإلكتروني، فقسم الدليل الإلكتروني كما يلي:

- الأدلة الإلكترونية الخاصة بأجهزة الكمبيوتر وشبكاتها.
- الأدلة الإلكترونية الخاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.
- الأدلة الإلكترونية الخاصة بالشبكة العالمية للمعلومات[2].

كما وجد هناك تقسيم آخر للأدلة الإلكترونية:

- أدلة إلكترونية أعدت لتكون وسيلة إثبات وأدلة لم تعد لتكون ووسيلة إثبات، يمكن إجماله فيما يلي:

  - السجلات التي تم أنشاؤها بواسطة الجهاز تلقائيا، وتعتبر هذه السجلات من مخرجات الجهاز ولم يساهم الإنسان في إنشائها.
  - السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الجهاز، وهي تلك البيانات التي تم إدخالها ومعالجتها من خلال برنامج خاص.

---

[1] – **عائشة بن قارة مصطفى**، مرجع نفسه، ص 39.

[2] – **ممدوح عبد الحميد عبد المطلب**، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، القاهرة، 2006، ص 88. **عائشة بن قارة مصطفى**، مرجع سابق، ص41.

– الأدلة الإلكترونية التي لم تعد لتكون وسيلة إثبات فهي تلك الأدلة التي تنشأ دون إرادة الشخص بمعنى أنها أي أثر يتركه دون أن يكون راغبا في وجودها، ويسمى هذا النوع من الأدلة بالبصمة الرقمية أو الآثار المعلوماتية للرقمية وهي تتجسد في الآثار التي يتركها مستخدم النظام المعلوماتي بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال النظام المعلوماتى وشبكة الاتصالات، والواقع أن هذا النوع من الأدلة لم يعد أساسا للحفظ من طرف من صدر عنه غير أن الوسائل التقنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من نشوئها فالاتصالات التي عبر المنظومة المعلوماتية المرتبة بشبكة الاتصالات وكذا المرسلات الصادر عن الشخص أو التي يتلقاها يمكن ضبطها بواسطة تقنية خاصة بذلك.

تبدو أهمية التمييز بين هذين النوعين في كون أن النوع الأول من الأدلة الإلكترونية قد أعد سلفا كوسيلة لإثبات بعض الوقائع التي يتضمنها، لذلك فإن عادة ما يعمد إلى حفظه للاحتجاج به لاحقا وهو ما يقلل من إمكانية فقدانه كما يكون من السهل الحصول عليه، بينما النوع الثاني من الأدلة الرقمية فلكونه لم يعد أصلا ليكون أثرا لمن صدر عنه لذا فهو في الغالب ما يتضمن معلومات تفيد في الكشف عن الجريمة ومرتكبها، ويكون الحصول عليه باتباع تقنيات خاصة لا تخلو من الصعوبة والتعقيد، وهو على العكس من النوع الأول، إذ لم يعد ليحفظ مما يجعله عرضة للفقدان بسهولة[1].

ثانيا: أشكال الدليل الإلكتروني

إضافة إلى هذا التقسيمات تم تحديد أشكال الدليل الإلكتروني حسب أشكال المخرجات، إذ له عدة أشكال وصور:

أ- **الصورة الرقمية:** وهي عبارة عن تجسد الحقائق المرئية حول الجريمة، وفي العادة تقدم الصورة في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية[2]، والصورة الرقمية[3] تمثل تكنولوجيا بديلة للصورة التقليدية، يقسم الدليل الرقمي إلى دليلين هما:

---

[1] – **طارق محمد الجملي**، الدليل الرقمي في الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون، المنعقد في الفترة 28-2009/10/29، محمول من الموقع الإلكتروني التالي:
http://www.droit-dz.com/forum/threads/5952/. تم الاطلاع عليه يوم: 2016/05/14.

[2] – يتمثل هذا الشكل في عرض البيانات المعالجة أليا بواسطة الحاسب الآلي على الشاشة الخاصة به.

[3] – مخرجات ذات طبيعة ورقية يسجل فيها المعلومات على الورق ويستخدم في ذلك الطابعات.

الدليل الرقمي الأصلي وهو البنود العينية أو الحسية وكذلك المستمسكات البيانية التي تتعلق بهذه البنود عند الإمساك بها وحجزها، المحرر الإلكتروني الأصلي، فهو بيانات يدخلها المزود ويرسلها عن طريق وسيط إلكتروني فيترجمها الوسيط وفق برنامج معين ويمررها إلى المتلقي الذي يمكنه استخراجها بالاستعانة بوسيط إلكتروني أخر ويمكنه قراءتها بذات البرنامج وإظهارها على صورة الإدخال، الدليل الإلكتروني المكرر وهو استنساخ رقمي دقيق لجميع المستمسكات البيانية التي تحتويها البند العيني الأصلي المحرر الرسمي المكرر أو الصورة المأخوذة عن الدليل الرقمي فهي صورة دقيقة وطبق الأصل للمعلومات الواردة في الوثائق البيانية والمستقلة عن البنود العينية الأصلية.

ب- التسجيلات الصوتية: وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات الصوتية على الأنترنت.

ج - النصوص المكتوبة: وتشمل النصوص التي يتم كتابتها بواسطة الآلة الرقمية ومنها الرسائل عبر البريد الإلكتروني والبيانات المسجلة بأجهزة الحاسب الآلي.

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

- السجلات المحفوظة في الحاسوب وهي الوثائق المكتوبة والمحفوظة مثل البريد إلكتروني وملفات برامج معالجة الكلمات وإرسال غرف المحادثة على الأنترنت[1].

- السجلات التي تم إنشاؤها بواسطة الحاسوب وتعتبر مخرجات برامج الحاسوب لم يلمسها الإنسان.

- السجلات التي جزء منها تم حفظه بالإدخال، وجزء أخر تم إنشاؤه بواسطة الحاسوب بعد معالجتها من خلال برامج معينة[(2)]، وهي السجلات التي تجمع بين التدخل الإنساني ومعالجة الكمبيوتر، كما لو ادخل متهم بيانات معينة وطلب من الكمبيوتر أن يقوم بمعالجتها توصلا إلى نتائج يسمح بها البرنامج المستخدم، كمن يتهرب من الضرائب فيقوم بتسجيل بيانات غير صحيحة

[1] - عائشة بن قارة مصطفى، مرجع سابق ص 43.

[2] - **سعيداني نعيم**، مرجع سابق، ص 134، 136.

عن دخله وربحه طالبا من الكمبيوتر حساب الضريبة المستحقة[1]، ومن أمثلتها، أوراق العمل المالية التي تحتوي على مدخلات تم تقليمها إلى برامج أوراق لعمل مثل Excel، ومن تم تمت معالجتها بإجراء العمليات الحسابية عليها[2].

ان هذا التقسيم هو نفسه الذي أخذ به القضاء الأمريكي، فسجلات الحاسوب المقبولة استثناء أمام القضاء الأمريكي إذا كانت معدة في هيئة نصوص تتخذ أحد هذه الأشكال: سجلات الحاسوب المتوالدة، وسجلات الحاسوب المخزنة، والفرق بينهما يتوقف على ما إذا كان الشخص أو الآلة تنشئ محتويات هذه السجلات أي مصدرها، فسجلات الحاسوب المخزنة تشير إلى الوثائق التي تحتوي على كتابات شخص أو بعض الأشخاص وحدث وإن صارت في شكل إلكتروني، مثل رسائل البريد. أما سجلات الحاسوب المتوالدة، فالكمبيوتر هو الذي يصدرها، وهي تحتوي على مخرجات برامج الحاسوب التي لم تمسها الأيدي البشرية مثل سجلات الدخول على الأنترنت ومصدرها مزود خدمة الأنترنت، فهذه السجلات لا تحتوي على بيانات بشرية، فهي مجرد مخرجات كان لا بد من وجود مدخلات لها ممثلة في لوغارتمات البرمجة[3].

تجدر الإشارة إلى أن هذا التنوع في الدليل الإلكتروني يفيد بالضرورة انه ليس هناك وسيلة وحيدة للحصول عليه، وإنما تتعدد هذه الوسائل، وفي كل الأحوال يظل الدليل المستمد منه رقميا، حتى وإن اتخذ هيئة أخرى، ففي هذه الحالة وإن اعترف القانون بذلك فانه يكون مؤسسا على طابع افتراضي، ولكي يحدث تواصل بين القانون وهذا الدليل، فانه يجب اتخاذ مسلك الافتراض من حيث اعتباره دليلا أصليا[4].

---

[1] – **شيماء عبد الغني محمد عطا الله**، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص 409.

[2] – راجع كل عن: **عائشة بن قارة مصطفى**، مرجع سابق، ص 43. **عمر محمد بن يونس**، الإجراءات الجنائية عبر الأنترنت، مرجع سابق، ص 420.

[3] – **عائشة بن قارة مصطفى**، مرجع نفسه، ص 43.

[4] – **عمر محمد بن يونس**، "الدليل الرقمي"، ورقة عمل مقدمة لندوة حول قانون الإجراءات عبر الأنترنت والإعلام، جامعة الدول العربية، الفترة بين5 و8 مارس 2006، ص 12، محمول من الموقع الإلكتروني التالي: http://unpan1.un.org/intradoc/groups/public/documents/arado/unpan026347.pdf تم الاطلاع عليه يوم: 2016/09/20.

المطلب الثاني

خصائص الدليل الإلكتروني

الدليل الإلكتروني هو الدليل المأخوذ من أجهزة الرقمية، وهو يكون في شكل نبضات مغناطيسية أو كهربائية من الممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهو مكون رقمي لتقديم المعلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون.

تقوم خصائص الدليل الإلكتروني على مدى ارتباطه بالبيئة التي يحي فيها، وهي البيئة الافتراضية المتطوّرة بطبيعتها، فهي تشمل على أنواع متعددة من البيانات الرقمية التي تصلح منفردة أو مجتمعة لكي تكون دليلا للإدانة أو البراءة، وانعكس هذا على طبيعة هذا الدليل فأصبح يتصف بعدة خصائص جعلته يتميز عن الدليل التقليدي، ندرج في هاذين الفرعين أهم هذه الخصائص:

الفرع الأول

الخصائص المتعلقة بطبيعته

أولا: دليل علمي

الدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة أن القانون مسعاه العدالة أما العلم مسعاه الحقيقة، له منطق لا يجب أن يخرج عنه إذ يستبعد تعارضه مع القواعد العلمية السليمة، والدليل الإلكتروني يتميز بذات الطبيعة، حيث لا يجب أن يخرج هذا النوع من الأدلة عمّا توصل إليه العلم الرقمي وإلاّ فقد معناه[1].

إن الدليل الإلكتروني يحتاج إلى بيئته التقنية التي يتكون فيها من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات، وأدوات الحاسبات الآلية. واستخدام نظم برامجية حاسوبية، فهو يحتاج إلى بيئته التقنية

[1] – **عمر محمد أبو بكر يونس**، مرجع سابق، ص 977.

التي يتكون فيها لكونه من طبيعة تقنية المعلومات، ولأجل ذلك فإن ما ينطبق على الدليل العلمي ينطبق على الدليل الإلكتروني[1].

ثانيا: ذو طبيعة تقنية

إنّ الطبيعة التقنية للدليل تقتضى ان يكون هناك توافق بين الدليل المرصود، وبين البيئة التي يعيش فيها فلا تنتج التقنية سكينا يتم به اكتشاف القاتل، أو اعترافا مكتوبا أو مالا في جريمة الروشة، أو بصمة أصبع وإنما ما تنتجه التقنية هو نبضات رقمية تشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب على أية شاكلة يكون عليها، ومثل هذا الأمر يجعلنا نقرر انه لا وجود للدليل الإلكتروني خارج بيته التقنية وأنه لكي يكون هناك دليل إلكتروني يجب أن يكون مستوحا أو مستنبطا من البيئة الرقمية أو التقنية وهي في إطار جرائم المعلوماتية ممثلة في العلم الافتراضي وهو العالم الكامن في الحاسوب والخوادم والمضيفات والشبكات التي يتم تداول الحركة فيه عبرها.

نتيجة للطبيعة التقنية للدليل الإلكتروني فإنه اكتسب مميزات عن الدليل المادي من حيث قابليته للنسخ، بحيث يمكن استخراج نسخ من الأدلة الإلكترونية مطابقة للأصل ولها نفس القيمة العلمية، وهذه الخاصية لا تتوافر في أنواع الأدلة الأخرى مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير، بالإضافة إلى إمكانية تحديد ما إذا كان الدليل الرقمي قد العبث به أو تعديله وذلك لإمكانية مقارنته بالأصل باستخدام البرامج والتطبيقات الصحيحة[(2)].

ثالثا: ذو طبيعة رقمية ثنائية

الدليل الإلكتروني ليس على هيئة واحدة، وإنما له خصية الالتصاق بمفهوم تكنولوجيا المعلومات من حيث تكوينه، إذ يتكون من تعداد غير محدود لأرقام ثنائية موحدة في الصفر والواحد، والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي الذي تتكون منه، فالكتابة مثلا في العالم الرقمي ليس لها وجود مادي في شكل ورقي وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه، فأي شيء في العالم الافتراضي يتكون

[1] - **عائشة بن قارة مصطفي**، مرجع سابق، ص 34.

[2] – **سعيداني نعيم**، مرجع سابق، ص 131.

من الصفر والواحد وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة، وأما تكوين معطياته فإنها تختلف من حيث الحجم والموضوع[1].

الفرع الثاني

الخصائص المتعلقة بمرونته

أولا: دليل قابل للنسخ

يمكن استخراج نسخ من الأدلة الإلكترونية مطابقة للأصل ولها نفس القيمة العلمية[2] وهذه الخاصية لا تتوافر في أنواع الأدلة الأخرى التقليدية، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير عن طريق النسخ طبق الأصل من الدليل[3] بالإضافة إلى إمكانية تحديد ما إذا كان الدليل الإلكتروني قد تم العبث به أو تعديله وذلك لإمكانية مقارنته بالأصل باستخدام البرامج والتطبيقات الصحيحة.

ثانيا: دليل سهل الإخفاء

إن التخلص من الدليل الإلكتروني قد يقابله مسألة أخرى ذات علاقة بمسألة التطوير المستمر في تكنولوجيا المعلومات، وهي أن الدليل الإلكتروني نتيجة لمرونته وضعفه، فإنه يسهل فقدانه أو إتلافه بالتالي يمكن التخلص منه بشكل آخر غير الحذف أو الإلغاء[4].

ثالثا: دليل متنوع ومتطوّر

يشمل الدليل الإلكتروني كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقميا، بحيث يكون بينها وبين الجريمة رابطة من نوع خاص وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني، وتعنى هذه الخاصية أنه على الرغم من أن الدليل الإلكتروني في

---

[1] – **رشيدة بوكر**، مرجع سابق، ص311.

3– هذا ما جاء به المشرع البلجيكي في نص المادة 39 من القسم الرابع من قانون التحقيق الجنائي، حيث سمح بعرض نسخ مخزنة في نظم المعالجة الآلية للبيانات على الجهات القضائية.

-Code d'instruction criminelle Belge ,in ;
http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1808111730&table_name=loi..

[3] - **عائشة بن قارة مصطفى**، مرجع سابق ص 36.

[4] – **فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص 653.

أساسه متحد التكوين بلغة الحوسبة والرقمية إلا أنه مع ذلك يتخذ أشكالا مختلفة يمكن أن يظهر عليها، كأن يكون بيانات غير مقروءة من خلال ضبط مصدر الدليل كما هو الشأن حال المراقبة عبر الشبكات والملقمات والخوادم، وقد يكون بيانات مفهومة كما لو كان وثيقة معدة بنظام المعالجة الآلية، كما من الممكن أن يكون صورة ثابتة أو متحركة معدة بنظام التسجيل السمعي البصري[1] أو يكون مخزنا في البريد إلكتروني، وقد يكون أيضا مرتبطا بالتشفير، وهذا التنوع إنما يعد عن أتساع قاعدة الدليل الرقمي بحيث يمكنه بهذه الصور أن يشمل أنواعا متعددة من البيانات الرقمية التي تصلح منفردة أو مجتمعة لان تكون دليلا بالإدانة أو البراءة.

أما عن كون الدليل الإلكتروني دليلا متطورا فهي خاصية تكاد تكون تلقائية، نظرا لارتباطه بالطبيعة التي تتمتع بها حركة لاتصال عبر الأنترنت والعالم الافتراضي الذات لا يزالان في بداياتهما ولم يصلا بعد إلى منتاها ولن يكون من السهل احتواؤهما[2].

الدليل الإلكتروني يرصد معلومات عن الجاني ويحللها في ذات الوقت، حيث يمكنه أن يسجل تحركات الفرد، كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه، لذا فان البحث قد يجد غايته بسهولة أيسر من الدليل المادي[3].

---

[1] – **Jacques FRANCILLION**, « Les crimes informatiques et d'autre crimes dans le domaine de la technologie informatique en France », RIDP, v 64, 1er et 2eme trim, 1993, p 309.

[2] – **سعيداني نعيم**، مرجع سابق، ص 132.

[3] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 36.

الفصل الثاني

إجراءات جمع الدليل الإلكتروني

يشهد العالم في الآونة الأخيرة نوعان من الجرائم المرتكبة بواسطة نظام المعالجة الآلية، نوع من الجرائم يستخدم فيه نظام المعالجة الألية كوسيلة مساعدة لارتكاب الجريمة: مثل استخدامه في تبييض الأموال أو تهريب المخدرات، لا علاقة له بالوسط الافتراضي إلا من حيث الوسيلة، كذلك قد يستعمل نظام المعالجة الإلية للتمهيد لارتكاب الجريمة، أو لإخفاء معالمها، كالمراسلات التي يبعث بها الجاني لشريكه وتتضمن معلومات عن جريمة ينويان ارتكابها أو يطلب منه إخفاء معالم هذه الجريمة، فتلك المراسلة تصلح كدليل إثبات لهذه الجريمة حال وقوعها رغم أنها لم ترتكب ضد نظام المعالجة الآلية ولا بواسطته[1]، وجرائم الاعتداء على نظم المعالجة الآلية: هذا النوع من الجرائم هو ما يمكن تسميته بجرائم المعلوماتية بالمعنى الدقيق والتي يكون الدليل الإلكتروني فيها هو الدليل الأفضل لإثباتها.

يصلح الدليل الإلكتروني لإثبات النوعين من الجرائم، ألا ان خصائصه وأقسامه جعلت منه الأفضل لإثبات الجرائم المعلوماتية، حيث أهمية هذا النوع من الأدلة بالنسبة لهذا النوع من الجرائم تظهر عند صعوبة إثبات وقوعها.

أمام ذاتية الدليل الإلكتروني يبقى دور بعض الإجراءات التقليدية في بيئة تكنولوجيا المعلومات –كالمعاينة أو الشهادة مثلا– ضئيل مما إستوجب مجموعة أخرى من الإجراءات التي يمكنها أن تتلاءم وطبيعة هذا الدليل.

بناءا على هذا قسم الفصل إلى مبحثين، الإجراءات التقليدية لجمع الدليل الإلكتروني(المبحث الأول)، الإجراءات الحديثة لجمع الدليل الإلكتروني(المبحث الثاني).

[1] – **رشيدة بوكر**، مرجع سابق، ص 313.

المبحث الأول

الإجراءات التقليدية لجمع الدليل الإلكتروني

أن الحق موضوع التقاضي يتجرد من كل قيمة إذا لم يقم الدليل على الواقعة التي يستند إليها، فالدليل هو عصب الواقعة الذي يستنتج باتباع وسائل الإثبات المختلفة.

يقصد بالإثبات، القواعد المتعلقة بالبحث عن الأدلة لإظهار الحقيقة وإقامتها أمام القضاء وتقديرها من جانبه فالأدلة تؤكد وقوع الجريمة، وتحقق حالة اليقين لدى القضاء لإدانة المتهم، أو ترجح حالة الشك لديه فيقضي بالبراءة.

ان الدليل الإلكتروني مثل باقي الأدلة يحتاج لاستخلاصه اتباع إجراءات الإثبات، يقسم هذا المبحث إلى مطلبين، الأول يتضمن إجراءات التحقيق المادية، والثاني إجراءات التحقيق الشخصية.

المطلب الأول

الإجراءات المادية

يتناول هذا المطلب ثلاث إجراءات ذات طبيعة مادية تتم بنتائج مادية ملموسة تتبع لاستنتاج الدليل الإلكتروني، وهي التي سيتم دراستها في الفروع التالية:

الفرع الأول

المعاينة

تعتبر المعاينة[1] إجراء من إجراءات التحقيق تتطلب سرعة الانتقال إلى محل الواقعة الإجرامية لمباشرتها وذلك لإثبات حالته وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى

[1] – عرفت المعاينة بأنها "الإجراء الذي يتضمن وصف مكان الحادث بما فيه من أشياء وأشخاص، والفحص الدقيق لكافة المحتويات بهدف كشف مخلفات وآثار الجاني بالمكان، والتي تشير إلى شخصيته وشركائه وما قد يفيد في إثبات ارتكاب الجريمة وتوضيح قدرا من الاستنتاجات المنطقية تشكل في حد ذاتها الأساس الذي تقام عليه عملية التحقيق والبحث التالية » . **محمد بن نصير محمد السرحاني**، مهارات التحقيق الجزائي الفني في الجرائم الحاسوب والأنترنت، رسالة الماجستير في علوم الشرطة، جامعة نايف للعلوم الأمنية، الرياض، 2004، ص 100.

فاعلها [1].

أولا: دور المعاينة في استنتاج الدليل الإلكتروني

تعد المعاينة ذات أهمية بالغة في الجرائم التقليدية حيث تساهم في تصوير كيفية وقوع الجريمة وظروف ملابسات ارتكابها كما توفر الأدلة المادية التي يمكن تجميعها، إلا أن دورها يتضاءل في الكشف عن الأدلة الإلكترونية وضبطها[2]، ويرجع ذلك للأسباب التالية:

- الجرائم التي تقع على الشبكات أو بواسطتها قلّما ما يترك مرتكبها آثار مادية وراءه.
- الأعداد الكبيرة من الأشخاص الذين قد يترددون على مسرح الجريمة خلال المدة الزمنية –التي غالبا ما تكون طويلة نسبيا – ما بين اقتراف الجريمة المعلوماتية والكشف عنها، الأمر الذي يتيح فرصة لحدوث تغيير أو تلفيق أو عبث بآثار الجريمة أو زوال بعضها وهو ما يلقي ظلالا من الشك على الشك وعلى الدليل المستقى من المعاينة[3].
- إمكانية تلاعب الجاني في البيانات عن بعد أو محوها.

أمام هذه الأسباب قررت جزاءات جنائية –المشرع الجزائري في المادة 43 من قانون الإجراءات الجزائية الجزائري، والمشرع الفرنسي في المادة 55 من قانون الإجراءات الجزائية الفرنسي[4]– على

---

[1] –أنظر عن هذا التعريف:

– المادة 79 من الأمر رقم 66–155 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966، الذي يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية عدد 48 بتاريخ 11 جوان 1966 المعدل والمتمم.

–Art 77-1 **du** Code de procédure pénale Français Modifié par Loi n°99-515 du 23 juin 1999 renforçant l'efficacité de la procédure pénale - art. 12, JORF 24 juin 1999.

Art77-1-1 Code de procédure pénale Modifié par Loi n°2016- du 3 juin 2016731renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure penale art. 58 **,**in ;

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032627231.

[2] – **علي احمد البسيوني**، "الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية"، مجلة الفكر الشرطي عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، دولة الإمارات العربية المتحدة، المجلد الحادي والعشرون، العدد 81، ص 51.

[3] - **عائشة بن قارة مصطفى**، مرجع سابق، ص49.

[4] – Article 55 du Code de procédure Pénale Français Modifié par Loi n°92-1336 du 16 décembre 1992 - art. 11, JORF 23 décembre 1992 en vigueur le 1er mars 1994 dispose que :" Dans les lieux où un crime a été commis, il est interdit, sous peine de l'amende prévue pour les contraventions de la quatrième classe, à toute personne non habilitée, de modifier avant les premières opérations de l'enquête judiciaire l'état des lieux et d'y effectuer des prélèvements quelconques".

كل من يقوم بإجراء أي تغيير أو تعديل في المكان الذي وقعت فيه الجريمة قبل قيام سلطة التحقيق بإجراء المعاينة، وان كانت أحكام هذه النصوص تنصرف إلى أغلب الجرائم التقليدية، إلاّ أنه يمكن تطبيقها عند معاينة مكوّنات الحاسوب ذات الطابع المادي كأشرطة الحاسوب، والأقراص وغيرها.

ثانيا: مسرح المعاينة

في كل الأحوال عند تلقي بلاغ عن وقوع إحدى الجرائم المعلوماتية وبعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته، ومسرح الجريمة هنا يختلف عن مسرح الجريمة التقليدية كالقتل أو السرقة، فعند الشروع في معاينة مسرح الجريمة المعلوماتية ينبغي التعامل معه على أنه مسرحان:

•المسرح التقليدي: هو مسرح بعيد عن المجال الإفتراضي، وقعت فيه الجريمة والذي يتم معاينته من أجل إيجاد ما قد يمكن أن يخلفه الجاني وراءه من أثار عديدة كالبصمات، أو متعلقات شخصية أو أدوات مادية إستعملت في إرتكاب الجريمة.

ربما كان الأمر الأكثر أهمية للمحقق فور وصوله إلى مسرح الجريمة هو السيطرة الكاملة على المنشآت والأشخاص في كافة حدود مسرح الجريمة والمناطق المحيطة به والتي من الممكن أن تطالها المعاينة، ونتيجة لاختلاف مسرح الجريمة المعلوماتية عن غيره من الجرائم– لكون هذا النوع من الجرائم يتميز بوجود الأدلة الإلكترونية ذات الطبيعة غير المرئية– ينبغي تعامل خاص معه، ويكون ذلك من خلال اتباع عدة قواعد فنية[1].

---

[1]– أبرزها ما يلي:

– حماية وتأمين مسرح الجريمة، بتوفير معلومات مسبقة عن مكان الجريمة، نوع وعدد الأجهزة المتوقع مداهمتها وشبكات الاتصال الخاصة بها.

– وإعداد خطة للهجوم علي ذلك المكان وتكون موضحة بالرسومات.

– إعداد اعوان متخصصين للتفتيش يرفقون دائما بالإذن بالتفتيش، لأن اغلب الجرائم المعلوماتية تكون داخل أماكن لها خصوصيتها.

– إيجاد الأدلة، ومعالجتها.

– اخذ كل الأجهزة الضرورية لتسهيل التفتيش. **محمد الأمين البشري**، "التحقيق في الجرائم الحاسب الآلي"، المجلة العربية للدراسات الأمنية والتدريب، تصدر عن جامعة نايف العربية للعلوم الأمنية، الرياض، العدد الثلاثون، نوفمبر 2000، ص 357.

المسرح افتراضي: هو البيانات الرقمية التي تتواجد وتنتقل داخل بيئة الحاسوب وشبكاته، في ذاكرته وفي الأقراص الصلبة الموجودة بداخله[1]، والتعامل مع الأدلة الموجودة في هذا المسرح يجب ألا يتم إلا على يد خبير متخصص في ذلك.

أن القاعدة العامة التي يوصي بها الخبراء عند جمع الأدلة الإلكترونية– وعلى الرغم من أن لكل قضية ظروفها الخاصة– هي جمع قدر ما يستطاع من الأدلة، فمجرد مغادرة مسرح الجريمة يصبح من الصعب العثور على أية أدلة في حال قرر المحقق العودة إليه مرة أخرى.

الفرع الثاني

التفتيش

هناك الكثير من التعريفات الاصطلاحية للتفتيش، مجملها أنه إجراء من إجراءات التحقيق الابتدائي التي تهدف إلى البحث عن الأدلة المادية سواء لجناية أو جنحة تتحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم تبعا لإجراءات قانونية محددة [2].

محل التفتيش قد يكون مسكنا أو شخصا، متعلقا بالمتهم أو غير المتهم في كل الأحوال التفتيش جائز بالشروط القانونية المقررة[3].

– يقصد بالشخص كمحل لتفتيش الوسائل الإلكترونية، قد يكون من مستغلي أو مستخدمي الأجهزة الإلكترونية أو خبراء البرامج، سواء أكانت برامج نظام أو برامج تطبيقات، أو من أي أشخاص آخرين يكون بحوزتهم أجهزة أو معدات معلوماتية أو أجهزة حاسب آلي محمولة أو هواتف متصلة بجهاز المودم أو مستندات، وفي جميع الأحوال يقصد بالشخص كمحل قابل للتفتيش كل ما يتعلق بكيانه المادي وما يتصل به.

---

[1] - **عائشة بن قارة مصطفى**، مرجع سابق، ص51.

[2] – راجع كل عن: **عوض محمد عوض**، قانون الإجراءات الجنائي، الجزء الأول، مؤسسة الثقافة الجامعية، الإسكندرية، 1989، ص 475. **أحمد فتحي سرور**، الوسيط في قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1981، ص 544. **أحمد شوقي الشلقاني**، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الجزائر، 1999، ص 40.

[3] – **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، القاهرة، 2005، ص 377.

– يقصد بالمنازل وما في حكمها لتفتيش الوسائل الإلكترونية كافة محال الإقامة أو المأوى والملحقات المخصصة لمنافعها والتي يستغلها الشخص سواء بصفة دائمة أو مؤقتة وسواء كانت مكونات مادية أو منطقية أو شبكات اتصال خاص، وعملية التفتيش هنا تخضع لذات شروط وقواعد إجراءات تفتيش المنازل[1].

أولا: قابلية تفتيش نظام الوسائل الإكترونية

أن محل التفتيش في الجرائم المعلوماتية ينصب على المكونات الآتية:

– مكونات مادية وهي القطع الصلبة الملموسة

– مكونات منطقية وهي البرمجيات.

– شبكات الاتصال البعدية السلكية واللاسلكية [2].

أ– صلاحية تفتيش الكيانات المادية للوسائل الإلكترونية:

لا مانع قانوني من تفتيش الكيان المادي للأجهزة الإلكترونية كالمكونات المادية للحاسوب وملحقاته ومعداته، لأنه يرد على أشياء مادية لا خلاف حول خضوعها للتفتيش طبقا لقواعد الإجراءات الجزائية الخاصة بهذا الإجراء[3]، إلا أن حكم هذه المكونات يتوقف على طبيعة المكان الموجودة فيه، سواء في الأماكن العامة أو الأماكن الخاصة، إذ أن لصفة المكان أهمية خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه، فلا يجوز تفتيشها إلاّ في الحالات التي يجوز فيها تفتيش مسكنه، وبنفس الضمانات المقررة قانونا في أغلب التشريعات الجزائية.

جاء المشرع الجزائري بمجموعة من الإستثناءات بموجب القانون رقم 06– 22 السالف الذكر، حيث استثنى تطبيق الضمانات الواردة في المادة 64 من قانون الإجراءات الجزائية على طائفة من الجرائم المذكورة في الفقرة الثالثة من المادة 47 ومن بينها الجرائم الماسة بأنظمة

[1] – **حسن أحمد الشهري**، مرجع سابق، ص 262.

[2] – **محمد فهمي**، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، مطابع المكتب المصري الحديث، القاهرة، 1991، ص 11.

[3]– ورد في المادتين 44 و64 قانون إجراءات جزائية جزائري أن التفتيش يرد على الأشياء، وهي كلمة يقصد من معناها المكونات المادية.

المعالجة الآلية للمعطيات، حيث أجاز إجراء التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص.

إن المشرع الجزائري غلب في هذه الحالة مصلحة المجتمع في تحقيق العدالة على مصلحة الأفراد في حقهم على الحفاظ على حرمتهم الخاصة لاسيما حرمة المسكن باعتبار مستودع أسرارهم، فظاهر النص يشير إلى أن الاعتداء مشروع على حرمة الحياة الخاصة للشخص، إلا أن ما يبرره ويقل من خطورته الطبيعة الخاصة للجريمة المعلوماتية، فهي جريمة قابلة للمحو والتعديل في اقل من ثانية، ومرتكبها ذو دراية بالأمور التقنية، وقد تكون الصعوبة أكثر إذا كان هذا الدليل الإلكتروني الوحيد في الدعوى الجزائية[1].

أما بالنسبة للاماكن العامة، فإذا وجد الشخص في هذه الأماكن وهو يحمل مكونات الحاسب ومكوناته أو ما يشابهه فان تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال.

ب- صلاحية تفتيش الكيانات المعنوية للوسائل الإلكترونية:

إذا كان الأمر قد انتهى بصلاحية المكونات المادية للنظم المعلوماتية كمحل يرد عليه التفتيش، فإن امتداد ذلك إلى مكوناته غير المادية مسألة معقدة لأن تكون موضوعا للتفتيش تمهيدا لضبط الأدلة.

أن التفتيش وسيلة للبحث عن الأدلة المادية المتعلقة بالجريمة لتقديمها إلى المحكمة المختصة كدليل إدانة، لذلك يثور الشك والتساؤل حول إمكانية اعتبار البحث عن أدلة الإلكترونية في نطاق نظم الحاسوب نوعا من التفتيش باعتبار أن البيانات الإلكترونية أو البرامج في حد ذاتها ليس لها مظهر مادي محسوس في المحيط الخارجي ويستشعر الفقه صعوبة المسألة نظرا لغياب الطبيعة المادية للمعلومات [(2)]، سلك الفقه بهذا الشأن مسارين رئيسين:

[1] - عائشة بن قارة مصطفى، مرجع سابق، ص54.

[2] – **عبد العظيم وزير**، شرح قانون العقوبات القسم الخاص جرائم الاعتداء على الأموال، مرجع سابق، ص 40.

المسار الأول: يعتمد في التفسير على الربط بين النصوص الإجرائية التي أوردت عبارة "أي شيء" والتي يقصد بها المادة وبين العلوم الطبيعية ومفهومها في البيانات المنطقية أو البرامج[1]، فبرامج الحاسوب يمكن أن تنطبق عليها خصائص وسمات المادة، وبالتالي تدخل في نطاق الأشياء المادية ويستوي في ذلك أن تكون برامج نظام أو برامج تطبيقات[2]، مستندين في ذلك إلى أن المادة هي كل ما يشغل حيزا ماديا في فراغ معين، وأن هذا الحيز يمكن قياسه والتحكم فيه وبناء عليه فإن الكيان المنطقي للحاسوب أو البرنامج يشغل حيزا ماديا في ذاكرة الحاسوب ويمكن قياسه بمقياس معين هو البايت (Byte)، وهكذا تقاس سعة أو حجم الذاكرة الداخلية للحاسوب بعدد الحروف التي يمكن خزنها فيها[3] .

أخذت بذلك المادة 251 من القانون الإجراءات الجزائية اليوناني[4] تخول سلطات التحقيق إمكانية القيام بأي شيء ضروري لجمع وحماية الدليل، ويفسر الفقه الجنائي عبارة أي شيء، بأنها تمتد لتشمل ضبط البيانات المخزنة أو تلك التي تمت معالجتها إلكترونيا، لذلك فان ضبط البيانات المخزنة في الذاكرة الداخلية للحاسب الآلي لا تشكل أية مشكلة في القانون اليوناني.

المسار الثاني: عدم إمكانية انسجام وتطابق أحكام التفتيش في القانون الجزائي الإجرائي مع ما قد يتطلبه كشف الحقيقة في الجرائم المعلوماتية من بحث وتنقيب عن الأدلة في برامج الحاسوب وبياناته[5].

---

[1] – **أشرف توفيق شمس الدين**، الحماية الجنائية للمستند الإلكتروني دراسة مقارنة، دار النهضة العربية، القاهرة، 2006، ص 101. **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص 379.

[2]– Loi Canadienne concernant le droit criminel, L.R.C ,1985,ch.c-46, in ;law-loi.justice.g.c.ca/pdf/c-46.pdf.

[3] – مأخوذ عن: **هلالي عبد اللاه أحمد**، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، دار النهضة العربية، القاهرة،2006، ص 75.

[4] – **Code of penal procedure Greece**, in ;
https://www.unodc.org/res/cld/document/grc/penal_code_excerpts_html/Greece_Criminal_Code_Excerpts.pdf

[5] – مأخوذ عن: **علي حسن محمد الطوالبة**، التفتيش الجنائي على نظم الحاسوب والأنترنت، عالم الكتب الحديثة، القاهرة، 2004، ص 146.

يقترح هذا المسار، إزاء النقص التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش إمكانية البحث والضبط المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي، لتصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هو البحث عن الأدلة المادية وأية مادة معالجة بواسطة الحاسب الآلي[1].

لا تعد المعلومات الإلكترونية الممغنطة في القانون الفرنسي من قبيل الأشياء المحسوسة، وبالتالي لا تعتبر شيئا ماديا بالمعني الشائع، ولمواكبة هذه التغيرات قام المشرع الفرنسي بتعديل نصوص التفتيش، فبعدما كانت المادة 94 من قانون الإجراءات الجزائية الفرنسي[2] تجيز التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء مادية تكون مفيدة لإظهار الحقيقة، تمت إضافة عبارة "المعطيات المعلوماتية" مباشرة بعد كلمة الأشياء، وبهذا المشرع الفرنسي سد الفراغ القانوني.

أن المشرع الجزائري جرم أفعال المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم (04-15) [3] ويتضح موقف المشرع الجزائري من خلال القانون09-04 السالف الذكر، حينما أجاز صراحة تفتيش المنظومات المعلوماتية، وذلك بموجب المادة 05 منه التي نصت على أنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين معلوماتية.

---

[1] – صرحت اتفاقية بودابست سالفة الذكر، في هذا الصدد بحق الدول الأعضاء في تفتيش أجهزة الكمبيوتر في إطار الإجراءات الجزائية، وذلك من خلال المادة 19 من القسم الرابع، حيث نصت على أن لكل طرف من حقها أن تسن من القوانين ما هو ضروري لتمكين السلطات المختصة بالتفتيش أو الدخول إلى:

– نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة به.

– الوسائط التي يتم تحزين معلومات الكمبيوتر بها ما دامت مخزنة في إقليمها.

[2] –Art 94 du Code de procédure pénale Français, in ;
https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=0C44325B43422F8B25815066DDC94
Voir aussi : Art 56 du Code de procédure pénale Français modifié par Loi n 2016-731 du 3 juin 2016, renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, in ;
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032627231.

[3] قانون رقم 04-15 المؤرخ في27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية عدد 71، بتاريخ 10 نوفمبر 2004.

يجدر الإشارة هنا إلى المادة 10من القانون 06-22 السالف الذكر، التي تجير التفتيش في 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، إذا تعلق الأمر بجرائم المخدرات والجرائم المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

في هذا الصدد يمكن أن يطرح التساؤل حول الحالة التي يمكن أن يكون فيها مالك الحاسوب أو الملفات قد قام بتشفيرها، فإن مجرد التفتيش الروتيني في هذه الحالة لا يعد كافيا، إذ لا يرتبط الأمر هنا بمجرد القيام بعمليات التفتيش الإداري في داخل الحاسوب، وإنما يلزم هنا أن يتضمن الدخول إلى معترك التشفير والقيام بفكه كي يمكن معرفة محتوى الملف المشفر، ويعد مثل هذا الأمر من أقوى اهتمامات الجهات القائمة على تنفيذ القانون في العالم المعاصر[1]، فهذا الأمر يستلزم الاعتراف للحاسوب بالخصوصية تجريدا له من التصاقه بالمكان الموضوع فيه.

ج- تفتيش شبكات الإتصال البعدية السلكية واللاسلكية:

وضعت التكنولوجيا الحديثة تحديات كبيرة أمام أعمال التفتيش خاصة بعد إنتشار إستعمال الشبكة المعلوماتية في كل أرجاء العالم والتي سهلت من نقل الأدلة الإلكترونية بين عدة أماكن، لكن قد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد آخر، فهل يمكن تفتيش الأنظمة المتصلة بالنظام المأذون بتفتيشه إذا تواجدت في دوائر اختصاص مختلفة أو حتى خارج البلاد؟

ان الحاسوب أو النهاية الطرفية التي يمكن أن ترتكب عليها أو بواسطتها الجريمة المعلوماتية تخضع للقانون الإجرائي الخاص بتلك المنطقة[2].

---

[1] – **فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص 629.

[2] – **علي حسن محمد الطوالبة**، التفتيش الجنائي على نظم الحاسوب والأنترنت، مرجع سابق، ص 42.

جاء في المادة الأولى من المرسوم تنفيذي رقم 06- 348 مؤرّخ في 12 رمضان عام 1427 الموافق 5 أكتوبر سنة 2006 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية للجمهورية الجزائرية عدد 63 بتاريخ 08 أكتوبر 2006، على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. كذلك، نظم المشرع الجزائري في القانون رقم 09-04 سالف الذكر، أحكاما جديدة خاصة بالاختصاص في مجال بالجريمة المعلوماتية تتماشى والتطور الذي لحق الجريمة، ففي المادة 15 منه نص على أنه زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا، وتستهدف مؤسسات الدولة الجزائرية والدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

إذا كانت بعض منظمات الضبط القضائي العالمية مثل المباحث الفيدرالية الأمريكية وغيرها استطاعت التوصل إلى برمجيات يمكنها القيام بإجراء التفتيش عن بعد[1]، فإن تطبيق هذا الموضوع بالنسبة للدول الأخرى يجد صعوبات كبيرة، لاسيما وإن اتباع مثل هذا المنهج يعم الفوضى ويضفي عدم المشروعية لكونه لا يستند إلى مبرر قانوني في الدول الأخرى عرضت للبحث في حيث قد يتم انتهاك حواسب وخوادم دول من قبل دول أخرى.

إزاء الإمكانيات القائمة في التفتيش عن بعد فإن الأمر لا يخلو من ضرورة التوصل إلى اتفاق دولي في هذا الإطار، بحيث يسمح في هذا الشأن بإقرار التفتيش عن بعد في ظل المشروعية الدولية ذاتها، وإقرار المجتمع الدولي لمثل هذا الإجراء يجعل منه أمرا مشروعا إذا تم في الحدود المتفق عليها.

للإجابة عن التساؤل السالف وجب التفرقة بينما يلي:

---

[1]- وهذا ما أكد عليه:

Loi française n° 2011-267, du 14 Mars 2011, dire d'orientation de programmation pour la performance de la sécurité intérieure L'OPSI 2, à légalité la hacking au détour des disposition de l'article 706-102-1 du code de procédure pénale.

La troisième section de XVIII^{ème} congrès international de droit pénal, Istanbul du 20 au 27 Septembre 2009, in ; www.uterchtlawreview.org/article/abstract/10.18352/ulr.105/

- **تفتيش أنظمة متصلة بالنظام المأذون بتفتيشه المتواجد في مكان آخر داخل الدولة:** وجدت بعض التشريعات الإجرائية المقارنة حلا لهذه المشكلة وذلك من خلال نصها على جواز تفتيش نظم المعلومات المتصلة بالحاسوب الذي يجرى تفتيشه، وتسجيل كل البيانات اللازمة كأدلة إثبات لإدانة المتهم أمام المحكمة. ومن بين هذه التشريعات، التشريع الألماني الذي يجيز التفتيش في هذه الحالة إلى سجلات البيانات التي تكون في موقع آخر استنادا إلى المقتضيات 110 من قانون الإجراءات الجزائية الألماني[1].

كذلك المشرع البلجيكي في المادة 88 مكرر من قانون التحقيق الجنايات البلجيكي السالف الذكر، التي تنص على: « إذا أمر قاض التحقيق بالتفتيش في نظام المعلوماتي أو في جزء منه فإن البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي »، والمشرع الفرنسي قد حسم هذه المسألة، فأجاز لرجال الضبط القضائي الأطلاع على البيانات المخزنة في النظام المذكور أو أي نظام معلوماتي أخر ما دامت هذه البيانات متصلة في شبكة واحدة مع النظام الرئيسي أو يتم الدخول إليها أو تكون متاحة ابتداء من النظام الرئيسي.

سار المشرع الجزائري على نهج التشريعات المقارنة فأجاز بموجب نص المادة 05 الفقرة الثانية من القانون رقم 09-04 في حالة تفتيش منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها إذا كانت هناك أسباب تدعو للاعتقاد 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.

إنا إمتداد التفتيش إلى الأجهزة المرتبطة به يظهر لنا بصورة واضحة جدا قصور الإجراءات التقليدية لجمع الدليل الإلكتروني،فلا تكمن الأهمية في تغيير المكان إلى مكان الجهاز الثاني، بل إن ذلك يتم باستعمال وسائل تقنية حديثة "برامج الدخول"، وهنا يبقى السؤال مطروحا ألا يعد استعمال هذه البرامج اعتداء على حرمة الحياة الخاصة للأفراد، خاصة وأن الأجهزة الأخرى تنتمي إلى أشخاص غير المتهم؟

[1] -§110, Strafprozebordnung(stPO), in ; www.gesetze-im-internet.de/stpo/stPO.pdf.

- **تفتيش أنظمة متصلة بالنظام المأذون بتفتيشه الموجود في مكان آخر خارج الدولة:** يفترض أن يقوم مرتكب الجريمة المعلوماتية بتخزين بياناته في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكات الاتصال بهدف عرقلة سلطات التحقيق في جمع الأدلة، فمن المشاكل الحقيقية التي تواجه جهات التحقيق في جمع الأدلة، حالة تطلب امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة، ودخوله في المجال الجغرافي لدولة أخرى، وهو ما يسمى بالتفتيش العابر للحدود، وقد يتعذر القيام به بسبب تمسك كل دولة بسيادتها[1].

ان امتداد التفتيش إلى نظم الحاسوب الواقعة في إقليم بلد أجنبي ينبغي مراعاة العديد من الضمانات التي يكون متفق عليها سلفا عن طريق اتفاقيات ومعاهدات في هذا المجال، وهذا ما يؤكد أهمية التعاون الدولي في مكافحة الجرائم المعلوماتية.

أجاز المجلس الأوروبي إمتداد تفتيش الكمبيوتر إلى الشبكة المتصل بها، ولو كانت تلك الشبكة تقع خارج إقليم الدولة، في نص المادة 1 من التوصية رقم 13 لسنة 1995[2] المتعلقة بالمشكلات القانونية لقانون الإجراءات الجزائية المتصلة بتقنية المعلومات على أنه يمكن أن يمتد نطاق تفتيش الكمبيوتر إلى النظام المتواجد في الخارج، إذا كان من الضروري اتخاذ إجراءات عاجلة في هذا الشأن، ويتعين أن يوجد أساس قانوني لامتداد مجال هذا النوع من التفتيش، حتى لا يشكل ذلك الأجراء مخالفة لسيادة دولة أجنبية، فإنه من الضروري الحصول على موافقة الدولة التي يمتد التفتيش إلى نظام يتواجد على إقليمها.

أما المادة 32 من اتفاقية بودابست عام 2001 تجيز تفتيش وضبط أجهزة أو شبكات موجودة خارج إقليم الدولة مصدرة الإذن وبدون إذن الدولة الثانية التي تتواجد فيها الأجهزة وذلك إذا كانت البيانات المراد تفتيشها مباحة للجمهور أو أن تكون الدولة مصدرة الإذن حائزة على رضا صاحب هذه البيانات.

أجاز المشرع الفرنسي تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج الإقليم الوطني وهو ما ورد في المادة 57 – 1 الفقرة الثانية من قانون الإجراءات الجزائية الفرنسي المضافة

---

[1] −Myriam QUENER, op.cit, p 2.

[2] - Conseil de l'Europe, recommandation n° R (95) 13 du comité des ministres aux états membre , cité précédement,p2.

بموجب المادة 2/17 من القانون رقم 239-2003 « إذا تبين مسبقا أن هذه المعطيات المخزنة في نظام معلوماتي موجود خارج الإقليم الوطني وأنه يمكن الدخول إليها وأنها متاحة انطلاقا من النظام الرئيسي فإنه يمكن الحصول عليها من طرف ضباط الشرطة القضائية مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية ».

أخذ المشرع الجزائري المسار نفسه مثل المشرع الفرنسي حيث أجاز هو كذلك تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة، وهذا ما نصت عليه المادة 05 فقرة 3 من القانون رقم 09-04 « ... إذا تبين مسبقا بأن المعطيات البحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل ».

ثانيا: ضوابط التفتيش في البيئة الإلكترونية

يعتبر التفتيش من إجراءات التحقيق الابتدائي الخطيرة التي تمس الحرية، فكان لا بدّ أن يتم وضع قيود وضوابط لتنظيم التفتيش لكي يضمن عدم التجاوز على حرية الأشخاص وحرمة منازلهم إلا في إطار حاجة التحقيق، تضمنت معظم التشريعات الإجرائية المقارنة ضوابط معينة يجب إتباعها عند التعرض للحريات الشخصية بإجراء من الإجراءات الماسة بالحرية كالتفتيش وهدف ذلك هو تحقيق الموازنة بين مصلحة المجتمع في عقاب المجرم وبين حقوق الأفراد وحرياتهم.

تنقسم الضوابط العامة للتفتيش إلى نوعين، ضوابط موضوعية وشكلية:

أ- الضوابط الموضوعية للتفتيش نظم الحاسوب:

يقصد بهذه الضوابط بصفة عامة، الشروط الضرورية والتي يجب أن تكون متوفرة قبل القيام بإجراء التفتيش، وهي:

1. وجود سبب للتفتيش في البيئة الإلكترونية:

سبب التفتيش في الجرائم المعلوماتية هو السعي نحو الحصول على دليل إلكتروني في تحقيق قائم من أجل الوصول إلى حقيقة الحدث ،على النحو التالي:

2. وقوع الجريمة المعلوماتية بالفعل سواء كانت جناية أو جنحة:

أن التفتيش الذي يقع من أجل فعل لا يشكل جريمة يعتبر باطلا، بالإضافة إلى أن تكون هذه الجريمة قد وقعت فعلا فلا يجوز القيام بهذا الإجراء لضبط أدلة في جريمة مستقبلية ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل، إلا أنه بالرجوع إلى نص المادتان 04 و05 من القانون رقم 09-04 يتبين أن المشرع قد أجاز إمكانية اللجوء إلى إجراء تفتيش النظام المعلوماتي إما للوقاية من حدوث جرائم أو في حالة توفر معلومات عن احتمال وقوع جرائم معينة.

3. ضرورة الاشتباه في شخص معين أو اتهامه بارتكاب الجريمة المعلوماتية أو المشاركة فيها:

لا يكفي لقيام سبب التفتيش وقوع جريمة معلوماتية، بل لا بد أن يكون هناك اتهام موجه ضد شخص معين أو أن تتوافر دلائل كافية تدعو للاعتقاد بارتكاب للجريمة حتى يمكن انتهاك حق الخصوصية لديه وتفتيش حاسوبه الشخصي وبرامجه الخاصة ويمكن الاستدلال على ذلك بما نصت عليه المادة 46 قانون إجراءات جزائية الجزائري، ومن الدلائل المستمدة من الواقع والقرائن التي تنبئ عن ارتكاب الشخص لجريمة معلوماتية وترجح إمكانية نسبتها له وفق السياق العقلي والمنطقي أن يتم تحديد هوية الحاسوب (IP) الذي تم ارتكاب الجريمة بواسطته، وكان ذلك الحاسوب يخص شخصا بعينه، وهو الشرط ذاته المتطلب في حال التفتيش بصدد جريمة تقليدية، ذلك أنه لا يمكن تفتيش شخص أو مسكن ما لم تكن هناك دلائل على ارتكابه إحدى الجرائم بوصفه فاعلا أو شريكا.

4. توافر إمارات قوية على وجود معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم أو غيره:

لا بد أن يكون لدى المحقق حتى يؤذن له بإجراء التفتيش ما يكفي من الإمارات والأسباب على وجود مستندات إلكترونية –يحتمل أن تكشف لن الحقيقة– عند أو في مسكن المتهم أو غيره.

5. محل التفتيش: يقصد بمحل التفتيش ذلك المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره[1]، فان محل التفتيش هي كل مكونات الحاسوب سواء كانت مادية أو معنوية، وكذلك شبكات الاتصال الخاصة به، كما سبق بيانه.

[1] – **قدري عبد الفتاح الشهاوي**، ضوابط التفتيش في التشريع المصري والمقارن، منشاة المعارف، الإسكندرية، 2005، ص 63.

حكم تفتيش هذه المكونات يتوقف على طبيعة المكان الموجودة فيه، فيما إذا كان من الأماكن العامة أم من الأماكن الخاصة، وتكمن أهمية التفرقة هنا في أن هذه الكيانات إذا وجدت في الأماكن الخاصة يكون لها حكم تفتيش المساكن بنفس الضمانات المقررة قانونا لاسيما اشتراط الإذن بالتفتيش من السلطات القضائية المختصة وهو ما نصت عليه المادة 44 من قانون الإجراءات الجزائية أنه لا يجوز لضباط الشرطة القضائية الدخول إلى المساكن وإجراء التفتيش إلا بإذن مكتوب من وكيل الجمهورية أو من قاضي التحقيق، وهذه الضمانة خاصة بجميع الجرائم بما فيها الجرائم المعلوماتية، أما التفتيش الواقع على مكونات الحاسوب الموجودة في الأماكن العامة فإن أغلب التشريعات تجيز لرجال الضبطية دخول المحال العامة المفتوحة للجمهور كمقاهي الأنترنت من أجل مراقبتها والتأكد من احترامها للأخلاق والآداب العامة بكل سهولة دون حاجة لإذن بالتفتيش.

سبق وأن أشير إلى مدى قابلية المكونات المادية والمعنوية للحاسوب وشبكات الاتصال الخاصة به للتفتيش.

6. السلطة المختصة بالتفتيش:

إن التفتيش إجراء من إجراءات التحقيق التي تمس بالحرية الشخصية للأفراد، حرصت التشريعات الجزائية على إسنادها لجهة قضائية تكمل تلك الحريات والحقوق وتضمنها.

ذهبت القوانين في الجزائر وفرنسا إلى الأخذ بنظام الفصل بين سلطتي الاتهام والتحقيق، حيث عهدت هذه الأخيرة لقاضي التحقيق[1] أما الأولى فعهدت للنيابة العامة[2].

7. الإذن بالتفتيش:

يجب أن يتضمن إذن التفتيش من أصدره ووظيفته وتاريخ وساعة صدوره واسم وأسماء

---

[1] – قام المشرع الفرنسي بتعديل قانون الإجراءات الجزائية بموجب

Loi n° 2007-291 du 5 mars 2007 tendant à renforcer l'équilibre de la procédure pénale, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000271253&dateTexte.

حيث جاء في نص المادة 2 منه :

collège d'instruction dans les articles 80-1, 80-1-1 , 113-8, 116,137-1,137-2,138,139,140,141-1,142,144-1,145,146,147,148,148-1-1,175,175-1,175-2,176,177,179,180,181,182,184,188,197,496,495… du code du procédure pénale , les mots : « juge d'instruction sont remplacés par les mots : collège de l'instruction ».

[2] – المواد 44 و45 من قانون الإجراءات الجزائية الجزائري، سالف الذكر

المقصودين بالتفتيش وأن يحدد له فترة معقولة ويمكن تجديدها عند انقضائها بغير تنفيذ.

يصدر الإذن بتفتيش مسكن المتهم وينصرف هذا الإذن إلى كل ما يتواجد في المسكن، ومن ثم هل يجوز بمقتضى هذا الإذن لضباط الشرطة القضائية الولوج إلى البيئة الرقمية والتغلغل في المنظومة المعلوماتية للبحث عن أدلة إثبات التي يمكن أن تكون محل الضبط؟

في هذه الحالة يجب أن يحدد في إذن التفتيش المكان المراد تفتيشه والشخص أو الأشياء المراد تفتيشها وضبطها (أجهزة الحاسوب، صور جنسية إلكترونية خاصة بالأطفال، مصنفات إلكترونية مقلدة...)، الهدف من هذا التحديد في إذن التفتيش هو تجنب التفتيش الاستكشافي، إلا أن هناك صعوبة في احترام هذا الشرط أثناء الممارسة العملية في تفتيش أجهزة الكمبيوتر، ويرجع ذلك إلى الطبيعة الخاصة لهذه الأخيرة الذي يحتوي بدوره على عدد كبير من الملفات، بالإضافة إلى أن أسماء هذه الملفات لا تدل بالضرورة على ما تحتويها، فقد يعمد المتهم إلى وضع أسماء مستعارة لملفات تحتوى على مواد غير مشروعة. كما تثار صعوبة قانونية أثناء تنفيذ إذن التفتيش على هذه الملفات، فهل يعتبر كل ملف "صندوقا مغلقا" يحتاج كل واحد منها إلى إذن قضائي مستقل عن الآخر ؟[1]

تضاربت أحكام القضاء الأمريكي بخصوص مدى ضرورة صدور إذن تفتيش مستقل لكل ملف من ملفات الحاسوب، حيث اعتبرت بعض الأحكام أن الديسك بما فيه من ملفات وجهاز الكمبيوتر بما يحتويه من ملفات، صندوقا مغلقا واحدا ومن ثم لا يشترط صدور إذن قضائي مستقل لكل ملف على حدا[2].

خلاف ذلك اتجهت أحكام أخرى للقضاء الأمريكي[3] إلى أن كل ملف في الكمبيوتر يتطلب إذنا خاصا لتفتيشه، وبناء على ذلك فإنها اعتبرت أن الملف الواحد صندوق مغلق، ويرجع أساس هذا الحكم

---

[1] - **عائشة بن قارة مصطفى**، مرجع سابق، ص 65.

[2] - **عائشة بن قارة مصطفى**، مرجع نفسه، ص 65.

[3] – قضت المحاكم الأمريكية بقبول التفتيش على أحد الموظفين للكشف عن دليل جريمة في قضية سيمون vs. United States 206 f.3d 392 (4th cir 2000) Simon, in; caselaw.findlaw.com/us-4th-circuit1452089.html. Consulté le: 23/04/2016.

ورفضت تفتيش قامت به الشرطة على أحد الموظفين للتدخل في عمل الموظف بحذف ملفات عمل قبل التفتيش، قضية Rossi Vs. Town of Pelham 35f.supp.(D.N.H 1997)2d 58 65-66, in; https://www.gpo.gov/fdsys/pkg/uscourts-paed-2_06-cv-05315/pd//. Consulté le: 23/04/2016.

إلى اعتبار أن الكمبيوتر يحتوى على الكثير من المعلومات التي تتعلق بالحياة الخاصة لصاحب هذا الجهاز –بمعنى اختلاط الملفات المجرمة مع البريئة– وإذا أجيز لرجال الضبط القضائي فتح الملفات الأخرى الموجودة داخل الجهاز فإن ذلك سوف يؤدي بالفعل إلى الاعتداء على الحياة الخاصة للأفراد. والواقع العملي لا يبرر ذلك، لأنه لا يعقل صدور أذون تفتيش بحسب عدد الملفات، هذا من جهة، ومن جهة ثانية لا يتصور امتداد إذن التفتيش إلى كل ملفات الحاسوب لان إذن التفتيش ليس إذنا على بياض باستباحة حرمة الشخص أو حرمة مسكنه بغير قيد، ولكنه مقيد بالغرض منه[1].

لم يقدم المشرع الجزائري حلا لهذه المسألة بصورة صريحة، ذلك أن القواعد الخاصة بإجراء التفتيش المذكورة في قانون الإجراءات الجزائية تتعلق بالتفتيش التقليدي الذي محله المساكن وملحقاتها، وأن القواعد الخاصة بإجراء التفتيش المعلوماتي الواردة بالقانون 09-04 لم يتحدث المشرع عن هذا الشرط إطلاقا، كل ما في الأمر أنه تحدث عن إعلام جهات التحقيق السلطة القضائية المختصة في حالة تمديد التفتيش إلى منظومة معلوماتية أخرى.

فهل يعني هذا السكوت أنه يجوز تفتيش المنظومة المعلوماتية دون حاجة إلى إذن آخر بالتفتيش يخص المنظومة المعلوماتية ويكفي فقط الإذن المتعلق بالمسكن الذي يتواجد فيه الحاسوب؟

طبقا لمعيار الخصوصية التي يحميها المشرع فإن النظام المعلوماتي وما يحتويه من أسرار وخصوصيات الأشخاص، فإنه يخضع بالتبعية لمبدأ عدم جواز الدخول إلى هذا النظام المعلوماتي وتفتيشه دون إذن من السلطة القضائية المختصة.

ب– الضوابط الشكلية لتفتيش نظم الحاسوب الآلي:

أضف إلى الضوابط الموضوعية لصحة إجراء تفتيش الوسائل الإلكترونية وشبكات الاتصال، هناك ضوابط شكلية تهدف إلى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة، وتقيم – بالإضافة إلى مقتضيات الإجراء – سياجا يحمي الحقوق والحريات الفردية. وتتمثل هذه الضوابط الشكلية في:

[1] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 65 .

1- إجراء التفتيش بحضور بعض الأشخاص المعنيين بالقانون:

لضمان الإطمئنان على سلامة الإجراء، وجب حضور الاشخاص المعينين بالقانون:
إن التشريعات الإجرائية المقارنة لم تشترط لصحة التفتيش حضور شهود عند تفتيشهم، أما فيما يتعلق بتفتيش المساكن وما في حكمها توجب حضور عملية التفتيش شهودا أو المشتبه فيه أو المتهم. ينص كل من القانونين الإجراءات الجزائية الجزائري والفرنسي[1] على وجوب حصول إجراء التفتيش المتعلق بالمساكن أو ملحقاتها بحضور المشتبه فيه أو المتهم عندما يتم تفتيش مسكنه – سواء من طرف قاضي التحقيق أو ضابط الشرطة القضائية – وإذا تعذر ذلك بامتناعه عن حضور التفتيش أو كان هاربا، يتم هذا الإجراء بحضور شاهدين من غير الموظفين الخاضعين لسلطة القائم بالتفتيش.

ان التعديل الذي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب القانون رقم (06-22) في المادة 45 منه، استغنى المشرع عن ضمانه حضور الأشخاص المحددين في الفقرة الأولى من هذه المادة في جرائم معينة منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، والحكمة من ذلك ترجع إلى ضرورة إضفاء نوع من السرية أثناء جمع الدليل الإلكتروني، خاصة وأن هذا الدليل ذو طبيعة خاصة من حيث سرعة تعديله والتلاعب فيه حتى عن بعد، كما أن هذه الضمانة بدأت تتضاءل أهميتها في الدول التي بدأت تأخذ "التفتيش عن بعد"، أو ما يطلق عليها في الفقه الفرنسي مصطلح Perquisition en ligne [2]

2- الميعاد الزمني لإجراء التفتيش في الجرائم المعلوماتية:

يقصد بشرط الميعاد الزمني أن يتم التفتيش خلال الفترة الزمنية المحددة حرصا على تضييق نطاق الاعتداء على الحرية الفردية وحرمة المسكن فاختلفت التشريعات الإجرائية في وقت تنفيذ التفتيش.

إن قانونين الإجراءات الجزائية الجزائري والفرنسي يحظران تفتيش المنازل وما في حكمهما

[1] – المادة 45 من قانون الإجراءات الجزائية الجزائري، سالف الذكر، والتي هي ترجمة حرفية للمادة 56 من قانون الإجراءات الجزائية الفرنسي سالف الذكر.

[2] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 67.

في وقت معين[1]، إلا ان هناك حالات استثنائية[2] نصت عليها المادة 10 من القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية، يجوز فيها الخروج عن هذه المواعيد ويصح إجراء التفتيش في أي ساعة من ساعات الليل والنهار، ذلك اذا تعلق الأمر بالجرائم المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف.

تدارك المشرع الجزائري قابلية الدليل الإلكتروني للمسح والتغيير في وقت قياسي باستثناء الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من حظر التفتيش ليلا.

3- محضر التفتيش في الجرائم المعلوماتية:

إن التفتيش في الأصل يعتبر عملا من أعمال التحقيق، ينبغي تحرير محضر يثبت فيه كل ما تم من إجراءات وما أسفر عنه التفتيش، لذلك إشترطت الكتابة في إذن التفتيش ولزوم وجوب التوقيع عليه ممن أصدره إقرارا بما جاء فيه، وإلا فإنّه لا يعتبر موجودا، ذلك لأن التوقيع هو السند الوحيد الذي يشهد بصدوره ممن صدر عنه.

تحرير محضر يتناول دليلا علميا يعني في الحقيقة ضرورة توافر مسلك علمي في تحريره يتوافق مع ظاهرة الدليل العلمي تحديدا بحيث يجب ألا يتخذ المحضر المظهر التقليدي فقط، فيجب مثلا التذكير بضرورة الارتباط بالخبرة وتحديد الخبرة في تحرير المحضر، فتحديد الخبرة لا يعني أن يكون كاتب المحضر من الخبراء العلميين هنا بقدر ما تعني ضرورة توافر الخبرات في هذه النوعية من القضايا، والمفارقة قائمة بين الخبرة والخبرات[3].

---

[1]- المادة 47 من قانون الإجراءات الجزائية الجزائري سالف الذكر، تجيز التفتيش من الساعة الخامسة صباحا إلى الساعة الثامنة مساء، أما في المادة 59 من قانون الإجراءات الجزائية الفرنسي تجيز التفتيش من الساعة السادسة صباحا إلى الساعة التاسعة مساء.

Article 59 du Code de procédure pénale Français Modifié par Loi 93-1013 du 24 août 1993 en vigueur le 2 septembre 1993, modifiant la loi n° 93-2 du 4 janvier 1993 portant réforme de la procédure pénale (rectificatif), in ;

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000732008&dateTexte=.

[2] - **عائشة بن قارة مصطفى**، مرجع سابق، ص 68.

[3] - **فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص 639.

الفرع الثالث

الضبط

يقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو من إجراءات التحقيق[1].

أن التشريعات الإجرائية عادة ما تجمع بين أحكام الضبط والتفتيش في موضع واحد، لكن ليس معنى ذلك أن الضبط لا يقع إلا نتيجة التفتيش، إذ من الممكن أن يكون الضبط نتيجة معاينة، كما أنه يجوز أن تضبط أشياء قدمها الشهود أو المتهمون باختيارهم، كذلك يجوز لسلطة التحقيق أن تطالب أحد الأفراد بتقديم شيء موجود في حيازته إليه ويلزمه بذلك[2].

أما الضبط في المجال المعلوماتية هو وضع اليد على المكونات –التي تفيد كشف الحقيقة في جريمة وقعت وجار التحقيق فيها– المادية للحاسوب والأدلة المعلوماتية المخزنة في الحاسوب محل التفتيش أو في الشبكة أو في الحاسوب الخادم والتي يطلق عليها تسمية المنقولات المعلوماتية[3]، لإمكانية نقل البيانات المعالجة إلكترونيا أو المعلومات من حاسب معين إلى حواسب أخرى سواء عن طريق شبكات الاتصال التي تربط بينها أو عن طريق الأقراص والشرائط الممغنطة، فمكونات الحاسب الآلي يصدق عليها وصف الشيء المنقول.

أولا : صلاحية ضبط الدليل الإلكتروني

إن ضبط المكونات المادية للحاسوب لا يثير مشاكل في الفقه المقارن ولا يوجد خلاف بين فقهاء القانون في إمكانية ضبط هذه المكونات، بل حتى إمكانية ضبط الحاسوب بشكل كامل لتأكيد

---

[1] – **محمد أبو العلا عقيدة**، شرح قانون الإجراءات الجزائية، الطبعة الثانية، دار النهضة، القاهرة، 2001، ص 448.

[2] – راجع كل عن: **هلالي عبد اللاه أحمد**، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص193. **محمد زكي أبو عامر**، الإجراءات الجنائية، دار الجامعة الجديدة، الإسكندرية، 2008، ص 554.

[3] – لأنها أشياء ذات طبيعة معنوية وهي البيانات، المراسلات والاتصالات الإلكترونية، فالبيئة الافتراضية لا تنتج سكينا أو سلاحا ناريا، وإنما تنتج نبضات رقمية تشكل قيمة وجوهر الدليل إلكتروني. **نبيلة هبة مولاي علي هروال**، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2005، ص 266.

الاحتفاظ بالدليل إذا كان مشغل الجهاز غير متعاون مع جهات التحقيق[1] أما بالنسبة لمكونات الحاسوب المعنوية، ولما فرض الواقع ضرورة ان يشمل التفتيش المكونات المعنوية للحاسوب، **وجب إباحة** إجراء الضبط على الكيانات المنطقية للحاسوب لكن ليس بالكيفية المنصوص عليها بموجب النصوص التقليدية لانتفاء الطابع المادي عن هذه البيانات، وعلى هذا الأساس استلزم التدخل التشريعي لتوسيع دائرة الأشياء التي يمكن أن يرد عليها الضبط لتشمل بجانب الأشياء المادية البيانات الإلكترونية بكافة أنواعها وأنماطها.

تدخل المشرع الجزائري بموجب القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، واستحدث المادة 06 التي تنص على أنه «عندما تكتشف السلطة التي تباشر التفتيش في منظومة المعلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وانه ليس من الضروري حجز كل المنظومة يتم نسخ كل المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحراز وقف القواعد المقررة في قانون الإجراءات الجزائية... ».

قام المشرع الفرنسي بإدخال تعديل على قانون الإجراءات الجزائية لسد هذا الفراغ التشريعي بموجب قانون الأمن الداخلي رقم 239 لسنة 2003[2]، حيث أن المادة 17 استحدثت المواد 57-1، 76-3، 97-1، من قانون الإجراءات الجزائية، وتنص فقرة 3 من المادة 57-1 على وجوب نسخ وتحريز البيانات التي يتم الحصول عليها من إجراء تفتيش النظام المعلوماتي يتعين نسخها على دعامات. كذلك المشرع البلجيكي فقام بمقتضى قانون 28 نوفمبر 2000 بتعديل قانون التحقيق الجزائي بإضافة المادة 39 bis التي سمحت بضبط الأدلة الإلكتروني، مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية.

---

[1] – **عفيفي كامل عفيفي**، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، مرجع سابق، ص 353.

[2] – Art 57-1 Créé par Loi 2003-239 , cité précédemment, art. 17 dispose que :

« Les données auxquelles 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. »

ثانيا : إجراءات الضبط الدليل الإلكتروني

أمام غياب الثقافة المعلوماتية عند المحقق–مما يجعل تلك الأدلة عرضة للإتلاف والإفساد– يتعين اتخاذ بعض الإجراءات الخاصة للحفاظ عليها وصيانتها من العبث[1] وذلك على النحو التالي:

وضع المشرع الجزائري في قانون رقم 09-04 المتعلق بتكنولوجيات الإعلام والاتصال ومكافحتها طريقتين لضبط الأدلة الإلكترونية، الأولى تكون عن طريق نسخ المعطيات محل البحث على دعامة تخزين إلكترونية تكون هذه الأخيرة قابلة لحجزها ووضعها في أحراز حسب ما هو مقرر في قواعد تحريز الدليل المنصوص علها في قانون الإجراءات الجزائية، والطريقة الثانية تكون باستعمال التقنيات المناسبة، وحاليا يتم استخدام برامج متخصصة في النسخ مثل برامج Lap Link، كما يوجد أسلوب تجميد التعامل بالحاسوب أو إحدى القطع المكونة له التي استخدمت في ارتكاب الجريمة، ويتخذ هذا الأسلوب عدة مظاهر، ويتم اللجوء إلى هذا الإجراء في حالة ما إذا كانت البيانات تتضمن خطرا أو ضررا بالمجتمع، لمنع الوصول إليها.

ثالثا: الصعوبات التي تواجه المحقق أثناء عمليات الضبط

إنّ الضبط الذي يرد على عناصر معلوماتية منفصلة مثل الديسكات والأسطوانات الممغنطة لا يثير أي صعوبات حينما يتم الضبط، ولكن الصعوبات تثور:

–عندما يلزم ضبط النظام كله أو الشبكة كلها، ذلك لأنها تحتوي على عناصر لا يمكن فصلها، ومع ذلك يتعين ضبطها لأنها تتضمن عناصر للإثبات في الجريمة، لهذا يتم إعمال مبدأ التناسب والذي يقصد به، اقتصار الضبط على الأدلة التي تفيد في كشف الحقيقة، بطريقة لا يؤدي الضبط إلى تعطيل كل العمل في النظام والشبكات المتصلة به[2]. يفيد مبدأ التناسب إقامة التوازن بين مصلحتين، مصلحة الدولة في كشف الحقيقة، ومصلحة صاحب النظام في تسيير إعماله وعدم ضياع فرص الربح عليه .

– إذا كانت عملية الضبط لهذه الوسائل التقنية تتم في الأنظمة المعلوماتية الكبيرة أو الشبكات الكبيرة فقد يؤدي إجراء الضبط إلى عزل النظام المعلوماتي بالكامل عن دائرته لمدة زمنية قد تطول

[1] – أنظر المواد 45 و84 قانون الإجراءات الجزائية الجزائري سالف الذكر

[2] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 71.

أو تقصر، مما قد يتسبب في إلحاق أضرار بالجهة المستخدمة بالنظام بالإضافة إلى عدم إبداء مستخدمي الأنظمة المعلوماتية الاستعداد للتعاون الكامل والفعال مع سلطات التحقيق لما قد يعنيه إجراء الضبط بالنسبة لها مساسا بالسرية.

– أن الضبط في مجال المعلوماتية قد يمثل أحيانا اعتداء على حقوق الغير أو على حرمة حياتهم الخاصة مما يستوجب اتخاذ الضمانات اللازمة لحماية هذه الحقوق والحريات[1].

– قد تفرض أحزمة أمنية من قبل مستخدم النظام حول البيانات التي يحويها هذا النظام، ومما يزيد من صعوبة الأمر على المحقق عدم معرفته لكلمات السر أو شفرات المرور أو شفرات ترميز البيانات وقد لا يبدي المشتبه فيه تعاونه في الكشف عن هذه الشفرات لجهات التحقيق.

– كذلك من الصعوبات التي تواجه المحقق انه عندما يتلقى بلاغ يفيد ارتكاب جريمة جنائية على أحد المواقع، ولا يستطيع التحري عن مرتكبيها إلا بالدخول للموقع الإلكتروني للمرسل أو لمواقع عدة لضبط مرتكب الجريمة، وهو أمر لا يجوز البدء فيه إلا بموجب إذن من النيابة العامة وندبها لخبير الفني بعد أداء اليمين، لأن ذلك الأمر يتطلب القيام بالتفتيش والمعاينة فإذا قام مأمور الضبط بذلك قبل الإذن من النيابة كان الإجراء باطل وإذا تم ضبط الأجهزة بموجب إذن ولكنه فحص الدليل المعثور عليه فنيا بمعرفته لا يعد ذلك من قبل الخبرة لأن المشرع أوجب مراعاة إجراءات معينة يترتب البطلان على مخالفتها[2].

---

[1] – **محمد أبو العلا عقيدة**، "التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية"، ورقة عمل مقدمة في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث والدراسات، أكاديمية شرطة دبي، الإمارات العربية المتحدة، المنعقد في الفترة 26 – 28 أبريل 2003، ص 39.

[2] – **فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص 625.

المطلب الثاني

الإجراءات الشخصية

يقصد بالإجراءات الشخصية، تلك الإجراءات التقليدية –حتى وإن كان بعضها مستحدث في الأونة الاخيرة– التي يتدخل فيها بعض الأشخاص بحكم صفتهم، وبواسطتهم يتم الحصول على الدليل.

الفرع الأول

الشهادة

الشهادة بصفة عامة هي إثبات حقيقة واقعة معنية، علم بها الشاهد من خلال ما شاهده أو سمعه أو أدركه بحواسه الأخرى عن تلك الواقعة بطريقة مباشرة، والشهادة على هذا النوع تعد وسيلة إثبات أساسية في المسائل الجزائية، لأنها تنص في الغالب على وقائع مادية تقع فجأة، يتعذر إثباتها إلا عن طريق الشهادة[1].

لا تقل الشهادة أهمية في الجرائم المعلوماتية عن باقي الإجراءات في الحصول على الدليل الإلكتروني، فالقاعدة العامة تقتضي بأن يلتزم الشاهد بالإفصاح بما يعلمه من معلومات بخصوص واقعة الجريمة والفاعلين فيها، والإدلاء بكل ما يفيد في كشف الحقيقة من وقائع أخرى[2].

يجب إلمام المحقق في الجرائم المعلوماتية بمبادئ الحاسوب والأنترنت والمصطلحات المتعلقة، ومبادئ وأسس أمن المعلومات بالشكل الذي يمكّنه من التواصل الجيد مع الشهود والمتهمين من جهة ومع خبير الحاسوب في فريق التحقيق من جهة أخرى[3].

فيما يلي سيتم التطرق إلى المقصود بالشاهد في الجريمة المعلوماتية- الشاهد المعلوماتي- والتزاماته.

---

[1] – **إبراهيم الغمار**، الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1980، ص 30.

[2] – وهو ما حدث فعلا في قضية Broderbund حيث شهد فيها الشهود بأن مبرمجي "يونيسون" قد طلب منهم نسخ برمجية "بردرباند" إلا أنهم قاموا ذلك بإهمال .**عائشة بن قارة مصطفى**، مرجع سابق، ص78.

[3]– كان الأسلوب الأمثل في عملية استجواب الشهود في الجريمة المعلوماتية ضرورة حضور خبير الحاسوب لعملية الاستجواب وتمكينه من الاشتراك فيها بتوجيه الأسئلة الفرعية للشاهد، وربما قام بكتابة السؤال على قطعة من الورق ووضعها أمام المحقق ليقوم الأخير بتحيّن الفرصة المناسبة لإلقاء السؤال بما يتناسب والأصول الفنية للاستجواب. **محمد الأمين البشري**، التحقيق في الجرائم المستحدثة، مرجع سابق، ص 380 .

أولا : المقصود بالشاهد المعلوماتي

إنّ الشاهد المعلوماتي أو الشاهد في الجريمة المعلوماتية يختلف من حيث صفته عن غيره من الشهود في الجرائم التقليدية، غالبا ما يكون من أصحاب المعرفة التقنية للنظام المعلوماتي وذلك بحكم عملهم، ولا يقصد من ذلك أن يكون الشاهد خبيرا، بل كلاهما يختلفان عن بعضهما البعض، حيث يقدم هذا الأخير تقارير وآراء توصل إليها بتطبيق قوانين علمية أو أصول فنية، أما الشاهد يقدم إلى القاضي معلومات حصلها بالملاحظة الحسية[1].

يعرف الشاهد المعلوماتي بأنه " ذلك الشخص الفني صاحب الخبرة المعلوماتية والتخصص في التقنية وعلوم الحاسب الآلي، الذي تكون لديه معلومات أساسية وجوهرية هامة لازمة للولوج في نظام المعالجة الآلية للمعطيات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة تتعلق بالجريمة داخله"[2].

نماذج عن هؤلاء الشهود[3] كما يلي:

- مشغلو الحاسوب: ذلك الشخص الذي تكون لديه خبر كبيرة في استخدام جهاز الحاسب الآلي ومكوناته، وهو المسؤول عن تشغيل الجهاز ومعداته والملحقات والمعدات المتصلة به.
- خبراء البرمجة: وهم مخططو البرامج، متخصصون في كتابة أوامر البرامج الخاصة بجهاز الحاسب الآلي، وهم فئتين، مخططو البرامج التطبيقية ومخططو برامج النظم.
- المحللون: هم الذين يحللون الخطوات ويقومون بتتبع البيانات داخل النظام، كما يقومون بتجميع بيانات النظام ودراستها وتحليلها وتقسيمها إلى وحدات.
- مهندسو الصيانة والاتصالات: هم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به.
- مديرو النظم: وهم الذين لهم أعمال الإدارة في النظم المعلوماتية [4].

---

[1] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 78.

[2]– **عادل عبد الله خميس المعمري**، "التفتيش في الجرائم المعلوماتية"، مجلة الفكر الشرطي، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، دولة الإمارات العربية، المجلد الثاني والعشرون، العدد 86، ص 52.

[3] – **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، مرجع سابق، ص 157.

[4] - **عائشة بن قارة مصطفى**، مرجع سابق، ص79

إضافة إلى هذه الفئات، هناك أشخاص آخرون يعدون بمثابة شهود في الجريمة المعلوماتية، وهي فئة لها دور كثير في شبكة الأنترنت إلى المستهلك من بينهم: مقدمو الخدمات الوسطية في مجال المعلوماتية والأنترنت، أيضا متعهدو الوصول ومتعهدو الإيواء مسؤولو المنتج مسؤولو ناقل المعلومات ومسؤولو متعهد الخدمات، كذلك مورد المعلومات ومؤلف الرسالة[1].

ثانيا : التزامات الشاهد المعلوماتي

تعد التزامات الشاهد المعلوماتي نفسها التزامات الشاهد في الجرائم التقليدية، ومن أهم هذه الالتزامات يذكر:

أ- حضور الشاهد:

ان سلطة التحقيق كامل الحرية في أن تسمع الشهود عن الوقائع التي تثبت أو تؤدي إلى ثبوت الجريمة وظروفها وإسنادها إلى المتهم أو براءته منها، ولها كذلك أن تسمع شهادة الشهود الذين يطالب الخصم سماعهم ما لم يرى عدم الفائدة من سماعهم[2].

نص المشرع الجزائري في المادة 223- 1قانون الإجراءات الجزائية الجزائري، والتي تحيل إلى المادة 97 من القانون نفسه – صراحة على عقاب الشاهد المتخلف عن الحضور أو رفض حلف اليمين أو أداء الشهادة.

أجاز القانون 15-03[3] في المادة 14 و15 منه إذا استدعى بعد المسافة أو تطلب ذلك حسن سير العدالة استجواب وسماع الأطراف عن طريق المحادثة المرئية عن بعد مع مراعاة احترام الحقوق والقواعد المنصوص عليها في قانون الإجراءات الجزائية.

ب- حلف اليمين:

تنص المادة 227 من قانون الإجراءات الجزائية الجزائري على إلزام أن يؤدي الشاهد اليمين

---

[1] – **عائشة بن قارة مصطفى**، مرجع نفسه، ص 79.

[2] – **محمد نجيب حسني**، شرح قانون الإجراءات الجزائية، الطبعة الثانية، دار النهضة العربية، القاهرة،1988، ص 448.

[3] – قانون رقم 15-03 مؤرخ في 11 ربيع الثاني عام 1436 الموافق أوّل فبراير2015 يتعلق بعصرنة العدالة، الجريدة الرسمية للجمهورية الجزائرية عدد 06، بتاريخ 10 فبراير 2015.

القانونية حسب الصيغة القانونية المنصوص عليها في المادة 93 من القانون نفسه[1]، ويترتب على مخالفة هذا الإجراء بطلان شهادته.

قد استقرت المحاكم الفرنسية طبقا للمادة 331-3 من قانون الإجراءات الجزائية الفرنسي[2] على الحكم ببطلان الشهادة إذا حلف الشاهد "أن يقول الحق" بدلا من عبارة "كل الحق" لأنه قد يخفي جزءا من الحقيقة، أو إذا حلف بأن يقول "كل الحق" ولم يقل عبارة "لا شيء غير الحق" لأنه قد يقول الحقيقة ويضيف لها شيء غير حقيقي[3].

ج- أداء الشهادة:

يلتزم الشاهد بالإدلاء بشهادته[4] والتزام بقول الحقيقة، حيث الشهادة كذبا من أجل تضليل الحقيقة تعد شهادة زور منصوص عليها في المادة 332 من القانون العقوبات الجزائري، بالتالي يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في الحاسبات والمواقع التي تحتوي على المعلومات التي تشكل جريمة بحثا عن أدلة تثبتها. طرح الفقه المقارن عدة تساؤلات، منها مدى إجبار الشاهد المعلوماتي على تقديم دليل فني يتعلق بهذه الجريمة والذي يكشف لجهات التحقيق -بطباعة أو تحليل ذاكرة النظام المعلوماتي- عن آثار بعض البيانات التي تساعد في كشف الحقيقة.

هناك بعض القوانين الأوربية - مثل القانون الإنجليزي الصادر في 1984 بشان البوليس والأدلة الجزائية[5]- التي أوجبت على " الشاهد أن يقوم بإجراء إنعاش الذاكرة، وذلك لفحص الأماكن والمستندات التي توجد تحت سيطرتهم إذا لم تترتب على ذلك أضرار خطيرة، لان الالتزام بالتعاون ليس

---

[1] - جاءت صيغة اليمين القانونية حسب المادة 93-2 من قانون الإجراءات الجزائية الجزائري السالف الذكر« أقسم بالله العظيم أن أتكلم بغير حقد ولا خوف وأن أقول كل الحق ولا شيء غير الحق ».

[2]- Article 331, paragraphe 3, dispose que : « avant de commencer leur déposition, les témoins prêtent le serment " de parler sans haine et sans crainte, de dire toute la vérité, rien que la vérité ".

[3] - راجع كل من: **هلالي عبد اللاه أحمد**، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص 846. **عائشة بن قارة مصطفى**، مرجع سابق، ص 83.

[4]- المادة 331 من قانون الإجراءات الجزائية الفرنسي سالف الذكر، تحدد واجبات الشاهد في الشهادة بخصوص الوقائع المسندة إلى المتهم أو بخصوص شخصية هذا الأخير أو أخلاقياته.

[5] -Art 53, **Police and Criminal Evidence Act 1984** , in ; http://www.legislation.gov.uk/ukpga/1984/60/pdfs/ukpga_19840060_en.pdf.

فقط بمجرد إصدار الأمر بإحضار الشهود، ولكن إلزام الغير بتقديم المساعدة للسلطة القضائية عن طريق تقديم الأدلة أو المساعدة للوصول إليها، كما تسمح هذه التشريعات بالاستفادة بالشهود كخبراء[1].

لذلك فان الشاهد يلتزم بالكشف عن الشفرات أو كلمات السر التي يكون على علم بها، لكن لا يجوز إكراهه على ذلك[2]، يميل لهذا الاتجاه الفقه الألماني حيث يرى أن عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب، ولا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية أو كشف شفرات تشغيل البرامج المختلفة[3].

أن بعض الفقهاء في فرنسا يؤيدون هذا الاتجاه ويبررون موقفهم على أساس أن المشرع الفرنسي طالما لم ينظم هذه المسألة فإنه لا مناص من تطبيق قواعد العامة في الشهادة، ومن ثم فإن الشهود الذين تقع على عاتقهم الالتزام بالشهادة يكونون مكلفين بالكشف عن كلمات المرور السرية التي يعرفونها، وشفرات تشغيل البرامج، باستثناء حالات المحافظة على سر المهني فإنهم يكونون في حل من هذا الالتزام[4].

يجب الإشارة في هذا الصدد أنه نتيجة قصور أحكام الشهادة في الحصول على الدليل الإلكتروني، وجب البحث عن وسيلة قانونية جديدة تحقق ما لم تستطع فكرة الالتزام بأداء الشهادة أن تؤديه، وهذه الوسيلة هي "الالتزام بالإعلام في الجريمة المعلوماتية"، وهي أن تستعمل بعض الدول وسائل للضغط على الشهود بهدف حملهم على التعاون الإيجابي مع سلطات التحقيق، حيث يسأل الشاهد الذي يخفي الشفرة أو كلمة السر أو الذي يعطي أوامر خاطئة عن جريمة شهادة الزور لأنه يعوق سير العدالة، كما قد يسأل باعتباره شريكا في الجريمة موضوع المحاكمة[5]. أوصى المؤتمر

---

[1] – **جميل عبد الباقي الصغير**، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دراسة مقارنة، دار النهضة العربية، القاهرة، 1992، ص 106.

[2] –**Sahir ERMAN**, « Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Turquie », RIDP, v 64, 1er et 2eme trim, p 624.

[3] – **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر والأنترنت، مرجع سابق، ص 162. كذلك: **Jacques FRANCILLON**, op.cit, p 309.

[4]- **Jacques FRANCILLON**, ibid, p 309.

[5] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 85.

الدولي الخامس عشر للجمعية العامة لقانون العقوبات الذي عقد في ريو دي جانيرو بالبرازيل [1]بالتعاون الفعال بين المجني عليهم والشهود وغيرهم من مستخدمي تكنولوجيا المعلومات بقيام الشاهد بالإفصاح عن كلمات السر أو الكشف عن الشفرات الخاصة بالبرامج المختلفة.

الفرع الثاني

الخبرة

تنصرف الخبرة إلى رأي الخبير الذي يثبته في تقريره الذي يعتبر من الأدلة الفنية، فان إجراء ندب خبير هو من إجراءات جمع الأدلة، للمحقق الاستعانة بالخبراء ليستطلع رأيهم في بعض الأمور التي تعرض له أثناء تأدية مهمته في التحقيق الذي ينتهي بإصدار قرار بأن لا وجه لإقامة الدعوى أو بإحالتها إلى محكمة الموضوع[2]، وأما الخبرة في مرحلة المحاكمة فإنها تساعد القاضي في تكوين عقيدته للفصل في القضية .

أولا: المقصود بالخبرة

الخبرة هي الاستشارة الفنية التي يستعين بها المحقق أو القاضي في مجال الإثبات لمساعدته في تقدير المسائل الفنية أو الإدارية التي لا تتوافر لدى عضو السلطة القضائية المختص بحكم عمله وثقافته[3].

إهتم المشرع الجزائري بتنظيم أعمال الخبرة، حيث أجاز قانون الإجراءات الجزائية الجزائري للنيابة العامة ولقاضي التحقيق وللمحاكم كذلك الاستعانة بخبير واحد أو أكثر[4].

تزداد أهمية الخبرة في إثبات الجرائم المعلوماتية، حيث ان نجاح الاستدلالات وأعمال التحقيق في الجرائم المعلوماتية يكون مرتهنا بكفاءة وتخصص هؤلاء الخبراء' فأصبح إنشاء المعامل الجزائية الإلكترونية مطلبا ملحا لفحص الأدلة الإلكترونية، ولتقييم عملية الإثبات

---

[1] –**congrès international de droit pénal**, 15ème, Rio De Janeiro, Brésil , 4-10 septembre 1994, in ; http://www.penal.org/sites/default/files/files/RIDP_1995_1_2.pdf. consulté le 19/10/2017.

[2] – **حسين بن سعيد بن سيف الغافري**، السياسة الجنائية في مواجهة جرائم الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2009، ص 440.

[3] – راجع كل عن: **عبد الناصر محمد محمود فرغلي**، محمد عبيد سيف سعيد المسماري، مرجع سابق، ص 24. **أمال عثمان**، الخبرة في المسألة الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1964، ص 28.

[4] – المواد من 143 إلى 156 قانون الإجراءات الجزائية الجزائري سالف الذكر.

الإلكتروني وتحليل الجرائم في نطاق ما يعرف باسم "نظم الخبرة الأمنية"[1]. تساعد الخبرة في المجال المعلوماتي على:

- الكشف عن الدليل الإلكتروني.
- إجراء الاختبارات التكنولوجيا على الدليل الإلكتروني للتحقق من أصالته ومصدره كدليل يمكن تقديمه لأجهزة إنقاذ القانون.
- تحديد الخصائص الفريدة للدليل الإلكتروني.
- إصلاح الدليل الإلكتروني وإعادة تجميعه من المكونات المادية للكمبيوتر.
- عمل نسخة أصلية من الدليل الإلكتروني للتأكد من عدم وجود معلومات أثناء عملية استخلاص الدليل.
- جمع الآثار المعلوماتية الإلكترونية التي تكون قد تبدلت خلال الشبكة المعلوماتية[2].

تخضع الخبرة التقنية لنفس القواعد القانونية التي تحكم الخبرة عموما باختلاف الأمور الفنية التي تحكم عمل الخبير الفني، إلا أن هناك بعض التشريعات نظمت أعمال الخبرة في مجال الجرائم المعلوماتية بنصوص قانونية خاصة فلم تكتف بالنصوص التقليدية التي تنظمها، مثل القانون التحقيق الجزائي البلجيكي [3].

أشار المشرع الجزائري في المادة 05 الفقرة الأخيرة من القانون رقم 09-04 المتضمن القواعد الخاصة بالوقائع من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها أنه يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

ثانيا: القواعد القانونية التي تحكم الخبرة التقنية

الخبرة هي إجراء يستهدف استخدام قدرات شخص الفنية والعلمية والتي لا تتوافر لدى رجل

[1] – **ممدوح عبد الحميد عبد المطلب**، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والأنترنت، مرجع سابق، ص 9.

[2] – **سعيداني نعيم**، مرجع سابق، ص 170.

[3] – art 88bis du Code d'instruction criminelle, cité précédemment.

القضاء أو المحقق من أجل الكشف عن دليل يفيد في معرفة الحقيقة بشأن وقوع الجريمة.

بهذا سيتم التطرق إلى النقاط التالية:

أ- تعيين الخبراء:

قد تعترض المحقق أثناء سريان التحقيق، بعض المسائل الفنية الهامة التي يحتاج كشفها إلى خبرة علمية دقيقة، حدد المشرع الجزائري طرق اختيار الخبراء في المادة 144 من قانون الإجراءات الجزائية الجزائري، ويشترط في الخبير حقيقة الجمع بين العلم ذي الاختصاص والخبرة العلمية، فلا يكفي فقط كفاءة علمية عالية في مجال التخصص، بل يضاف إليها سنوات من أعمال الخبرة في المجال، يجوز للقاضي ندب خبير من خارج الجدول، وإن كان القضاء الفرنسي يستلزم في هذه الحالة ضرورة أن يقوم القاضي بتسبيب قراره وإلا ترتب البطلان على قرار ندب الخبير[1].

يصح لقاضي التحقيق أن ينتدب بقرار مسبب أي شخص يأنس فيه الكفاءة خاصة في مجال الحاسوب والأنترنت، سواء كان اسمه مقيدا في جدول الخبراء أم لم يكن، إلا أن هذا الأخير يجب استحلافه اليمين بأن يؤدي عمله بصدق وأمانة[2]، وتنص المادّة 19من المرسوم الرئاسي رقم 15-261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته[3] على انه يمكن ان تستعين الهيئة بأي خبير أو أي شخص يمكن أن يعينها في أعمالها.

---

[1] – **سليمان عبد المنعم**، بطلان الإجراء الجنائي، دار الجامعة الجديدة، الإسكندرية، 1999، ص 182.

[2]– هذا ما جاء في نص المادة 145– 3 قانون الإجراءات الجزائية الجزائري، ترك القانون لقاضي التحقيق حرية ندب خبير واحد أو خبراء متعددين وهذا حسب المادة 147 قانون الإجراءات الجزائية الجزائري كما تنص المادة 149 من هذا القانون على استطاعة هذا الخبير الاستنارة في مسألة خارجية عن تخصصه بفنيين آخرين ويتعين على هؤلاء أن يخلفوا اليمين وفقا للشروط المنصوص عليها في المادة 145 من القانون نفسه. وهذا التعدد ضروري في مال الخبرة التقنية، ذلك أنه من الصعوبة وجود متخصص منفرد له الدراية الكاملة بتقنيات الحاسوب ونظمه، حتى وإن كان يملك القدرات المالية على الظهور بمظهر المنفرد في مجال الخبرة القضائية هذا من جهة.

[3]– مرسوم رئاسي رقم 15-261 مؤرّخ في 24 ذي الحجة عام 1436الموافق 8 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، الجريدة الرسمية للجمهورية الجزائرية عدد 53 بتاريخ في 08 أكتوبر 2015.

ب- أنواع الخبراء الإلكترونيين:

1. **المبرمج:** هو المتخصص في كتابة أوامر البرامج سواء كانت برامج النظم أو برامج التطبيقات، فالمتخصص في كتابة أوامر التطبيقات يعرف مواصفات النظام الإداري المطلوب من محلل النظم، ثم يقوم بتحويل ذلك إلى برامج الإلكترونية رقمية، أم المتخصص ببرامج النظم فيقوم باختيار وتعديل وتصحيح برامج نظام الحاسب الداخلية، التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين، بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج.

2. **المحلل:** هو الشخص الذي يحلل خطوات العمل ويقوم بتجميع بيانات نظام معين كما هو الحال في نظم المعلومات الإدارية وغيرها.

3. **مهندس الصيانة والاتصال:** هو المسؤول عن صيانة التقنيات الإلكترونية الرقمية وشبكاتها وفحصها.

4. **مشغل الحاسب الآلي وشبكاته:** هو المختص بتشغيل الحاسب الآلي ومكوناته، ولديه خبرة في قواعد كتابة البرامج وتشغل الجهاز واستخدام أدوات إدخال البيانات.

5. **مدير النظام المعلوماتي:** هو المختص بالإدارة في النظم المعلوماتية[1].

ج- حلف اليمين:

يجب لصحة عمل الخبير أداء اليمين القانونية طبقا للمادة 145 من قانون الإجراءات الجزائية الجزائري، ولا ينبغي عن هذا الإجراء أي ضمانة أخرى من الضمانات. وكما سبق الذكر إن أداء الخبير لليمين يوم تسلمه العمل يغنى عن أدائه اليمين عند مباشرة كل مأمورية له، إما إذا كان الخبير من غير خبراء وزارة العدل المعنيين بالقانون، أو كان اسمه غير مقيد في الجدول، يجب في هذه الحالة أداء اليمين بأن يؤدي عمله بكل صدق وأمانة.

[1] – **فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص 104.

د- تقرير الخبرة:

يعد الخبير بعد انتهائه من إجراء الخبرة اللازمة تقريرا يحمل الإستنتاجات التي توصل إليها، فيودع تقرير كتابي مرفق بملحق إيضاحي مفسر، حتى يسهل على جهات التحقيق فهم الخبرة، وحتى تتمكن جهات الحكم من تكوين عقيدتها واقتناعها الذاتي بالدليل، وعلى الخبير تقديم التقرير الفني خلال المدة المحددة بأمر الندب، وإلا جاز للقاضي استبداله في الحين مع إلزامه برد جميع الأشياء والأوراق والوثائق التي تكون قد عهد بها إليه في ظرف 48 ساعة[1]، كما قد يتعرض الخبير المقصر إلى عقوبات تأديبية وحتى جزائية[2].

هـ- حجية تقرير الخبير التقني:

ان المبدأ المستقر عليه ان القاضي خبير الخبراء، إلا أنه – رغم استقراره – يتعرض لهزات عنيفة إزاء التزايد المتواصل لمبدأ التفاعل القانوني مع الظواهر العلمية التي تقع في اختصاص آخر غير الجوانب النظرية، أو التي لا تسمح ثقافة القاضي المبنية على معايير العدالة والدراسات القانونية من التفاعل معها، لاسيما في فرضية أو منطق التفاعل مع ظاهرة مثل الأنترنت التي تشكل، ثقافة جديدة على الجيل المعاصر[3].

ان الخبرة شأنها شأن باقي أدلة الإثبات تخضع حجيتها لتقدير القاضي، فالقانون لم يضفِ على تقرير الخبير أية قوة ثبوتية خاصة، فهي لا تلزم القاضي[4]، ولهذا الأخير مطلق الحرية في تقديره، فله أن يأخذ بنتائج الخبرة أو استبعادها كما يشاء، وله كذلك أن يأمر بإجراء خبرة تكميلية أو القيام بالخبرة مضادة أو مقابلة لاسيما إذا تعارضت النتائج التي توصل إليها الخبراء حول نفس المسألة أو تعارض تقرير الخبير مع شهادة أحد الشهود.

---

[1] – المادة 149 قانون الإجراءات الجزائية الجزائري، سالف الذكر

[2]-**Jean Lamarque**, « la responsabilité pénale de l'expert », RSC, 1976, p. 724.

[3] – **فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص 670.

[4] –**Jean PRADEL,** Les rôles respectifs du juge et du technicien dans l'administration de la preuve en matière pénale, 10ème Colloque des Instituts d'études judiciaires, Poitiers, Paris , 1975,p 69.
عائشة بن قارة مصطفى، مرجع سابق، ص 91.

إن عمل الخبير التقني من أعمال الخبرة غير مطلقة في طبيعتها، يلتزم الخبير التقني بما هو مقرر في مفاهيم المشروعية واحترام المواطن، إذ ليس للخبير أن يلجأ إلى أساليب غير مشروعة من أجل القيام بعمله.

كذلك يكون للخبير أن يطلع على شهادات وأقوال الجناة، إذ كثيرا ما يكون في مثل هذه الأقوال عوامل مساعدة لخبرته، فيمكن من خلالها التعرف على أسلوب عمل مرتكب الجريمة المعلوماتية والتعامل معه على أساس أقواله، [1].

إنّ استعانة خبير قضائي بمجرم معلوماتي للتعرف على أسلوب ارتكاب جريمة معلوماتية لا يجعل من الهاكر خبيرا في الدعوى، إذ أن التقييم المعلوماتي يظل هنا للخبير القضائي ثم للقاضي الموضوع في نهاية المطاف. وما دور الهاكر إلا دور مساعد للخبير، وللخبير أن يطلب مساعدة من يشاء في هذا الإطار، على أن المساعدة المطلوبة في هذا الحالة تكون من مجرم لاسيما إذا كان مطلوبا للعدالة في جريمة أخرى مرتكبة[2].

ثالثا: القواعد الفنية التي تحكم الخبرة التقنية

إنّ نجاح التحقيق في الجرائم المعلوماتية مرتهن على كفاءة هؤلاء الخبراء فيجب على المحقق أن يحدد للخبير المعلوماتي دوره في المسألة المنتدب فيها على وجه الدقة .

أ- **أساليب عمل الخبير التقني:**

للخبير التقني في سبيل تحري الحقيقة أن يقوم بكل ما يمكنه للتوصل إليها، وأن يستخدم الأساليب العلمية التي يقوم عليها تخصصه وليس للمحكمة أن ترفض تلك الأساليب. **وهناك أسلوبان لعمل الخبير التقني:**

- القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها، كما هو الشأن في

---

[1] – معلوم أن الكونجرس الأمريكي قد استدعى أحد كبار فكرة العالم الافتراضي، بل وأخطرهم على الإطلاق، وهو كيفين متينيك، لكي يدلي بشهادته كهاكر عن كيفية الاختراق ورأيه في إعداد تشريع يحظر الاختراق، ولقد تضمنت شهادته الكثير من الأمور التي كانت خافية على رجال التشريع والقانون .**فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص 698.

[2] – **فتحي محمد أنور عزت**، دور الخبرة في الإثبات الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، 2007، ص 42.

التهديد أو النصب أو السب أو جرائم النسخ وبث صور فاضحة بقصد الدعاية للتحريض على ارتكاب جرائم الدعارة والرقيق ودعارة الأطفال وغيرها، ثم القيام بعملية تحليل رقمي لها لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه، وتحديد عناصر حركاتها، وكيف تم التوصل إلى معرفتها، ومن ثم التوصل في النهاية إلى معرفة بروتوكول الأنترنت IP الذي ينسب إلى جهاز الحاسوب الذي صدرت عنه هذه المواقع[1].

– القيام بتجميع وتحصيل مجموعة المواقع التي لا تشكل موضوعها جريمة، وإنما تؤدي حال تتبع موضوعها إلى قيام الأفراد بارتكاب جرائم، كما هو الحال في المواقع التي تساعد الغير على التعرف على جرعات المخدرات والمؤثرات العقلية التي تناسب وزن الإنسان بادعاء أنه إذا تتبع التعليمات الواردة فيها فلن يصاب الشخص بحالة إدمان، وأيضا كيفية زراعة المخدرات بعيدا عن أعين الغير وأيضا كيفية إعداد القنابل وتخزينها، وكيفية التعامل مع القنابل الزمنية وتركيبها والقيام بفكها وحفظها[2].

ب– القواعد التي يتعين على الخبير الإلمام بها:

– مكونات التقنية الإلكترونية الرقمية من مادية ومعنوية ونظم وبرامج وكلمات مرور وغير ذلك من تلك التقنيات.

– شبكات التقنية الإلكترونية الرقمية وبيئتها الإلكترونية من تردد وموجات البث وأماكن اختزانها.

– المواضع المحتملة للأدلة الإلكترونية الرقمية الثبوتية والشكل أو الهيئة التي تكون عليها.

– أثر التحقيق في الجرائم عبر الحاسب الآلي وشبكة الأنترنت اقتصاديا وماليا على المشاركين في استخدام النظام.

– كيفية عزل النظام المعلوماتي دون تلف الأدلة أو تدميرها أو تعديلها أو الحاق الضرر بالأجهزة.

---

[1] – **فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص 693.

[2] – **Patrick S CHEN**, An automatic system for collection crime information on the internet, 31 October 2000, Journal of information law and technology, in; http://elj.warwick.ac.uk/jit/00-3/chen.html.consulté le: 22/04/2016.

– كيفية نقل أدلة الإثبات الإلكترونية إلى وحدات خارجية بغير أن يلحقها تلف. كيفية إخراج الأدلة الإلكترونية الرقمية في وسيلة ورقية وتقديمها للقاضي لقراءتها وفهمها مع إثبات أن المسطور على السطور هو مطابق للمسجل على الحاسب أو النظام أو الشبكة[1].

لا ينجح الخبير المعلوماتي في أدائه لمهنته المنوط بها وإتمامه للمهمة المكلف بها إن لم يكن لديه هذا القدر من المتطلبات الفنية.

إن أهم المسائل التي على الخبير أن يستعان بها في الخبرة التقنية هي:

– وصف تركيب الحاسوب وصناعته وطرازه ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها بالإضافة إلى الأجهزة الملحقة به وكلمات المرور أو السر ونظام التشفير.

– وصف طبيعة بيئة الحاسوب أو الشبكة من حيث التنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائل الاتصالات وتردد موجات البث وأمكنة اختزانها.

– وصف الوضع المحتمل لأدلة الإثبات والهيئة التي تكون عليها.

– التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة، أو المحافظة على دعامتها بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائمها لممغنطة.

– بيان كيفية عزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو إلحاق الضرر بالأجهزة.

– معرفة وسائل وطرق فحص نظام الحاسب الآلي كبرنامج كشف وإزالة الفيروسات وبرامج استرجاع البيانات والمعلومات وإصلاح التلف وإظهار المخفي منها.

– معرفة وسائل نسخ البرامج والملفات وعمل نسخ من القرص الصلب طبق الأصل.

– معرفته لكيفية الربط بين الدليل المادي والدليل الإلكتروني في الوقائع محل البحث[2].

---

[1] -**فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص106.

[2] – **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في الجرائم الكمبيوتر والأنترنت، مرجع سابق، ص 330.

لما كانت عملية تجميع الدليل الإلكتروني من أصعب الأمور التي تواجه الخبير التقني، كان لزوما عليه إتباع كل الخطوات والأساليب العلمية التي تتناسب مع البيئة التي يتواجد بها هذا النوع من الدليل.

ج- خطوات اشتقاق أو اكتشاف الدليل الإلكتروني:

يمكن إيجار خطوات اشتقاق الدليل بمعرفة الخبير المعلوماتى فيما يلي :

1. خطوات ما قبل التشغيل الفحص:

- التأكد من مطابقة محتويات إحراز المضبوطات لما هو مدون عليها.
- التأكد من صلاحية وحدات النظام للتشغيل.
- تسجيل بيانات الوحدات المكونات المضبوطة، كالنوع والطراز أو الموديل، والرقم المتسلسل...الخ.

2. خطوات التشغيل والفحص:

يعتمد عمل الخبير المعلوماتي في سبيل تحري الحقيقة في مجال الجرائم المعلوماتية على جمع مجموعة من الأدلة الإلكترونية وتحصيلها من خوادم المواقع (Les serveurs) من جهاز المعتدي بعد التوصل إلى تحديده، ثم يقوم بعملية تحليل رقمي لها لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه وتحديد عناصر حركتها، ومن ثم التوصل في النهاية إلى معرفة بروتكول الأنترنت IP للحاسوب الذي صدرت منه الرسائل والنبضات الإلكترونية، ويرى بعض المتخصصين أن عمل الخبير المعلوماتي في اشتقاق وتجميع الأدلة الإلكترونية يتم عبر ثلاث مراحل:

المرحلة الأولى: تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة من خلال تتبع الحاسبات الخادمة التي دخل منها المجرم المعلوماتي ومحاولة إيجاد أثر له.

المرحلة الثانية: مرحلة المراقبة ويتم ذلك بطرق مختلفة أهمها استخدام برامج مراقبة يمكن تحميلها للبحث عن المعلومات المشتبه فيها وحصر وتسجيل بيانات كل دخول وخروج بالموقع.

المرحلة الثالثة: فحص النظام المعلوماتي المشتبه فيه بعد ضبطه من طرف جهات التحقيق بمكوناته المادية والمعنوية لاشتقاق الدليل وتقديمه لجهات التحقيق وتقرير مدى وقوع الجريمة باستخدام النظام المضبوط من عدمه[1].

د – تحديد الترابط بين الدليل المادي والدليل الإلكتروني:

يتم في هذه المرحلة فحص كل من الدليل المادي المضبوط والدليل الإلكتروني المستخرج من جهاز الحاسب الآلي الموجود بملفات النظام المضبوط صور نصوص أصوات الخ وبذلك يكون تم الربط بين الدليل الإلكتروني والدليل المادي، مما يكسب الدليل الوثوقية، واليقينية، اللتان تؤديان إلى قبوله لدى جهة الحكم.

❖ تطبيقات عملية لاشتقاق الأدلة في الجرائم المعلوماتية، التزييف والتزوير الإلكتروني[2]:

أحالت النيابة العامة بالقاهرة قضية لقسم أبحاث التزييف والتزوير، بوزارة العدل، متضمنة حرز أوراق العملة المصرية المزيفة فئة عشرون جنيها، وحرز به أوراق تجميع رزم وأحراز النظام الحاسوبي وهو مكون من جهاز الحاسوب محتويا على وحدة المعالجة المركزية، والشاشة، ولوحة المفاتيح والفأرة، وكذا طابعة حاسوبية، وماسح ضوئي، ومجموعة من الأقراص المرنة والأسطوانات، وطلبت النيابة العامة تحديد ما إذا كانت العملات مزيفة من عدمه، تحديد ما إذا كان النظام الحاسوبي تم استخدامه في تزييف العملة المضبوطة من عدمه.

سيركز في هذا العرض على عملية استخلاص الدليل الإلكتروني، والربط بينه وبين الدليل المادي، دون أن عرض عملية فحص العملات الورقية ذاتها والتي أثبتنا بأنها بالرغم من التشابهات بينها وبين العملات الورقية الصحيحة المناظرة، إلا أنها عملات ورقية مزيفة وفق أسلوب التزييف الكلي، عن طريق التقليد باستخدام طابعة حاسوبية ملونة تعمل بتقنية نفث الحبر (INK JET)، لطباعة كل من الوجه والظهر، وذلك على النحو التالي:

---

[1] – **سعيداني نعيم**، مرجع سابق، ص 179.

[2] – **رياض فتح الله بصلة**، حدود الإثبات العلمي في قضايا التزييف والتزوير، دراسة في المفاهيم والأساليب والإجراءات، دار نوبار للطباعة، القاهرة، 2001، ص83.

تم تشغيل الجهاز بعد التأكد من صلاحية أجزائه، وتم فحص وحدات ومكونات النظام، وتسجيل أنوعها وتوصيفها، وأسفرت عملية البحث والفحص للمجموعات البرامجية والملفات الموجودة على القرص الصلب والأقراص المرنة والأسطوانات المدمجة عن الآتي:

-وجود برامج لمعالجة الصور والتي تعمل في بيئة التشغيل النوافذ منها Windows 95 Adope photoshop 5.0

- وجود ملفات وفهارس لصور وجه وظهر عملة ورقية مصرية فئة عشرون جنيها، على القرص الصلب المشغل.

– أن الأقراص المرنة المضبوطة، والأقراص المضبوطة، لم يوجد عليها أية برامج.

لوحظ بمجرد توصيل وصلات النظام بالكهرباء بما في ذلك الطابعة أن الطابعة تعمل وتخرج منها ورقة طبع عليها وجه غير مكتمل من العملة الورقية المصرية فئة عشرون جنيها مع وجود عملية طباعية مكتملة لثلاث صور لظهر عملة ورقية مصرية فئة عشرون جنيهًا بظهر الورقة.

تم تفسير ذلك فنيا وعلميا بالتقرير بأن أخر أمر بالطباعة لم تتمكن الطابعة من إكماله حيث تم فصل الكهرباء بطريقة غير صحيحة عند ضبط أدوات الجريمة.

تم أخذ مخرج طباعي لكل منها من الطابعة المضبوطة، وهو يمثل تفريغ الدليل الإلكتروني في شكل مادي وقد تم إيداعها داخل الحرز الرابع بعد التأشير عليها منا بالنظر وبرقم قيد تقريرنا الحالي.

بعد إجراء التشغيل وعمليتي الفحص والمقارنة بين ورقات العملة الورقية المصرية فئة عشرون جنيها المضبوطة، والعملة – مكتملة الظهر وغير مكتملة طباعة الوجه –، والتي خرجت من الطابعة المضبوطة بمجرد توصيل وصلات وحدات النظام بالكهرباء وهما يمثلان الدليل المادي، ووجه وظهر العملة الورقية المصرية فئة عشرون جنيها المحملة على القرص الصلب هي تمثل الدليل الإلكتروني ثبت الآتي:

– أن بيانات العملة الورقية المحملة بالقرص الصلب المشغل C بالجهاز الدليل الإلكتروني، هي ذاتها التي تحملها ورقات العملة الورقية المصرية فئة عشرون جنيها الدليل .

-الاتفاق في خواص المخرج الطباعي بين ورقات العملة الورقية المصرية فئة عشرون جنيها المضبوطة، وبين المخرج الطباعي للطابعة -للعملة مكتملة الظهر وغير مكتملة طباعة الوجه- والتي

خرجت من الطابعة المضبوطة بمجرد توصيل وصلات وحدات النظام بالكهرباء، هذا من جانب، وبين المخرج الطباعي الذي أخذ بمعرفتنا أثناء فحص وتشغيل الجهاز من جانب آخر.

و- التحفظ على الأدلة:

تتم عملية حفظ الأدلة الإلكترونية داخل الحاسوب بأساليب متعددة تتشكل في أبسط مظاهرها باستخدام أسلوب الحفظ العادي وأقوى مظاهرها[1] في عمليات حجز الحاسوب الدليل الموضوع فيه، ذلك أن الدليل الإلكتروني في العادة ملف يحتوي على بيانات رقمية تعطي مظهرا معلوماتيا محددا غير قابل للتحويل إلى مظهر آخر، إلى حين يتم القيام بإجراء تعديلات رقمية في البيانات المذكورة.

ان عملية حفظ الأدلة في العالم الإلكتروني يتطلب من الخبير التقني القيام برصد موقع الأنترنت في المعلومات التي تشير إلى الجريمة، والتي تكون في مظاهر مختلفة الأشكال، كما لو كانت الجريمة من جرائم القذف والسب في غرفة المناقشة، ففي مثل هذه الحالة الأخيرة يتم اللجوء إلى ذاكرة الخادم الذي يتولى ربط هذه الغرف عبر العالم الرقمي لكي يمكن التوصل إلى تحديد موضوع السب والقذف وتاريخه، وإذا كانت الجريمة من جرائم النشر عبر الأنترنت فقد يكتفي بمجرد اللجوء إلى ذاكرة الحاسوب المستخدم دون حاجة إلى تحديد الخادم، ففي مثل هذه الحالات يقوم الخبير باستخدام برمجيات مساعدة للتوصل إلى القيام بالحفظ في العالم الإلكتروني، كما هو الشأن في حجز وتشفير مثل هذه المواقع بعد تحديد جدليتها ودقتها ومسارها، وهذا أمر يترتب عليه عدم إمكانية حذفها في العالم الرقمي، وإذا قام أحدهم بذلك فإنه يكون قد ارتكب جريمة.

تستدعي عملية حفظ الأدلة في العالم الإلكتروني لزوم قيام الخبير بعرض الأدلة على المحكمة أو على جهات التحقيق، ومثل هذا الأمر يجعل عمل الخبير يستمر لمرحلة المحاكمة

[1]- إنّ التحفظ على الأدلة الإلكترونية من العمليات المعقدة التي تحتاج بداية إلى رصد دقيق لدى صحة البيانات التي يحتوي عليها الحاسوب، وهذا الأمر يستلزم بالضرورة قيام الخبير التقني بالكشف بداية على مدى صحة حركة الحاسوب لاسيما من حيث الخلل والعطب، إذ يكفي أن يكون هناك فيروس في الجهاز لكي يتم التشكيك في صحة الأدلة المستسقاة من هذا الحاسوب.

وأحيانا يتطلب منه ذلك القيام بعمله لمرحلة ما بعد المحاكمة كما هو الشأن حال عرض الدليل المقدم إلى محكمة الموضوع أمام جهة قضائية أعلى كالاستئناف أو النقض.

هـ- مرحلة تدوين النتائج وإعداد التقرير:

يتم إعداد تقرير بجميع خطوات وإجراءات البحث، ويرفق به في الغالب الملاحق الإيضاحية المصورة والمسجلة وغيرها، ثم تصديرها إلى جهة التحقيق أو الحكم.

المبحث الثاني

الإجراءات الحديثة لجمع الدليل الإلكتروني

تبين من الإجراءات التقليدية أنها صعبة الإتباع للحصول على الدليل الإلكتروني، فكان من الضروري على التشريعات المختلفة خلق إجراءات قانونية حديثة لمواجهة هذا الإجرام غير التقليدي وذلك حتى لا يفلت المجرمون من العقاب.

ان المقومات التشريعية التي أرساها المشرع الجزائري ضمن خطته في مكافحة الجريمة المعلوماتية ما جاء به القانون رقم 06-22 من خلال إجرائي التسرب واجراء إعتراض المراسلات ثم من خلال القانون رقم 09-04 استحدث إجراءين آخرين وهما المراقبة الإلكترونية وحفظ المعطيات المتعلقة بحركة السير البيانات في البيئة الافتراضية ليست دائما ساكنة.

المطلب الأول

التسرب

سنحاول في هذا الفرع تحديد مفهوم هذا الإجراء، شروط إجرائه، سير عملية التسرب وأخيرا الآثار المترتبة عنه.

الفرع الأول

مفهوم عملية التسرب

أولا : تعريف عملية التسرب

عرفت التسرب المادة 65 مكرر 12من قانون الإجراءات الجزائية الجزائري، بأنه قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضباط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم.

ان التسرب نظام من أنظمة التحري والتحقيق الخاصة التي تبيح لضباط وأعوان الشرطة القضائية اختراق الجماعات الإجرامية والتوغل في وسطها تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب تحت مراقبة مصدر الإذن "وكيل الجمهورية أو قاضي التحقيق" بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، وذلك بإخفاء المتسرب لهويته وصفته وتقديم نفسه على أنه أحد أفراد العصابة المشتبه فيها بوصفه فاعل أو شريك[1].

نظرا لتعقيدات هذا النظام ومساسه بحرمة الحياة الخاصة قيده المشرع بجملة من القيود احتراما لمبدأ الشرعية وربطه بمجموعة من الجرائم حددتها المادة 65 مكرر 05 من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بحيث لا يسمح بهذا الإجراء.

تتجسد عملية التسرب في الجرائم المعلوماتية كاشتراك ضابط أو عون الشرطة القضائية في محادثات غرف الدردشة أو حلقات النقاش حول دعارة الأطفال مثلا أو كلام يدور حول قيام أحدهم باختراق شبكات أو بث فيروسات، فيتخذ المتسرب أسماء مستعارة ويظهر بمظهر طبيعي كما لو كان فاعل مثلهم ويحاول الاستفادة من معارفهم حول كيفية اقتحام الهاكر لموقع ما، أو مباشرة الحديث في الموضوع الجنسي حتى يتمكنوا من اكتشاف وضبط الجرائم التي تتم من خلالها كالدعارة مثلا[2].

---

[1] – **علاوة هوام**، "التسرب كآلية للكشف عن الجرائم في قانون الإجراءات الجزائية الجزائري"، مجلة الفقه والقانون، العدد الثاني، ديسمبر 2012، ص2، محمول من الموقع الإلكتروني التالي:-http://taza2005.e monsite.com/medias/files/tasarrob.pdf، تم الاطلاع عليه يوم: 2016/03/14.

[2] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 74.

ثانيا: شروط صحة عملية التسرب

نظرا لأهمية التسرب ومساسه بحريات الأفراد فقد وضع له المشرع شروطا يجب مراعاتها والتقيد بها احتراما لمبدأ الشرعية من جهة وحرصا على حياة المتسرب وتسهيلا للمنفذين بلوغ الأهداف، والمتمثلة في الاتي:

أ- **الإذن بإجراء التسرب:** قبل مباشرة الإجراء يتعين أن يصدر إذنا بالقيام بعملية التسرب من الجهات القضائية التي حددتها المادة 65 مكرر 11 قانون الإجراءات الجزائية الجزائري والمتمثلة في وكيل الجمهورية أو قاضي التحقيق[1]، مع توفر الشروط التي حددتها المادة 65 مكرر 15 من القانون نفسه وهي الكتابة والتسبيب.

ب- **التسبيب:** حتى يكون الإذن قانونيا اشترط المشرع في المادة 65 مكرر 15 قانون الإجراءات الجزائية الجزائري أن يكون مكتوبا ومسببا، لأن التسبيب هو أساس العمل القضائي فكان لزاما على رجل القضاء المختص بإصدار الإذن بالتسرب أن يسببه وذلك بإبراز الأدلة القانونية والموضوعية بعد تقدير جميع العناصر الواردة في تقرير ضابط الشرطة القضائية، تقتضي عملية التسرب أن تحاط بالسرية التامة وقد نص قانون الإجراءات الجزائية على جزاءات عقابية مشددة في حالة كشف هوية المتسرب وتعدت هذه الحماية إلى عائلة المتسرب وحددت العقوبات في المادة 65 مكرر 16 من سنتين إلى عشرين سنة حبس مع الغرامة من 50 ألف إلى مليون دينار جزائري.

ج-**نوع الجريمة:** ينبغي أن يتضمن الإذن الصادر عن السلطة القضائية وكيل جمهورية أو قاضي التحقيق نوع الجريمة التي بررت اللجوء إلى التسرب وأن تكون من الجرائم التي حددتها المادة 65 مكرر 5 قانون الإجراءات الجزائية الجزائري. سكت قانون الإجراءات الجزائية عن الجرائم العرضية ولم يشر إليها في أحكام التسرب، غير أنه وباستقراء المادة 65 مكرر 6 قانون الإجراءات الجزائية الجزائري تنص على أنه إذا وقع اكتشاف جرائم أخرى غير تلك المنصوص عليها في إذن القاضي، فإن ذلك لا

[1]- يلاحظ أن المشرع الجزائري أسند مهمة إصدار إذن التسرب إلى وكيل الجمهورية أو قاضى التحقيق بعد إخطار وكيل الجمهورية، بمعنى أن المشرع خرج عن الأصل العام في التحقيق القائم على الفصل بين سلطتي الاتهام والتحقيق، وذلك أن وكيل الجمهورية مهمته الأساسية هي تقديم المتهم إلى العدالة، ومن الصعوبة أن يتجرد من صفته الاتهامية عندما يقوم بإصدار الترخيص بالتسرب، خاصة وان طبيعة عملية التسرب فيها نوع من الخطورة على حرمة الحياة الخاصة للأفراد لاسيما الحق في الخصوصية، لذلك فالأفضل منح هذه المهمة إلى قاضى التحقيق لما له من استقلالية وحسن التقدير ما يطمئن معه الأفراد.

يكون سببا لبطلان الإجراءات العارضة ورغم أن نص المادة 65 مكرر 6 جاء ذكره في الفصل المتعلق باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، إلا أنه وباعتبار التسرب تدبير له ميزة خاصة وأن المشرع قد أولى عناية كبيرة بمصلحة التحقيق وغلب المصلحة العامة على المصلحة الخاصة فإنه وبالنظر إلى الحلقة المشتركة بين جميع التدابير المنصوص عليها بالمادة 65 قانون الإجراءات الجزائية الجزائري والمتعلقة بالجرائم الماسة بأمن الدولة أمكن القول أن اكتشاف جريمة عرضية عند مباشرة عملية التسرب يخضع لإجراءات عارضة ولا يمكن أن يكون ذلك سببا للبطلان، فمتى اكتشف المتسرب بخلية المتاجرة بالمخدرات جريمة قتل وجب عليه رفع تقرير إلى المشرف عليه ليحوله إلى وكيل الجمهورية لاتخاذ ما يراه مناسبا[1].

تجدر الإشارة أن صياغة هذه الأفعال مأخوذة من المادة 706-32 من قانون الإجراءات الجزائية الفرنسي، وذلك في إطار مكافحته جريمة الإتجار غير مشروع للمخدرات[2]، أمام تسخير الوسائل المادية والقانونية.

د- إبقاء الإذن بالتسرب خارج ملف الإجراءات: حفاظا على السرية اللازمة لتنفيذ الإجراء والمحصورة بين وكيل الجمهورية أو قاضي التحقيق وضباط الشرطة القضائية المشرف على العملية وكذا العون المتسرب إلى غاية الانتهاء من العملية.

هـ-تنفيذ عملية التسرب: قبل البدء في تنفيذ إجراء التسرب يلزم القانون ضابط الشرطة القضائية المسؤول والمنسق للعملية أن يحرر تقريرا يضمنه العناصر الأساسية والضرورية لمعاينة الجرائم، مع مراعاة تلك الجرائم التي يمكن أن تشكل خطرا على العون المتسرب وكل ما يتم تسخيره لتنفيذ العملية وفق ما يراه مناسبا ومساعدا على التنفيذ. استنادا لنص المادة 65 مكرر 12 فإن مسؤولية سير عملية التسرب تقع على عاتق ضابط الشرطة القضائية الذي يتولى عملية التنسيق والتفكير والتحضير والتنظيم وكل ما يترتب عن ذلك من إجراءات.

و- تحديد مدة عملية التسرب في الإذن: والتي يمكن أن تتجاوز 4 أشهر، ويمكن أن تجدد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية، وفي نفس الوقت أجاز

[1] - **علاوة هوام**، مرجع سابق، ص 6.

[2] - Article 706-32 du Code de procédure pénale Français, cité précédemment.

القانون للقاضي الذي رخص بإجرائه أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة.

الفرع الثاني

الحماية القانونية للعون المتسرب

نتيجة لخطورة عملية التسرب على القائم بها، كفل له القانون حماية خاصة وأولاه الرعاية للحفاظ على أمن وسلامة روحه وسرية مهمته، إذ جعل المتسرب بمنأى عن تحمل المسؤولية الجزائية[1] عن الجرائم التي يكون قد ارتكبها عرضا أثناء تسربه تنفيذا للمهام الموكولة إليه، ومنع الكشف عن هويته الحقيقية وسمح له بأخذ هوية مستعارة، ورتب على مخالفة هذه الإجراءات عقوبات جزائية تتضاعف إذا أفضى هذا الكشف للهوية عن تعرض المتسرب أو أحد أفراد عائلته للضرب أو الجرح أو عرض حياته للخطر المادة 65 مكرر 16، وقد تتضاعف إذا حدثت الوفاة.

تعد من الحماية الخاصة للمتسرب عدم جواز سماعه كشاهد على العملية مع جواز ذلك بالنسبة للضابط المسؤول والمنسق، وإذا حدث أن وقع توقيف العملية أو انقضى أجلها دون تجديد فإن ضرورات حماية المتسرب تجيز له مواصلة نشاطه من دون تحمله لأي مسؤولية بشرط إخبار الجهة مصدرة الإذن، على أن لا تتجاوز فترة تأمين سلامة المتسرب مدة أربعة أشهر قابلة للتجديد مرة واحدة[2].

لقد أجاز المشرع في المادة 65 مكرر 14 قانون الإجراءات الجزائية الجزائري اقتناء 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 وكذا استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال وبالتالي يمكن للعون المتسرب استعمال الأموال المتحصل عليها من ارتكاب الجرائم

---

[1] – نصت المادة 65 مكرر 14 قانون الإجراءات الجزائية الجزائري على أن الضابط وأعوان الشرطة القضائية المسخرين في عملية التسرب لا يكونون مسؤولين جزائيا حسب الحالات التي ذكرها النص وهذه الحالات تعد تكريسا للمادة 39 قانون الإجراءات الجزائية الجزائري بحيث يصبح التسرب من ضمن أسباب الإباحة، مع ملاحظة أنه لا يجوز له تحت طائلة البطلان أن يتخذ من الأفعال المسموح له بها تحريضا على ارتكاب جرائم.

سكت المشرع الجزائري عن المسؤولية المدنية التي يقصد بها هنا كل التصرفات المدنية أو التجارية التي يقوم بها العون المتسرب كإبرام عقود ترتب التزامات كعقد بيع أو توريد أو مقارنة بذلك يبقى السؤال المطروح ما مصير العقود التي أبرمها المتسرب لتنفيذ مهمته بعد انتهاء العملية؟

[2] – **علاوة هوام**، مرجع سابق، ص 4.

المذكورة بنص المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري ومن هنا يمكن القول أن هناك استثناء لأحكام نص المادة 02 من القانون رقم 05-01[1] المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما الذي يعتبر العائدات الإجرامية عند عمله بها سواء بالتحويل أو النقل أو الاكتساب أو الحيازة تبييضا للأموال.

أما الوسائل القانونية فيقصد بها توفير الوثائق الرسمية إن كان هناك ضرورة – رخصة سياقة – بطاقة تعريف – جواز السفر – بطاقة رمادية...الخ، ولهذا يحتاج القائم بالعملية إلى أجهزة التزوير لعدم إمكانية المرور على الإدارة ضمانا للسرية.

المطلب الثاني

الإجراءات المتعلقة بالتخزين الإلكتروني

إن الإجراءات المتعلقة بالبيانات المتحركة كلها مستوحاة من اتفاقية بودابست التي تتكون هذه الاتفاقية من 48 مادة تم توزيعها على أربعة أبواب، يدرس فيها الجانب الإجرائي منها، حيث يدرج إجراء التحفظ المعجل على البيانات المخزنة (الفرع الأول) ومسؤولية المتدخلين في شبكة الأنترنت بتقديم بيانات معلوماتية متعلقة بالمشترك (الفرع الثاني).

الفرع الأول

التحفظ المعجل على البيانات المخزنة

تنص إتفاقية بودابست السالفة الذكر في المادة 16، أنه من الضروري على كل دولة طرف في الاتفاقية السماح لسلطاتها المختصة أن تأمر أو تفرض بطريقة أو بأخرى مزود الخدمة التحفظ العاجل على البيانات المعلوماتية المخزنة بما في ذلك البيانات المتعلقة بالمرور المخزنة بواسطة نظام المعلوماتي، وذلك عندما تكون هناك أسباب تدعو للاعتقاد بأن هذه البيانات على وجه الخصوص معرضة للفقد أو التغيير، وذلك خلال 90 يوم كحد أقصى، وهذه المدة قابلة للتمديد.

[1]– قانون رقم 05-01 مؤرخ في 27 ذي الحجة 1425 الموافق 6 فبراير 2005 يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية للجمهورية الجزائرية عدد 11 بتاريخ 9 فبراير 2005.

أولا :مفهوم التحفظ المعجل على البيانات المخزنة

يقصد به توجيه السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته، في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش، أو الأمر بتقديم بيانات معلوماتية[1].

حددت اتفاقية بودابست الأسباب التي تدعو إلى اتخاذ مثل هذا الإجراء، وذلك للمبررات التالية:

– قابلية البيانات المعلوماتية للتلاشي، حيث يكون محلا للمحو أو التغيير سواء كان ذلك بدافع إجرامي لطمس معالم الجريمة أو أي عنصر إثباتي لشخصية المجرم.

-غالبا ما يتم ارتكاب الجرائم المعلوماتية عن طريق نقل الاتصالات عبر نظم الحاسوب.

– تأمين الدليل الإلكتروني من الضياع والفقد بسرعة.

يعد إجراء التحفظ المعجل على البيانات المخزنة بالنسبة للجزائر أداة تحقيق مستحدثة في إطار مكافحة الجرائم المعلوماتية، حيث ألزم على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها –وفقا للمادة 11 من القانون 09–04– تحت تصرف السلطات المذكور، .ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[(2)].

نص المشرع الأمريكي على هذا الإجراء في القسم(F)2703 18U.S.C من قانون خصوصية الاتصالات المعلوماتية الأمريكي (A P C E)، على أنه يمكن لرجال الضبط القضائي في إطار ما يقومون به من جمع الاستدلالات الاطلاع على البيانات الموجودة في حوزة مزودي الخدمات، والتي تخص مستخدمي شبكة الأنترنت، وذلك من خلال توجيه تكليف إلى مزود

[1] - **عائشة بن قارة مصطفى**، مرجع سابق، ص100.

[2] – المادة 10 من **القانون رقم 09–04** سالف الذكر.

الخدمات للتحفظ على سجلات موجودة في انتظار اتخاذ إجراء قانوني إجباري[1]. تتمثل هذه السجلات في ثلاث طوائف هي:

– المعلومات الشخصية الخاصة بالمشترك مثل اسمه، عنوانه... الخ.

– المعلومات الشخصية الخاصة بالمتعامل مع المشترك (أي كل من يتصل به).

– المعلومات المتعلقة بمحتوى البيانات مثل مضمون المحادثات أو مضمون الملفات[2].

ثانيا : الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك

تنصت المادة 18 من اتفاقية بودابست على « يجوز للدول الأطراف في الاتفاقية تمكين السلطات المختصة من إلزام مقدمي الخدمات تقديم البيانات المتعلقة بالمشترك، سواء كانت في حيازته المادية أو تحت سيطرته حيث تكون هذه البيانات مخزنة بعيدا عن الحيازة المادية لمزود الخدمات ».

ينبغي تحديد السلطة المختصة بإصدار أمر تقديم البيانات، الملاحظ أن التشريعات ذات الأصل اللاتيني مثل القانون الفرنسي[3] والجزائري تختلف عن القانون الأمريكي، إذ لا تجيز تلك التشريعات أن يصدر رجل الضبطية القضائية مثل هذا الأمر، وإنما تجيزه لسلطة التحقيق[4]، فيسمح لرجال السلطة العامة بإصدار مثل هذا الأمر، إذا تعلق الأمر ببيانات المشترك المعلنة للجمهور، في حين أن دولا أخرى لا تشترط أن يكون هذا الأمر صادرا فقط من السلطات

---

[1]– قد عرفت اتفاقية بودابست السالفة الذكر، مزود الخدمات في المادة الأولى فقرة (ج) بأنه " كل من يقوم بخدمات الاتصال 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 ".

[2]– تجدر الإشارة إلى أن البيانات المعلوماتية المشمولة بالأمر تتضمن بينها بيانات المرور المتعلقة باتصالات سابقة، وذلك من أجل تحديد خط سير الاتصال بمعنى مصدر أو مكان وصول هذه الاتصالات والتي تعد من الأمور الجوهرية للتعرف على هوية الأشخاص الذين قاموا بتوزيع مواد إباحية طفولية مثلا. **عائشة بن قارة مصطفى**، مرجع سابق، ص101.**أشرف عبد القادر قنديل**، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015، ص 180.

[3]– أنظر القوانين التالية:

Loi n° 2000-719 du 1 août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, in ;
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000402408
Loi N° 2001-1062 du 15 Novembre 2001 relative à la sécurité quotidienne, chapitre 5, Article 9, in ;
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052.

[4] - **عائشة بن قارة مصطفى**، مرجع سابق، ص102.

القضائية، عند الحصول على نوعية معينة من البيانات المتعلقة بالحق في الخصوصية، مثل رقم بطاقة ائتمان بنكي.

حددت الاتفاقية السالفة الذكر المقصود بتلك البيانات، بقولها أنها تتعلق بـ:

– نوع خدمة الاتصال التي اشترك فيها الشخص والوسائل الفنية لتحقيقها.

– العنوان البريدي أو الجغرافي ورقم تلفون المشترك.

– رقم دخول المشترك للحصول على تلك الخدمة والفواتير التي ترسل إليه[1].

أن قانون الإجراءات الجزائية المقارن يأخذ في الاعتبار الكيفية التي يتم بها التراسل، دون أهمية لعامل الوقت، بحيث يعد زمن الاتصال يبدو كما لو لم يكن له قيمة في هذا الشأن، إذ عديدة هي النصوص التي لا تشترط الكتابة، مثل الفاكس والاتصالات الهاتفية، ومن ذلك ما هو مقرر في تشريع أحد الولايات المتحدة الأمريكية وهي ولاية أركانساس ARK Code amn. §5-41-108 (2000) الذي يعترف بارتكاب جريمة التخويف أو الترهيب أو التهديد أو الإساءة ضد أي شخص باستخدام البريد الإلكتروني أو أية وسيلة اتصال أخرى[2].

يثار في هذا الخصوص مشكلة تحديد طبيعة البريد الإلكتروني غير المفتوح والمنتظر في صندوق خطابات مقدم خدمات الأنترنت حتى يقوم المرسل إليه بإدخالها في نظامه المعلوماتي واستردادها[3]،حيث يعد اختراق البريد الإلكتروني والاطلاع على فحواه عدوانا وانتهاكا لقاعدة سرية الاتصالات بين الأفراد، فهل يجب اعتبار هذه بيانات معلوماتية مخزنة وبالتالي تطبق عليها الإجراءات المتعلقة بالبيانات الساكنة أم أنها بيانات في مرحلة النقل والتحويل وبالتالي تطبق عليها الإجراءات المتعلقة بالبيانات المتحركة والمتمثلة في اعتراض الاتصالات الإلكترونية؟

---

[1] – **أشرف عبد القادر قنديل**، مرجع سابق، ص 182.

[2] – ***Arkansas*** Code AMN. §5-41-108 (2000) ,in ; https://law.justia.com/codes/arkansas/2010/title-5/subtitle-4/chapter-41/subchapter-1/5-41-108/

[3] – **Jean Claude PATIN**, la surveillance des courriers électroniques par l'employeur, revue du droit des technologie de l'information, 1999,p2, in ; lthoumyre.chez.com/pro/1/priv19990810.htm.consulter le 19/06/2017

حسم المشرع الأمريكي هذا الأمر، واعتبر الاتصالات الإلكترونية المخزنة من قبل البيانات الساكنة، وبالتالي تطبق عليها كل الإجراءات التي تتناسب مع هذا النوع من البيانات من تفتيش والأمر بالتحفظ العاجل وتقديم هذه البيانات، بدليل أنه قام بتعديل القسم 2703 من قانون خصوصية الاتصالات الإلكترونية (A P C E)، ليشمل حماية الاتصالات الإلكترونية المخزنة من بريد إلكتروني، والرسائل الصوتية غير مفتوحة والمخزنة لدى مزود الخدمة، وقد تم تأكيد هذه القاعدة في العديد من التطبيقات القضائية مثل قضية United States V. Smith، حيث قرر القضاء بأنه لا يمكن مراقبة الاتصالات السلكية وهي في حالة التخزين الإلكتروني[1].

الفرع الثاني

مسؤولية المتدخلين في شبكة الأنترنت

سيتم التطرق إلى المقصود بالمتدخلين في شبكة الأنترنت بما فيهم مزودي الخدمات باعتباره الحائز لهذه البيانات ومدى التزامه بالتعاون مع سلطات التحري والتحقيق وتحديد مسؤوليتهم، كذلك موقف بعض التشريعات المقارنة من المسؤولية القانونية لمقدمي خدمات الأنترنت، كما يلي:

أولا: المقصود بالمتدخلين في شبكة الأنترنت وتحديد مسؤوليتهم

تعددت الأجهزة المتدخلة في شبكة الأنترنت، وفيما يلي سرد لأهما، كما يلي:

أ- متعهدي الوصول: هو مقدم الخدمات الفنية والذي يدير الآلة المتصلة فعلا بالأنترنت ويتيح للمستخدم الوصول إلى الشبكة، فمتعهد الوصول يقدم خدمات من طبيعة فنية، تتمثل في ربط المشتركين بالمواقع أو المستخدمين الآخرين بالشبكة، وذلك عن طريق وضع الحاسب الخادم الخاص به – الذي يرتبط بصفة دائمة بالأنترنت – تحت تصرف المشتركين، بحيث يسمح لهم بأن يتجولوا في هذه الشبكة، أو يدخلوا إلى المواقع ويتبادلون الرسائل الإلكترونية.

ان متعهد الوصول مجرد ناقل المعلومات، فهو لا يسأل عن تصرفات مستخدمي الشبكة (المشتركون)، ولا يسأل عن محتوى المعلومات التي قام بتوصيل المستخدمين بها، لأنه يكون

[1] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 105.

بمثابة ناقل في حالة البريد الإلكتروني، وسرية الاتصالات عن بعد تحظر عليه الاطلاع على المراسلات، وذلك باستثناء ما ينص عليه المشرع من حالات، ومع ذلك يمكن أن يسأل متعهد الوصول إذا كان يعلم أن هناك رسالة غير مشروعة ولم يتدخل من أجل منع الاستمرار في نشرها (وإن كان من الصعب إثبات العلم)، ولكن من الصعب توافر مسؤولية متعهد الوصول بشأن مراقبة مشروعية مواقع الويب لأنها تتجاوز الألف موقع وتتغير يوميا.

كما أن متعهد الوصول لا يملك الإمكانيات التقنية اللازمة لمحو المعلومات غير المشروعة التي يتم إيوائها على حاسبات خادمة تقع – غالبا – خارج إقليم دولته، وليس لمتعهد الوصول الحق في كل المعلومات التي تعتبر مشروعة في دولة البث، وبالنسبة لمنع الوصول إلى المعلومات غير المشروعة، فإن التقنيات التي توجد حاليا لتحقيق هذا الهدف غير فعالة.

ب– متعهد الإيواء: هو الذي يسمح بالوصول إلى الموقع من خلال شبكة الأنترنت، وهي عبارة عن شركة تجارية أو أحد أشخاص القانون العام، يعرض إيواء صفحات الويب على حاسباته الخادمة، ويتم ذلك غالبا في مقابل أجر، لتأجيره مكان على الويب للمستأجر (الناشر)، الذي ينشر عليه ما يريده من نصوص، صور، مؤتمرات، روابط معلوماتية مع مواقع أخرى.

لكن متعهد الإيواء له سلطة مراقبة محتوى ملفات صفحات الويب التي تسلم إليه، فإذا ثبت أن المعلومات التي تسلمها غير مشروعة فإن ذلك يستتبع قيام مسؤوليته، وغالبا ما ترفع الدعاوى ضد متعهد الإيواء لسهولة تحديد هويته.

ج– ناقل المعلومات: هو العامل الفني الذي يقوم بالربط بين الشبكات، فالناقل يؤمن – بموجب عقد – نقل المعلومات في هيئة حزم من جهاز المستخدم إلى حاسب الخادم لمتعهد الوصول، ثم نقلها من هذا الحاسب الأخير إلى الحاسبات المرتبطة بمواقع الأنترنت أو بمستخدمي الشبكة الآخرين، وذلك من خلال الحاسبات الموصلة، وقد يكون الناقل شخصا طبيعيا أو معنويا يستغل شبكة الاتصالات عن بعد المفتوحة للجمهور، ويورد لهم خدمة الاتصالات عن بعد (مثل

شركة التليفون)، ولا يسأل عن المعلومات الغير مشروعة التي تمر من خلال الشبكة، إلا إذا كان يعلم بالطابع غير المشروع وذلك على غرار متعهد الوصول[1].

د-مورد المعلومات: هو الشخص الذي يقوم بتحميل الجهاز أو النظام بالمعلومات التي قام بتأليفها أو جمعها حول موضوع معين، وبالتالي له سيطرة كاملة على المعلومات التي يقوم ببثها بواسطة الشبكة، ومن ثم يتحمل مسؤولية احترام القانون بالنسبة للمعطيات التي يقدمنها إلى المستخدمين الذين يتلقونها.

هـ- مؤلف الرسائل: هو المسؤول الأول عن المعلومات غير المشروعة التي تتضمنها الرسالة، فمستخدم شبكة الأنترنت يجب أن يسأل جنائيا عن عبارات القذف والسب التي يرسلها أو ينشرها على أحد المؤتمرات، ويسأل مدير النشر كفاعل أصلي والمؤلف كشريك، نظرا أن الأول موسرا، والثاني في الكثير من الأحيان لا يمكن الوصول إليه لتقديم أنفسهم باسم مستعار.

أما مورد الرسائل الفنية، فهو الذي يقوم بإدخال المعلومات في الخط، إلا أنه لا يتدخل في الخدمة ولا يمارس رقابته عليها، والمعلومة تمر في لحظة ومن ثم لا يسأل جنائيا عن المعلومات غير المشروعة التي تعبر شبكة الأنترنت .

و- مستخدمي الأنترنت : هو الشخص الذي يرتبط بالشبكة (أو الخادم المعلوماتي لمتعهد وصول الأنترنت) بواسطة خط تليفوني عادي، بهدف الحصول على المعلومات أو بثها أو تبادلها من خلال الحاسب الآلي الخاص به، وبالتالي يمكن أن يكون هو مورد المعلومات، ومن ثم تنعقد مسؤوليته عن الرسائل الخاصة التي يقوم ببثها. فهو لا يقتصر في أدائها على طائفة معينة من المتعاملين معه بمقتضى عقد العقود[2].

ز- متعهد أو مزود الخدمات: يسمى كذلك ناشر الموقع، وهو المسؤول الأول عن المعلومات التي تعبر من خلال الشبكة، لأنه الوحيد الذي يملك سلطة حقيقية لمراقبة المعلومات

---

[1] - **فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص 550.

[2] - **فتحي محمد أنور**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص 553.

والبث، يلتزم متعهد الخدمة – كقاعدة عامة – بحسن تنفيذ الخدمة المعلوماتية، مما يتفق مع أعراف المهنة، ويلتزم أيضا بالإعلام عن وسائل الدخول إلى الخدمة، مثل شفرة تحقيق الهوية، ويقوم بمراقبة محتوى الرسائل التي تصل إليه ويقرر عدم نشر تلك التي يقدر أنها غير مشروعة، وسلطة المراقبة هذه هي المقابل لمسؤوليته كمدير للنشر عن جرائم الصحافة التي تتضمنها بعض الوسائل.

يقوم مورد الخدمات بوظائف مختلفة منها: ممون المعلومات، مالك حاسب الخادم، متعهد وصول، متعهد خدمات، محترف البث، يمكن أن تتعدد مسؤوليته التعاقدية والجنائية بالنسبة للمعلومات الكاذبة أو الناقصة التي قام بإعدادها ونشرها على موقعه.

عرفت المذكرة التفسيرية لاتفاقية بودابست مزود الخدمات في المادة الأولى فقرة 8 بأنه «كل من يقوم بخدمات الاتصال أو خدمات معالجة البيانات أو خدمات تخزين البيانات، وقد يكون جهة عامة أو جهة خاصة، وقد يقدم خدماته للجمهور أو لمجموعة من المستخدمين اللذين يشكلون مجموعة مغلقة كشركة أو مؤسسة مثلا ».

يعرف قانون خصوصية الاتصالات المعلوماتية الأمريكي (A P C E) [1] في القسم 2 18U.S.C 2703(C)نوعين من مزودي الخدمات النوع الأول: مزودو خدمة الاتصالات الإلكترونية، ويقصد به كل من يقدم خدمة إلى مستخدمي الشبكة والتي تتمثل في تسهيل إرسال واستقبال الاتصالات السلكية والإلكترونية. النوع الثاني هو مزود خدمة معالجة المعلومات عن بعد، يقصد به كل من يقدم للجمهور خدمة معالجة البيانات عن بعد بوسيلة من وسائل الاتصالات الإلكترونية.

عرفه المشرع الفرنسي في المادة 43 – 8 من قانون رقم 2000–719 بأنه الذي « يقوم بمقابل أو بدون مقابل بتخزين المباشر والدائم لإشارات أو مكاتب أو صورا أو رسائل من أي نوع يمكن الحصول عليها توضح تصرف الجمهور ».

[1]- **Electronic Communications Privacy Act** of 1986" ,in ;
https://www.loc.gov/law/opportunities/PDFs/ElectronicCommunicationsPrivacyAct-PL199-508.pdf .

بناء عليه إذا أرسل شخص لشخص آخر رسالة عن طريق البريد الإلكتروني فإنها تمر بالضرورة بمزود خدمة الاتصالات الإلكترونية[1]، وقبل أن يتلقاه المرسل إليه، تظل مخزنة لدى مزود الخدمات، فإذا تلقاها المرسل إليه، فإن موقف هذا الأخير يتراوح بين أمرين:

أن يقوم بمسح تلك الرسالة أو أن يقوم بتخزينها، في هذا الفرض الأخير تعتبر الرسالة مخزنة لدى مزود خدمة الاتصالات الإلكترونية.

أما المشرع الجزائري، فقد عرف مقدم الخدمات في المادة 2 فقرة "د" من قانون الجزائري رقم 09-04 السالف الذكر على أنه، أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة . وتتمثل التزاماته في تلك التي نصت عليها المادّة 11، والمتمثلة في حفظ:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا 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 الاتصال وتحديد مكانه.

ثانيا: موقف بعض التشريعات المقارنة من المسئولية القانونية لمقدمي خدمات الأنترنت

إنّ مسئولية مقدمي خدمات الأنترنت قد تعرضت لها العديد من التشريعات المختلفة، يذكر البعض منها على النحو التالي:

[1] - **عبد الفتاح محمود كيلاني**، مدى المسؤولية القانونية لمقدمي خدمة الأنترنت، ص 476، محمول من الموقع الإلكتروني التالي، http://www.flaw.bu.edu.eg/flaw/images/part2.pdf، تم الاطلاع عليه يوم: 2014/09/06.
محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2003، ص 209.

أ- التوجيه الأوربي الخاص بالتجارة الإلكترونية:

الصادر في 17 جوان 2000 [1] الذي تضمن في المبحث الرابع المواد من 12الى15، وقد أقرت نصوص هذا التوجيه عدم التزام الوسطاء الفنيين برقابة مشروعية المعلومات والإعلانات التي تبث عبر الموقع وإنما فرضت عليهم أن يتصرفوا بشكل مناسب لمنع الوصول إلى هذا –المحتوى غير المشروع، وان المادة 1/12 من ذات التوجيه أعفت مزود الخدمة الوسيطة مشار إلية الأنترنت من المسئولية عن الأعمال غير المشروعة التي يتضمنها الموقع إذا توافرت الشروط الآتية:

ألا يكون مصدر الضرر، ألا يكون قد اختار المرسل إليه الذي ينقل إليه المعلومات، ألا يختار المعلومات التي يقوم بنقلها أو يعدل فيها[2]، وتنص الفقرة الثانية من ذات المادة على إن عمل مزود الخدمة يتضمن تخزين مؤقت للمعلومات التي يقوم بنقلها بيد أن هذا التخزين المؤقت لا يجعله مسئولا ولا يجعل عمله يرقى إلى عمل متعهد الإيواء، ومن ثم لا يسأل. وتجيز الفقرة الثالثة من المادة أن تنص في قوانينها الداخلية على التزام مزود الخدمة بأن يوقف الخدمة ويستبعد المحتوى غير المشروع للموقع.

ب- التشريع الفرنسي:

إنّ القانون الصادر في21 جوان 2004 الخاص بالثقة في الاقتصاد الرقمي[3] والذي يعد احدث القوانين الأوربية في هذا المجال خصص المواد من 5 إلى 9 في الفصل الثاني منه لتنظيم عمل المؤديين الفنيين، وفقا للمادة 6 فقرة 1 الأشخاص الذين يقتصر عملهم على تقديم خدمة الاتصال عبر الأنترنت ويقصد بذلك مزود الخدمة، يجب أن يخطروا المشتركين في الخدمة عن وجود وسائل تقنية تسمح بغلق الخدمة أو توقع جزاءات عليهم إذا توافرت شروط توقيعها وأكدت الفقرة السابعة من هذه المادة إن مزودي

[1]- Directive 2000/31/CE du parlement européen et du conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, in ; http://www.pedz.uni-mannheim.de/daten/edz-wf/gdm/00/R-2000-31-EG-FR.pdf. consulté le: 22/05/2016.

[2] – راجع كل عن: **شريف محمد غنام**، مرجع سابق، ص 148. **محمد حسين منصور**، مرجع سابق، ص 194.

[3] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164.

الخدمة ليس عليهم التزام بالإشراف والرقابة على مضمون البيانات التي يقومون بنقلها كما أنهم غير ملتزمين بالبحث عن الوقائع التي تشير إلى الأنشطة غير المشروعة.

ج- التشريع الأمريكي:

تتضمن نصوص القانون الأمريكي لحماية حق المؤلف عبر شبكة الأنترنت[1] الذي صدر في 28 أكتوبر 1998 ودخل حيز النفاذ في 1 أكتوبر 2000 وقد نص في المادة 5/2 منه التي تبرأ مزود الخدمة الذي يقتصر دوره على مجرد نقل بسيط للمعلومات من الغير إلى الموقع من أية مسئولية ناتجة عن المحتوى غير المشروع لهذه المعلومات.

د- التشريع البريطاني:

أصدر المشرع البريطاني تشريع خاص بتنظيمات التجارة الإلكترونية[2] الذي دخل حيز التنفيذ في 23 أكتوبر 2002 ففي هذا القانون نقلت أحكام التوجيه الأوربي في المواد 12، 13، 14 المتعلقة بمسئولية مزود الخدمة ومتعهد الإيواء.

هـ- التشريع الألماني:

صدر في 1أوت1997 قانون ينظم الاتصالات والمعلومات ويطلق عليه "TDG"الذي يعد في الواقع نقطة البداية التي انطلق منها التوجيه الأوربي للتجارة الإلكترونية الصادر عام 2000 في تنظيمه لمسئولية الوسطاء الفنيين عبر الشبكة، وتنص المادة 5 الفقرة 3 منه على إعفاء مزود الخدمة – الذي يقتصر دوره على مجرد توفير وسيلة الاتصال بالموقع- من المسئولية عن عدم مشروعية البيانات والمحتوى غير المشروع للموقع[3]. يرى بعض الفقه أن القانون الألماني يشابه مزود الخدمة بالمسئول عن الاتصالات التليفونية للموقع[4] والعناوين الجديدة، وتكون هذه الأنظمة الرقابية إضافية

---

[1]U.S. Code , Title 17 , Chapter 5 , § 51,**Online Copyright Infringement Liability Limitation Act** 1998, in ; https://www.law.cornell.edu/uscode/text/17/512.

[2] **The Electronic Commerce Directive Regulations** 2002,in ; http://www.legislation.gov.uk/uksi/2002/2013/pdfs/uksi_20022013_en.pdf.

[3]-**ALAIN Strowel, NICOLAS Ide**, "Responsabilité des intermédiaires actualités.: législatives et jurisprudentielles", revue Droit et Nouvelles Technologies10/10/2000 ,p16 , in ; https://www.droit-technologie.org/wp-content/uploads/2016/11/annexes/dossier/26-1.pdf..consulté le :06/06/2017

[4] – مأخوذ عن: **شريف محمد غنام**، مرجع سابق، ص326.

ومكملة للأنظمة الرقابية لدى مزودي خدمة الأنترنت، والالتزام بتسجيل البيانات الأساسية لمستخدمي خدمات الأنترنت، ومنع تقديم أي من خدمات الأنترنت لمن هم دون سن الثامنة عشرة، أن هذا التشريع موفق لتمشية مع أحكام الشريعة الإسلامية والتطور التكنولوجي الحديث.

و- التشريع الجزائري:

جاء في المادّة 12 زيادة على الالتزامات المنصوص عليها في المادة 11، يتعين على مقدمي خدمات "الأنترنت "، التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن، وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها. كما أضافت المادة 11 فقرة "ه" دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة 6 أشهر إلى خمس 5 سنوات وبغرامة من 50.000دج إلى 500.000 دج.،و يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

المطلب الثالث

الإجراءات المتعلقة بالبيانات المتحركة

يقصد بالإجراءات المتعلقة بالبيانات المتحركة إعتراض الاتصالات الإلكترونية الخاصة وإجراء المراقبة عليها أثناء بثها بين أطراف الاتصال، عكس الإتصالات إلكترونية مخزنة، ذلك أن لكل من النوعين قواعد خاصة بها، من حيث صرامة الحصول عليها في الأولى وخفتها في الثانية.

سيحاول تناول هذا المطلب في فرعين التاليين:

الفرع الأول

اعتراض الاتصالات الإلكترونية السلكية واللاسلكية

ميزت اتفاقية بودابست بين نوعين من البيانات المعلوماتية محل الاعتراض، بين البيانات المتعلقة بالمرور والبيانات المتعلقة بمحتوى الاتصال، وبالنسبة للنوع الأول، جاءت المادة الأولى من الاتفاقية على أنها كل البيانات التي تعالج الاتصالات التي تمر عن طريق نظام معلوماتي، والتي إنتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصرا في سلسلة الاتصال، مع تعيين المعلومات التالية: أصل الاتصال، مقصد الاتصال أو الجهة المقصودة بالاتصال، خط السير، ساعة وتاريخ، حجم وفترة الاتصال، أو نوع الخدمة.

أما بالنسبة للنوع الثاني تشير إلى المحتوى الإخباري لاتصال، بمعنى مضمون الاتصال أو الرسالة أو المعلومات المنقولة عن طريق الاتصال، فيما عدا البيانات المتعلقة بالمرور.

يلاحظ أن هناك نوعا من التقارب بين هذين النوعين من البيانات، من حيث المعنى، إلا أنهما مختلفان تماما من حيث درجة المساس بالحق في الخصوصية، حيث يكون ذلك أكثر أهمية بالنسبة لمراقبة محتوى الاتصال أو المراسلة، ومن تم تفرض ضمانات أكبر عن تجميع محتوى البيانات في الزمن الفعلي عن حركة البيانات سواء من حيث الجرائم التي من أجلها يتم توظيف هذا الإجراء، أو من حيث السلطة المختصة بإصدار أمر المراقبة.

أدرجت اتفاقية بودابست السالفة الذكر كل إجراء تحت عنوان خاص، فخصت تجميع حركة البيانات بعنوان "التجميع في الزمن الفعلي لبيانات المرور"[1]، أما تجميع محتوى البيانات فجاء تحت عنوان "اعتراض محتوى البيانات"[2].

أولا: مفهوم اجراء اعتراض الاتصالات الإلكترونية

كرس المشرع الفرنسي هذه التقنية في المادة 100 من قانون الإجراءات الجزائية الفرنسي التي تنص على أنه في المواد الجنائية والمواد الجنح إذا كانت العقوبة تفوق سنتين يمكن لقاضي التحقيق إذا دعت مقتضيات البحث والتحري أن يأمر باعتراض وتسجيل ونقل المراسلات التي تتم عن طريق وسائل

[1]– المادة 20 من اتفاقية بودابست سالفة الذكر

[2]– المادة 21 من نفس الاتفاقية.

الاتصال، ولقد حدد المشرع الفرنسي مفهوم المراسلات الخاصة التي تكون محلا للاعتراض من خلال المنشور في17 /1988/02 [1]الذي اعتبر أنه تكون المراسلة خاصة إذا كانت الرسالة موجهة بصورة حصرية لشخص أو أشخاص طبيعيين أو معنويين محددين على وجه الخصوص بغض النظر عن الشكل الذي تكون عليه. كذلك عرف القانون البريد والاتصالات الفرنسي[2] الاتصالات الإلكترونية بأنها « كل انتقال أو إرسال أو استقبال لإشارات أو علامات أو كتابة أو صور أو أصوات عن طريق النظام الكهرومغناطيسي ». تختلف وتتنوع المراسلات عبر وسائل الاتصال الإلكترونية والتي من أهمها التراسل عبر البريد الإلكتروني، الذي تم ابتكاره ليتمكن مستخدموها من تبادل الرسائل.

حدد المشرع الجزائري في المادة 8 فقرة 21 من القانون رقم 2000-03 [3] المؤرخ في 2000/08/05، المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية مفهوم الاتصالات السلكية واللاسلكية، كذلك عرفت المادة 5 من المرسوم الرئاسي رقم 15-261 الذي يحدد تشكيلة وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته [4]في حين أنه أغفل في قانون الإجراءات الجزائية تعريف إجراء اعتراض الاتصالات حيث اكتفى فقط بوضع تنظيم لهذه العملية، من خلال نص المادة 65 مكرر 05 من قانون الإجراءات فيقصد باعتراض الاتصالات، اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية، وهذه المراسلات هي عبارة عن بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض، كما ان المادة 09 من هذا القانون، اعتبرت أن مادة المراسلات هي كل اتصال مجسد في شكل كتابي يتم عبر كافة الوسائل المادية التي يتم ترحيلها إلى

[1] − circulaire française du 17 février 1988 prise en application de l'article 43 de loi 86-1067 du 30 septembreer 1986 relative a la liberté de communication concernant le régime déclaratif applicable a certains services de communication audiovisuelle JORF du 09 mars 1988, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068930.

[2] − art. 1du Décret n° 2007-29 du 5 janvier 2007 relatif au service universel postal et aux droits et obligations de La Poste et modifiant le code des postes et des communications électroniques, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000646118.

[3]− قانون رقم 2000-03 المؤرخ في 05 جمادي الأول عام 1421 الموافق ل 5 غشت سنة 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، الجريدة الرسمية للجمهورية الجزائرية عدد 48، بتاريخ 6 غشت سنة 2000.

[4]− مرسوم رئاسي رقم 15-261 مؤرّخ في 24 ذي الحجة عام 1436الموافق 8 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، الجريدة الرسمية للجمهورية الجزائرية عدد 53 بتاريخ 08 أكتوبر 2015.

العنوان المشار إليه من طرف الرسل نفسه أو بطلب منه، ولا تعتبر الكتب والجرائد واليوميات كمادة مراسلات، بالتالي فحسب مفهوم هذه المادة فإن المراسلات الخاصة تصبح محصورة في الرسائل المكتوبة بالمفهوم التقليدي، إلا أنه وبالرجوع إلى نص المادة 46 من الدستور الجزائري[1] التي تنص على أن سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، وكذا نص المادة 303 من قانون العقوبات التي تعاقب كل من يفض أو يتلف رسائل أو مراسلات موجهة للغير، فإنه يمكن التوصل للقول أن المراسلات الخاصة تعني كل رسالة مكتوبة بأي شكل من الأشكال سواء ماديا أو إلكترونيا وسواء كانت على دعامة ورقية أو رقمية، مرسلة بأي وسيلة لعدد معين ومحدد من المرسل إليهم، باستثناء الكتب والمجلات والجرائد التي لا تعتبر مراسلات خاصة.

هذا ما يؤكده القانون 04/09 في المادة 2 فقرة "و"، في تعريفها للمراسلات الإلكترونية على إنها على تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية[(2)]أثناء الإتصال نفسه ومن تم تسجيله.

مما لا شك فيه أن أسلوب اعتراض الاتصالات السلكية واللاسلكية دون علم أصحابها بقدر ما يفيد في كشف الحقيقة ويسهل إثبات كثير من الجرائم الغامضة كتلك المتعلقة بالجرائم المعلوماتية، فهو من جانب آخر يمثل انتهاكا لحرمة الحياة الخاصة للأفراد واعتداء على سرية مراسلاتهم واتصالاتهم التي كفلتها الدساتير والتشريعات العقابية.

---

[1]– تحرص الدساتير والقوانين الوطنية على احترم مبدأ السرية وتأكيده، الدستور الجزائري لسنة 2016 المادة 39 منه، والدستور الولايات المتحدة الأمريكية الصادر عام 1789 شاملا تعديلاته لغاية 1992، والقانون الفرنسي رقم 646 لسنة 1991. والتوجيه الأوروبي الصادر عام 1995. ولا يتم الكشف عن المعلومة أو الرسالة أو الاتصال إلا عن طريق السلطة القضائية أو السلطة الإدارية لأسباب حددها دستور 2016 الصادر بموجب قانون رقم 16 – 01 مؤرخ في 26 جمادى الأولى عام 1437 الموافق 6 مارس سنة 2016، يتضمن التعديل الدستور، الجريدة الرسمية للجمهورية الجزائرية عدد 14 بتاريخ 7 مارس 2016.

The Constitution of the United States (1787–1992), in ;https://www.encyclopediavirginia.org/The_Constitution_of_the_United_States_1787-1992.

Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000173519.

Conseil de l'Europe recommandation n R (95) 13, op, cit.

[2] – **سعيداني نعيم**، مرجع سابق، ص 185.

ثانيا: مشروعية اعتراض الاتصالات السلكية واللاسلكية الخاصة

يثير استخدام التقنيات الحديثة في التنصت على الأحاديث الشخصية وتسجيلها بعض المشكلات الفنية والقانونية[1].

إن مصلحة المجتمع في الوصول إلى الحقيقة في بعض الأحيان تقتضي التضحية جزئيا بمصلحة الفرد، وذلك باختراق حاجز الخصوصية بالسماح في حدود معينة بالتنصت على ما يدلى به الفرد من أحاديث خاصة بحثا عن الدليل بشأن جريمة يكون متهما بارتكابها أو التورط فيها، لا سيما في الأحوال التي يتعذر فيها الحصول عليه بوسيلة أخرى. وجاءت المادة 14 من القانون 06-220على توسيع مجال اختصاص النيابة العامة في مجال البحث والتحري عن هذه الجرائم بمنح الإذن باعتراض المراسلات عن طريق وسائل الاتصال السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور، ووضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص يتواجدون في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

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.

مكن المشرع الجزائي ضابط الشرطة القضائية من صلاحية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور للكشف عن الجرائم المعلوماتية، وهي إجراءات تباشر بشكل خفي، على الرغم من تناقضها مع النصوص المقررة لحماية الحق في الحياة الخاصة، فالتقاط الصور يكون بالتقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص، ويتم استخدام هذه الوسائل في المحلات السكنية والأماكن العامة والخاصة.أما تسجيل الأصوات، فيتم عن طريق وضع رقابة

[1] – فقد لا تكون التسجيلات الصوتية مطابقة لحقيقة الواقع نظرا لما قد يطرأ عليها من تشويه أو تحريف للحقيقة إما بالحذف أو بالإضافة أو بتغيير مواضيع الكلمات والجمل على الشريط المسجل (ما يطلق عليه المونتاج). ففي عصر التكنولوجيا الحديثة أصبحت أجهزة التصوير والتسجيل الدقيقة موجودة داخل أجهزة الهاتف المحمول الذي في إمكان أي شخص عادي إحرازه واستخدامه بالتالي استخداما غير مشروع بتسجيل محادثات الغير والتقاط الصور لهم بدون موافقة منهم على ذلك مما يعد معه انتهاكا للحرية الشخصية وحرية الحياة الخاصة. **أحمد حسام طه تمام**، الحماية الجنائية لتكنولوجيا الاتصالات دراسة مقارنة، دار النهضة العربية، القاهرة، 2002، ص 35.

على الهواتف[1] وتسجيل الأحاديث التي تتم عن طريقها، كما يتم أيضا عن طريق وضع ميكروفونات حساسة تستطيع التقاط الأصوات وتسجيلها على أجهزة خاصة، وقد يتم أيضا عن طريق التقاط إشارات لاسلكية أو إذاعية.

إن ما يهم هو أن مثل هذه الإجراءات يمكن لها المساس بالحرية الشخصية، خصوصا أن سرية المراسلات هي حق دستوري، فقد جاء في المادة 03 من القانون رقم 09-04 أنه: "مع مراعاة الأحكام القانونية التي تخص سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية"، وضع هذا القانون ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

حاول المشرع التوفيق بين هذه المتعارضات، بأن أجاز هذه الأساليب، ولكن بضوابط، أهمها مباشرة التحري بإذن من وكيل الجمهورية المختص، والتزام أعوان وضباط الشرطة القضائية القائمين بالإجراء السر المهني، فالمشرع على الرغم من إقراره أساليب تحري خاصة التي قد تمس بحرمة الحياة الخاصة إلا أنه يعاقب على اللجوء لاستعمالها بطرق غير مشروعة، كما لم يفتح الباب على مصراعيه في اللجوء إلى هذه الوسيلة بل أحاط استخدامها بشروط قانونية تعمل على منع التعسف وتصون الحرية الفردية وتتمثل هذه الشروط في:

أ- السلطة المختصة بإصدار إذن الاعتراض:

إن الحماية التي تكفلها التشريعات للاتصالات العادية لا يقتصر نطاقها على هذا النوع من الاتصالات فحسب، بل تمتد هذه الحماية إلى الاتصالات الإلكترونية عبر الانترنت.

إذا اقتضت ضرورة التحقيق اعتراض هذه الاتصالات وتسجيلها، فسنتبع حينها نفس الضمانات المقررة للمحادثات التلفونية، مع مراعاة خصوصية هذه الاتصالات الحديثة.

[1]- وجب التفريق بين مصطلح اعتراض المكالمات الهاتفية وبين مصطلح وضع الخط الهاتفي تحت المراقبة، فبينما يكون الأول دون رضا المعني، يكون الثاني برضا أو بطلب من صاحب الشأن، ويخضع لتقدير الهيئة القضائية بعد تسخير مصالح البريد والمواصلات لذلك.

طبقا للمادة 65 مكرر 05 من قانون الإجراءات الجزائية الجزائري فإنه لا يمكن لضباط الشرطة القضائية اللجوء إلى إجراء اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبب[1] من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي، فالسلطة القضائية هي وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمانة لذا الإجراء، وعلى وكيل الجمهورية أو قاضي التحقيق قبل منح هذا الإذن تقدير فائدة إجراء الاعتراض المراسلات وجديته وملاءمته لسير إجراءات الدعوى من خلال معطيات التحريات التي قامت بها الضبطية القضائية مسبقا.

نصت المادة 65 مكرر 09 على أن عملية تنفيذ إجراء اعتراض المراسلات تتم تحت رقابة السلطة القضائية التي أذنت به وذلك من خلال قيام ضباط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص بإعداد محضرا عن كل عملية اعتراض للمراسلات وكذا عن عملية وضع الترتيبات التقنية لهذا الغرض، ويذكر في هذا المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها.

في فرنسا، منذ صدور القانون رقم 2004-204 [2] المؤرخ في 2004/03/09 المعدل لقانون الإجراءات الجزائية أصبح حسب المادة 706-95 الإذن باعتراض المراسلات من اختصاص قاضي الحريات والاحتباس بمنحه بناء على طلب وكيل الجمهورية إذا تعلق الأمر

[1] – المادة107 حيث عاقب المشرع الجزائري لأول مرة اعتراض الاتصالات السلكية واللاسلكية دون إذن بذلك، بموجب القانون رقم 06-23 السالف الذكر، حيث تنص المادة 303 مكرر من قانون العقوبات سالف الذكر على أنه: « يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من، 50000دج إلى 30000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت وذلك:

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

– بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه ».

–يعاقب على الشروع في هذه الجرائم بنفس عقوبات الجريمة التامة.

لم تقتصر الحماية عند تجريم الأفعال الخاصة بالاعتراض، بل شملها أيضا في عقاب كل من احتفظ أو وضع أو سمح بأية وسيلة كانت التسجيلات المتحصل عليها بأحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون.

[2] - Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000249995.

بالتحقيق في الجرائم المحددة حصرا بالمادة 706-73، وتخضع إجراءات الاعتراض لرقابته في أجل 15 يوم قابلة للتجديد بنفس الشروط في الشكل والأجل.

ب- تسبيب إذن القاضي الصادر باعتراض الاتصالات:

يصدر القاضي الإذن باعتراض الاتصالات الإلكترونية بناء على ما يتكشف له من خلال أعمال الاستدلال التي قام بها أعوان الشرطة القضائية، وأن تبين له من خلالها ضرورة إصدار الإذن بالموافقة لما لذلك من أهمية في إظهار الحقيقة في الجريمة المعلوماتية.

ان العلة من تسبب الإذن القضائي ترجع إلى أن هذا الإجراء يمس بالحريات الخاصة للأفراد، فهو استثناء عن القاعدة العامة والمتمثلة في صيانة حرمة الحياة الخاصة للمواطنين وحقهم في سرية مراسلاتهم واتصالاتهم[1].

ج- الجرائم التي يجوز فيها إصدار الإذن باعتراض الاتصالات:

عموما إن الجرائم التي يجوز للسلطة القضائية الإذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية هي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم المعلوماتية، جرائم تبييض الأموال، الإرهاب، جرائم الفساد[2] وهذا إدراكا على عدم كفاية الوسائل التقليدية لجمع الدليل الإلكتروني نظرا لما تتمتع به هذه الجرائم من خصوصية.

د- مدة إجراء الاعتراض المراسلات:

حرصت معظم التشريعات المقارنة- تجنبا لإساءة إستعمال السلطة- على تحديد مدة معينة للاعتراض، وقد أطال كل من المشرعين الجزائري المادة 65 مكرر 7 فقرة 2 والفرنسي مادة 100 – 2 زمن المدة إلى أربعة أشهر قابلة للتجديد[3].

تجدر الإشارة إلى أن الطبيعة الخاصة التي يتمتع بها الدليل الإلكتروني من حيث سرعة فقده وزواله، تفرض علينا تخفيف من حدة شرط المدة وذلك للتحفظ على الدليل وضبطه.

---

[1]. **Robert BADINTER**, Le droit de l'écoute électronique en droit français, In ;https://www.u-picardie.fr/curapp-revues/root/1/badinter.pdf .consulté le :07/11/2012, pp16-8.

[2] – هذا ما نصت عليه المادة 65 مكرر 05 قانون الإجراءات الجزائية الجزائري سالف الذكر.

[3]– تنص المادتان 16 و17 من اتفاقية بودابست السالفة الذكر على التزام التحفظ لمدة 90 يوما.

هـ – ضبط التسجيلات ووضعها في أحراز :

تنص المواد 24، 25 و26 من المرسوم الرئاسي رقم 15–261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته[1]، على انه تحفظ المعلومات المستسقاة أثناء عمليات المراقبة خلال حيازتها من الهيئة وفقا للقواعد المطبقة على حماية المعلومات المصنفة، كما تسجل الاتصالات الإلكترونية التي تكون موضوع مراقبة وتحرر وفقا للشروط والأشكال المنصوص عليها في قانون الإجراءات الجزائية. وتسلّم التسجيلات والمحررات إلى السلطات القضائية وإلى مصالح الشرطة القضائية المختصة وتحتفظ السلطات القضائي دون سواها بهذه المعطيات أثناء المدة القانونية المنصوص عليها في التشريع الساري المفعول، ويجب – تحت طائلة العقوبات الجزائية المنصوص عليها في التشريع الساري المفعول– ألا تستخدم المعلومات والمعطيات التي تستلمها أو تجمعها الهيئة لأغراض أخرى غير تلك المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وذلك وفقا للأحكام المنصوص عليها في القانون رقم 09–04.

يمكن اعتبار المراسلات وتسجيلات الأصوات والتقاط الصور أو أشرطة الصور من قبيل الأشياء المضبوطة التي تخضع للمادة 18 قانون الإجراءات الجزائية الجزائري، وحكم المادة 45 من قانون الإجراءات الجزائية الجزائري بأن تغلق الأشياء المضبوطة ويختم عليها إذا أمكن ذلك، كما أن الأشرطة المسجلة تعتبر أدلة إثبات مادية أصلية تقتضي الشرعية الإجرائية حفظها بطريقة خاصة بوضعها في أحراز مختمة بما يضمن عدم التلاعب أو العبث في الحديث المسجل سواء بالحذف أو الإضافة، وضمها إلى ملف الإجراءات مع المحاضر التي تصف أو تنسخ محتواها المفيد لكشف الحقيقة.

[1]– مرسوم رئاسي رقم 15–261 مؤرّخ في 24 ذي الحجة عام 1436الموافق 8 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، الجريدة الرسمية للجمهورية الجزائرية عدد 53 بتاريخ 08 أكتوبر 2015.

يثور التساؤل أيضا عن من له الحق في الاطلاع على التسجيلات والصور؟

باستقراء النصوص القانونية للتشريع الجزائري، خول لضباط الشرطة القضائية حق الاطلاع على الصور بعد استخراجها ومضمون التسجيلات أثناء عملية وصفها ونسخها في محاضر وذلك بأنفسهم أو بتسخير خبير إذا كان الاطلاع عليها واستخلاص دليل يقتضي خبرة فنية، وسواء في إطار تحقيق ابتدائي أو حالة تلبس أو إنابة قضائية، لان الاستعانة بالخبير الفني المتخصص عند تنفيذ هذا الإجراء وكذا تقديم الدليل المستمد منه إلى القضاء، هو لضمان عدم تحريف التسجيل أو إدخال أي مونتاج أو تحوير ما عليه، ولإمكانية مطابقة الأصوات التي تجري تسجيلها مع صوت المتهم، وكذلك الأمر بالنسبة للصورة، كما رخص للنيابة العامة والهيئة القضائية حق الاطلاع عليها، على اعتبار أنها السلطة المخول لها حق الإذن باتخاذ هذه الإجراءات إلا أنه لم يشر صراحة إلى عرض هذه التسجيلات والصور على المشتبه فيهم في مرحلة جمع التسجيلات، على عكس ما يوجده في نص المادة 42 قانون الإجراءات الجزائية الجزائري، حيث أوجب عرض الأشياء المضبوطة على الأشخاص المشتبه في مساهمتهم في جناية للتعرف عليها، فهل يمكن تطبيق الأحكام نفسها على التسجيلات والصور الملتقطة كأدلة إثبات مادية؟ إن إجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور يتميز بطابع سري لخطورة الجرائم التي تتخذ في شأنها وكذا المراقبة المباشرة للهيئة القضائية التي أذنت بها، لذلك لا موجب لعرضها على المشتبه فيهم أثناء مرحلة جمع الاستدلالات على عكس الأشياء المضبوطة التي تتميز بطابع العلنية في غالب الأحيان، وخضوع ضبطها للسلطة التقديرية لضابط الشرطة القضائية دون حصوله على إذن قضائي كما في إجراء المعاينة مثلا، كذلك تلزم المادتان 27 و28 من المرسوم الرئاسي رقم 15-261 بالنسبة للرقابة الوقائية التي تقوم بها مستخدمو الهيئة بالسرّ المهني وواجب التحفظ بحيث يخضعون –ومن بينهم الذين يدعون إلى الاطلاع على معلومات سرّية– إلى إجراءات التأهيل، كما يؤدي مستخدمو الهيئة الذين يدعون إلى الاطلاع على المعلومات السرّية اليمين أمام المجلس القضائي قبل تنصيبهم.

و- تدوين محضر التحري:

نظرا لأهمية التدوين في مجال التحري الجزائي، فقد أوجب قانون الإجراءات الجزائية في نص المادة 18 منه، على ضباط الشرطة القضائية أن يحرروا محاضر بأعمالهم ويوقعوا عليها، ويبينون من خلالها الإجراءات

التي قاموا بها ووقت ومكان القيام بها ويوافوا وكيل الجمهورية بأصولها وبجميع الوثائق والمستندات المتعلقة بها، ومنه فانه يجب تدوين تفاصيل كل عملية لاعتراض المراسلات أو تسجيل الأصوات السمعية أو السمعية البصرية، وكذا وضع الترتيبات التقنية اللازمة لذلك، يذكر بالمحضر تاريخ وساعة وظروف بداية العملية والانتهاء منها. أما عن مضمون المراسلات المسجلة أو الصور الملتقطة فان ضابط الشرطة القضائية يقوم بنسخ أو وصف محتواها الضروري لإظهار الحقيقة في محضر يودع بملف الإجراءات، أما إذا كانت المراسلات أو الاتصالات بلغة أجنبية فإنه يتم تسخير مترجم لنسخ وترجمة محتواها.

الفرع الثاني

المراقبة الإلكترونية

إن المراقبة الإلكترونية تعتبر من الإجراءات الماسة بحرية سرية المراسلات والاتصالات الإلكترونية فالمراقبة الإلكترونية تشكّل انتهاكا لذا يجب أن ينظم هذا الإجراء في قواعد قانونية.

تستخدم كلمة المراقبة في مراقبة المحادثات التلفونية والاتصالات الإلكترونية، والمقصود بمراقبة المحادثات التليفونية وتسجيلها، التنصت على الأحاديث الخاصة بشخص أو أكثر مشتبه فيه، ويعتقد بفائدة محادثاته في الكشف عن الحقيقة، وذلك عن طريق إخضاعها لنوع من الرقابة بقصد التعرف على مضمونها، أثناء بثها وليس الحصول عليها وهي مخزنة، وغالبا ما يتم بعد ذلك تسجيلها للوقوف على ما تحويه من تفصيلات وأقوال يعول عليها بوصفها دليلا من أدلة إدانته بعد التأكد من صحة نسبتها إلى قائلها وعدم إدخال أي قدر من التغير أو التعديل عليها، وذلك إما بالحذف أو الإضافة لمضمونها ويتم ذلك عادة بوضع أداة للتسمع والتنصت تثبت بطريقة فنية على الخط التلفوني المراد مراقبة أحاديثه وتسجيلها.

تنص المادة 46 من دستور سنة 1996 [1] التي نصت على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون. سرية المراسلات والاتصالات الخاصة

[1]– الدستور الجزائري لسنة 1996، مرسوم رئاسي رقم 96-348 مؤرخ في 26 رجب 1417هـ الموافق ل 7 ديسمبر 1996 يتعلق بإصدار نص تعديل الدستور، المصادق عليه باستفتاء 28 نوفمبر 1996، الجريدة الرسمية للجمهورية الجزائرية عدد 76 بتاريخ 08 ديسمبر 1996.

بكل أشكالها مضمونة"، إلا أنه في تعديل الدستوري لسنة2016، حاول المشرع مواكبة التطور الذي يشهده العالم في مجال حماية البيانات الشخصية، من خلال إضافة فقرتين للمادة أعلاه تنصان على أنه:" لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون انتهاك هذا الحكم"

إن أضافت الفقرتين الثالثة والرابعة في التعديل الأخير، إنما ينم عن اقتناع المشرع الجزائري بضرورة المبادرة إلى وضع الآليات القانونية الكفيلة بحماية البيانات الخاصة بالأشخاص الطبيعيين خلال عملية المعالجة الآلية لها.

يكون المشرع الجزائري بهذا رغم ضمانه لسرية المراسلات والاتصالات بكل أشكالها، قد خول استثناء للسلطة القضائية وفي إطار قرار معلل بأن تتبع إجراءات تمس البيانات الشخصية، بالنظر لخطورة الجرائم المعلوماتية، كما بين القانون 09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مادته الرابعة، الحالات التي تسمح بتطبيق الإجراء الجديد المتمثل في مراقبة الاتصالات الإلكترونية، وذلك على سبيل الحصر.

هناك اختلاف في تحديد الطبيعة القانونية لمراقبة المحادثات الهاتفية والاتصالات الإلكترونية حيث انقسمت الآراء إلى ثلاث أقسام وهي:

الرأي الأول: اعتبار مراقبة المحادثات الهاتفية والاتصالات الإلكترونية نوعا من أنواع التفتيش، وذلك لأن المراقبة مثل التفتيش تشكل انتهاكا على حرمة الحياة الخاصة للإنسان وحريته الشخصية وعلى أثر ذلك تخضع المراقبة لشروط وضمانات التفتيش[1].

الرأي الثاني: مراقبة المحادثات الهاتفية والاتصالات الإلكترونية نوع من أنواع الاطلاع على الرسائل، لأن الرسالة تتضمن بعض أسرار الحياة الخاصة للمرسل والغير[2].

الرأي الثالث: مراقبة المحادثات الهاتفية والاتصالات الإلكترونية إجراء من نوع خاص، يرى أصحاب هذا الرأي أن مراقبة المحادثات الهاتفية والاتصالات الإلكترونية إجراء ذو طبيعة خاصة يماثل التفتيش لكنه ليس تفتيشا وهو يهدف إلى ضبط الأدلة التي تكشف الحقيقة في جناية أو

[1] – **قدري عبد الفتاح الشهاوي**، مناط مشروعية العمل الشرطي، دار النهضة العربية، القاهرة، 2007، ص 660.

[2] – **جمال جرجيس**، الشرعية الدستورية لأعمال الضبطية القضائية، النسر الذهبي للطباعة، القاهرة، 2006، ص 464.

جنحة وقعت وجاري التحقيق فيها.

إن المراقبة الإلكترونية للاتصالات الإلكترونية ومنها المحادثات الهاتفية، لا يمكن اعتبارها نوعا من أنواع التفتيش، ذلك لأنها ترد عن البيانات الإلكترونية المتحركة والتي تتجسد بالاتصالات الإلكترونية حال إجرائها، دون تلك التي انتهت وخزنت، في حين التفتيش إنما يرد فقط على البيانات الإلكترونية الساكنة.

لما كان استراق السمع بواسطة أجهزة التنصت الحديثة لضبط ما يفيد في كشف الحقيقة يعتبر اعتداء على الحق في الخصوصية والحرية الشخصية، لهذا تحرص الدول على أن تخضع مراقبة المكالمات التليفونية وتسجيلها لضوابط معينة حتى يمكن التوفيق بين المصلحة العامة في كشف الحقيقة وبين حماية الحق في الخصوصية وإن اختلفت هذه الضوابط ضيقا واتساعا من دولة إلى أخرى[1].

يلاحظ باستقراء نص المادة 303 مكرر من قانون العقوبات الجزائري، أنها تخص المحادثات الخاصة أو التي تتم في مكان خاص، وأيضا التي تتم عن طريق تلفوني، دون المحادثات التي تتم عن طريق الكمبيوتر والتي تتخذ شكل البريد الإلكتروني أو شكل المحادثة الفورية.

تدخل القانون الجزائري رقم 09-04 لتكملة وتنظيم المحادثات التي تتم عن طريق الأنترنت، حيث أجاز بموجب المادة الثالثة منه – وتبعا لمستلزمات التحريات والتحقيقات القضائية الجارية في إطار هذا النوع من الجرائم – اللجوء إلى وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتسجيل محتواها[2]، ومن بين تلك التقنيات يوجد، برنامج كارينفور وتقنية مراقبة البريد الإلكتروني، حيث يعتبر البريد الإلكتروني أهم وسيلة تقنية في مجال التراسل الإلكتروني ومن ثم فعملية المراقبة تنصب عليه.

---

[1] – **هلالي عبد اللاه أحمد**، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص 218.

[2] – تنص المادة 309 مكرر من قانون العقوبات السالف الذكر على "أن يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا أو بغير رضاء المجني عليه:

أ – استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون.

ب – النقط أو نقل بجهاز من الأجهزة أيا كان نوعه صورة شخص في مكان خاص".

ويتعين حسب نص المادة 309 مكرر سالفة الذكر أن تتم جريمة استراق السمع بمختلف صوره بالاستعانة بجهاز من الأجهزة التنصتية الحديثة، أيا كان نوعه، أما وقع التنصت بالأذن المجردة – أو بتدوين ما جرى من حديث على الورق، أو بروايته للغير نقلا عن الذاكرة مهما جاءت هذه الرواية دقيقة، ومطابقة لأصل الحديث الذي جرى فإنّ الجريمة لا تعتبر قد وقعت لافتقاد ركنها المادي المنصوص عليه وتحمي المادة 309 مكررا من المسارقة السمعية المحادثات بأية لغة كانت، ولو بلغة لا يفهمها سوى الذين اعتدوا بالمسارقة السمعية على حرمة حياتهم الخاصة وذلك متى جرت هذه المحادثات عن طريق التليفون، أو في مكان خاص، ويتميز المكان الخاص عادة بأنه مكان محاط بسياج يحول دون اطلاع من يوجدون

نظم قانون الإجراءات الجزائية أحكام وضوابط مراقبة المحادثات التليفونية والإلكترونية وتسجيلها واشترط توافر عدة شروط منها ما هو موضوعي ومنها ما هو شكلي للقيام بهذا الإجراء، ومن ذلك أنه لم يجز للنيابة العامة مراقبة المحادثات التليفونية والإلكترونية، أو أن تندب أحد من الضبطية القضائية لمباشرتها إلا بعد الحصول على أمر مسبب من القاضي الجزائي.

الواضح أن المشرع الجزائري لم يعتبر هذا الإجراء من ضمن طرق الحصول على الدليل الإلكتروني فقط، بل أدرجه ضمن التدابير الوقائية من الجرائم التي يمكن أن ترتكب بواسطة المعلوماتية، فإلى جانب إمكانية القيام بإجراء مراقبة الاتصالات الإلكترونية في إطار التحريات والتحقيقات القضائية من أجل الوصول إلى أدلة لم يكن بالإمكان الوصول إليها دون اللجوء إلى هذا الإجراء فإنه يمكن كذلك تطويع هذه التقنية لكي تعمل في بيئة الرقابة لغرض الوقاية من احتمال وقوع جرائم خطيرة بواسطة المعلوماتية من شأنها تهديد كيان الدولة وهو ما قررته المادة الرابعة من القانون رقم 09-04، أنه يمكن القيام بعمليات المراقبة الإلكترونية للاتصالات للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة وكذا في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني، وتكلف المادة 11 الفقرتان 1 و2 من المرسوم الرئاسي 15-261[1] -المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته- مديرية المراقبة الوقائية واليقظة الإلكترونية على الخصوص بتنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول وإرسال المعلومات المحصل عليها من خلال المراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة، وتضيف المادة 21 من نفس المرسوم انه في سبيل الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة تكلف الهيئة حصريا بمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها

خارجه على ما يجري بداخله وهو أيضا مكان لا يتواجد فيه عادة سوى أشخاص تربطهم صلة خاصة، ولو كان عددهم كبيرا... ومؤدى ذلك أنه إذا جرى الحديث في مكان خاص، ولكن كان باستطاعة من كانوا في مكان عام، أو أماكن خاصة أخرى أن يسمعوه بالإذن المجردة، فلا يتمتع بالحماية الجنائية المقررة بالمادة 309 مكرر وكذلك لا يتمتع بهذه الحماية الحديث الذي يجري في مكان عام سواء كان هذا المكان عاما بطبيعته أو بالتخصيص أو بالمصادفة.

في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية تحت سلطة قاض مختص ووفقا للأحكام المنصوص عليها في المادة 4 من القانون رقم 09-04 وجعلت المادة 8 من نفس المرسوم اللجنة المديرة للهيئة على الخصوص دراسة كل مسألة تخضع لمجال اختصاص الهيئة لا سيما فيما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للاتصالات الإلكترونية المنصوص عليها في المادة 4 من القانون رقم 09-04 السالف الذكر.

يعتبر تكريس المشرع لإجراء المراقبة الإلكترونية للاتصالات خطوة جريئة منه على اعتبار أن هذا الإجراء يعد من أخطر الإجراءات في إطار النظام الإجرائي عبر العالم الافتراضي لكونه يمس مباشرة خصوصيات الإنسان، وذلك بالرغم من أن البعض من الفقه يرى أن المراقبة لا تزال محل نظر في القانون من حيث ضرورة الالتزام بما هو مقرر في القوانين والضمانات الدستورية للحق في الخصوصية.

[1]- مرسوم رئاسي رقم 15-261 سالف الذكر.

الباب الثاني:

حجية الدليل الإلكتروني في الإثبات الجنائي

إنّ وصول القاضي الجزائي إلى حكم يعبر عن الحقيقة في الواقعة المطروحة عليه، ليس بالأمر الهين، حيث ليس بإمكانه أن يطالع بنفسه والتعرف على حقيقتها، إلا بإقامة الدليل على وقوع هذه الجريمة وعلى مسؤولية المتهم عنها، مما يستلزم منه الاستعانة بوسائل تعيد تمثيل أمامه تفاصيل حقيقة ما حدث، وهذه الوسائل هي أدلة الإثبات.

تعد عملية تقدير الأدلة جوهر مرحلة الحكم – وهي المرحلة الحاسمة في الدعوى الجزائية – حيث لا يمكن الوصول إلى الحكم ما لم يمارس القاضي سلطته التقديرية على الأدلة محل الوقائع، وتعتبر قاعدة حرية الإثبات الجنائي احدى أهم قواعد الإثبات في المسائل الجزائية على عكس الحال في المسائل المدنية، حيث جعل القانون وسائل الإثبات بكل الطرق القانونية، فجميع الأدلة لها نفس القوة والقيمة من حيث المبدأ سواء كانت أدلة مادية أو معنوية، فالدليل الإلكتروني في الجرائم المعلوماتية شأنه شأن باقي الأدلة الأخرى، يخضع لنفس القواعد المقررة لباقي الأدلة، سواء كانت هذه القواعد تتعلق بسلطة القاضي في قبول الدليل الإلكتروني، أو تتعلق بسلطته في تقدير هذا النوع من الدليل، ذلك أن القاضي لا يقدر إلا الدليل المقبول.

لتوضيح هذه النقاط، قسم هذا الباب إلى فصلين، قبول الدليل الإلكتروني(لفصل الأول)، تقدير الدليل الإلكتروني(الفصل الثاني).

الفصل الأول
قبول الدليل الإلكتروني

يعد قبول الدليل بصفة عامة والدليل الإلكتروني بصفة خاصة، الخطوة الإجرائية الأولى التي يمارسها القاضي الجزائي، حيث أن مسألة تقييم الدليل في إثبات الواقعة الإجرائية مسألة موضوعية محضة تخضع لسلطة القاضي التقديرية، أن القاضي له الحرية في أن يبنى حكمه على أي دليل متى اطمأن إليه حتى ولو كان هذا الدليل مستمدا من محاضر جمع الاستدلالات.

إن قبول القاضي الجزائي الدليل الإلكتروني في الإثبات لا بد أن يستند على أساس، وهذا الأخير يختلف من حيث النظام المتبع في الدول بين النظام اللاتيني والأنجلوسكسوني.

على هدى ما سبق يقسم هذا الفصل إلى مبحثين، أساس قبول الدليل الإلكتروني في الإثبات الجنائي(المبحث الأول)، والقيود الواردة على حرية القاضي الجزائي في قبول الدليل الإلكتروني(المبحث الثاني).

المبحث الأول

أساس قبول الدليل الإلكتروني في الإثبات الجنائي

يستهدف نظام الإثبات في كل تشريع الوصول إلى كشف الحقيقة، وهذا الأمر لا يتحقق إلا من خلال تقدير الأدلة المتحصلة في الخصومة القائمة.

إن موقف القانون المقارن من سلطة القاضي الجزائي في قبول الدليل الإلكتروني تخضع إلى طبيعة نظام الإثبات السائد في الدولة، إن هذه الأنظمة تنقسم إلى ثلاثة فئات:

نظام الإثبات القانوني أو المقيد، نظام الإثبات المعنوي أو مبدأ حرية الإثبات، نظام الإثبات المختلط .

سيحاول تبيين موقف النظم القانونية من الدليل الإلكتروني كدليل إثبات من خلال المطلبين التاليين، صلاحية القاضي في الاجتهاد في مجال الإثبات في النظام اللاتيني(المطلب الأول) وسلطة القاضي الجزائي في الاجتهاد في مجال الإثبات في النظام الأنجلوسكسوني(المطلب الثاني)

المطلب الأول

إجتهاد القاضي الجزائي في مجال الإثبات في النظام اللاتيني

يعد مبدأ حرية الإثبات المبدأ العام في قانون الإجراءات الجزائية للتشريعات اللاتينية، بمعنى أن ثبوت الوقائع المكونة لأركان الجريمة ونسبتها إلى المتهم، أمر يتوقف على اقتناع القاضي للوصول إلى الحقيقة، ثم يقدرها في حرية تامة، إلا أن التقدير الحر يجب ألا يصل إلى حد التحكم الكامل، لأن حرية القاضي الجزائي في ذلك غير مطلقة بل مقيدة بقواعد اليقين التي تتمثل في الحفاظ على القواعد الإجرائية الشهيرة بأن تكون الأدلة مشروعة' الأصل في الإنسان البراءة، كفالة حق الدفاع، طرح الدليل أمامه بالجلسة، كما تتبع المحاكم الجزائية في المسائل غير الجزائية التي تفصل فيها تبعا الدعوى الجزائية طرق الإثبات المقررة في القانون الخاص بتلك المسائل، وهذه القيود لا تهدر هذا المبدأ أو تقلل من شأنه، ولكن تساعد على بيان مصادر اقتناعه.

إن الأدلة ليست سوى وسائل تستهدف للتوصل للحقيقة ويمكن من حيث المبدأ إقامتها أمام القاضي الجزائي وتأسيس اقتناعه عليها ما دامت مشروعة، إلا أن قبول ما يكون منها ناشئا أو مستمدا من نظم المعالجة الآلية قد توجس القاضي الجزائي، ذلك لأن بيئة هذه الأدلة هي الوسائل الإلكترونية.

يجوز للقاضي الاستناد إلى الدليل الإلكتروني لإثبات الفعل الإجرامي في سائر الجرائم، وهو ما سوف يحاول تبيينه في الفرعين التاليين، مبدأ الإثبات الحر كأساس لقبول الدليل الإلكتروني (الفرع الأول) والنتائج المترتبة على تطبيق مبدأ حرية الإثبات(الفرع الثاني).

الفرع الأول

مبدأ الإثبات الحر كأساس لقبول الدليل الإلكتروني

ان ازدياد مستخدمات العلم الحديث أدى إلى تقليل فرص الخطأ القضائي نتيجة الاعتماد عليها ومن ثم الرغبة في التوصل إلى درجة اليقين المطلوب فقدمت مساعدة كبيرة للقاضي لتكوين عقيدته في الاقتناع بصورة أشد جزما ويقينا مما جعل لبعض هذه الوسائل أهمية أكثر في الإثبات من غيرها في الأدلة[1]، خاصة مع ظهور جرائم من أنواع جديدة لم تكن معروفة من قبل.

إن وجود جزء أكبر من المسائل تقوم على الخبرة العلمية لا يغير من جوهر نظام الاقتناع الذاتي، فالقاضي وإن كان غير مكلف ببيان أسباب اقتناعه الشخصي إلا أنه مكلف ببيان أسباب الحكم الذي انتهى إليه وهو في مقام هذه الأسباب لابد أن يذكر الأدلة التي اعتمد عليها وكانت مصدرا لاقتناعه، لكنه غير مكلف بتحديد علة اقتناعه بهذه الأدلة بالذات، فهو مكلف بإثبات ما اقتنع به دون ان يكون مطالبا بإثبات لماذا اقتنع[2].

[1] -**أحمد ضياء الدين محمد خليل**، مشروعية الدليل في المواد الجنائية، دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجزائية، رسالة دكتوراه، كلية الحقوق، جامعة عين الشمس، القاهرة، 1982، ص 47.

[2] – **Rached Aly A**, De l'intime conviction du juge, vers une théorie scientifique de la preuve en matière criminelle , thèse pour obtenir le grade de doctorat, Paris Pédone, 1942 , p 29. **Georges BRIERE DE L'ISLE et Paul COGNART**, Procédure pénale, Tome2 , Armand Colin, Paris, 1972,p 206.

لا يرسم القانون في نظام الإثبات المعنوي طرقا محددة للإثبات يتقيد بها القاضي الجزائي، بل يترك حرية الإثبات لأطراف الخصومة في أن يقدموا ما يرون أنه مناسب لاقتناع القاضي[1].

إنّ مبدأ حرية الإثبات في فرنسا ينطبق أمام جميع أنواع المحاكم الجنائية إلا إذا نص القانون على خلاف ذلك[2]، وللاستدلال على ذلك أن المحاكم الفرنسية في مواد الجنح والمخالفات يمكنها أن تتخذ جميع الإجراءات الضرورية لتكوين اقتناعها، فلها أن تسأل أو تستوجب المتهم حول أساس الاتهام الموجه إليه[3]، ويمكنها سماع الشهود واستدعاء الخبراء إذا واجهتها مسألة فنية، أما في مواد الجنايات[4] منح للقاضي الجنائي سلطة تقديرية خاصة للقيام بجميع الإجراءات التي يقدر فائدتها في كشف الحقيقة.

إن اقتناع القاضي سواء بالإدانة أو بالبراءة، لا يكون وليد فراغ، بل من خلال أدلة مشروعة، متساندة، طرحت أمامه في جلسة المناقشة أدت في سياقها العقلي والمنطقي إلى تلك النتيجة التي توصل إليها في حكمه، لكن ربما يتسرع فيخطئ، ومن هنا كان الالتزام بتعليل الأحكام القضائية[5]، وهكذا فإنه وإن كان التقدير الشخصي للقاضي بالنسبة للأدلة لا يخضع للرقابة، فإن التقدير الموضوعي لهذه الأدلة يخضع للرقابة، لذلك أوجب المشرع الفرنسي أن تشمل الأحكام على الأسباب التي بنيت عليها، ضمانا لجديتها، وتعزيز الثقة في عدالتها[6].

تنص المادة 427 من قانون الإجراءات الجزائية الفرنسي على جواز إثبات الجرائم بجميع طرق الإثبات، ويحكم القاضي بناء على اقتناعه الشخصي، بالرغم من الجدل الفقهي التي أثارته هذه المادة حول تطبيقها وهذا لأنها أدرجت ضمن أحكام الجنح.

---

[1] – **CASORLA Francis**, "Le droit Français, La preuve en procédure pénale comparé Association international de droit pénal", RIDP, 1992, p 183.

[2] – **Merle et Vitu,** op.cit**,** p 165.

[3] – ذلك حسب المادتين 442 و536 من قانون الإجراءات الجزائية الفرنسي سالف الذكر.

[4] – المادة 310 من القانون الإجراءات الجزائية الفرنسي سالف الذكر.

[5] – **Rached Aly.A**, op.cit, p 177.

[6] – المواد 485، 512، 536، من القانون الإجراءات الجزائية الفرنسي سالف الذكر، انظر كذلك حكم محكمة النقض الفرنسية:

Cass crim. 31 Oct. 1957, D. 1958, Som. 27.Cass crim. 12 mars 1957, D. 1957, Som. 87, in; www.persee.fr/doc/afdi_0066-3085_1957_num_3_1_1354. Consulté le: 23/04/2016.

يعد حكم هذه المادة هو حكم عام وعلى ذلك تفرض محكمة النقض الفرنسية – ويظهر ذلك في أحكامها – تطبيق صارم لهذا المبدأ، فهي تدعو القضاء إلى الاستعانة بأي دليل يكون لازما لتكوين عقيدتهم[1].

على هذا الأساس أن مهمة البحث عن الأدلة وتقديمها في مرحلة المحاكمة لا تقع فقط بصفة أساسية على عاتق الادعاء والدفاع، بل ان القضاة كذلك يتحملون جانبا من المسؤولية، يلقى عليهم عبء الإثبات شأنهم في ذلك شأن سلطة الاتهام[2].

ان قانون الإجراءات الجزائية الجزائري في هذا الإطار لم يفرد نصوصا خاصة تحظر على القاضي مقدما قبول أو عدم قبول أي دليل بما في ذلك الدليل الإلكتروني، وهذا أمر منطقي، لأن الجزائر تستند إلى مبدأ حرية الإثبات في المسائل الجزائية، حيث أنه أقر هذا المبدأ في المادة 212 من قانون الإجراءات الجزائية، التي أدرجها ضمن الأحكام المشتركة والمتعلقة بطرق الإثبات أمام جهات الحكم مما لا يدع أي شك في تطبيقها أمام الجهات القضائية الجزائية.

انطلاقا من ذلك إن الدليل الإلكتروني مقبول مبدئيا في الإثبات بصفة عامة والإثبات في مجال جرائم المعلوماتية بصفة خاصة بوصفه من الأساليب العلمية الحديثة في الإثبات.

الفرع الثاني

النتائج المترتبة على تطبيق مبدأ حرية الإثبات

إنّ إعمال مبدأ حرية الإثبات يجعل القاضي الجزائي يتمتع بدور إيجابي في كشف الحقيقة في الجرائم التقليدية منها والمستحدثة، ويبدو هذا الدور من ثلاثة جوانب، أن يكون له الحرية في توفير الدليل المناسب والضروري للفصل في الدعوى بما في ذلك الدليل الإلكتروني، أن يكون له

[1] –**George LEVASSEUR** , Le régime de la preuve en droit répressif Français , la présentation de la preuve et la sauvegarde des libertés individuelles, troisième colloque du département des droits de l'homme, Bruxelles, 1977, p47.

[2] – **السيد محمد حسن شريف**، النظرية العامة للإثبات الجنائي دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2002، ص 213.

الحرية في قبول أي دليل يمكن أن تتولد منه قناعته بما في ذلك الدليل الإلكتروني، أن يتمتع بالحرية نفسها في تقدير قيمتها الإقناعية[1].

أولا: الدور الإيجابي للقاضي الجزائي في توفير الدليل الإلكتروني

يقصد بالدور الإيجابي للقاضي الجزائي في توفير الدليل الإلكتروني عدم التزام القاضي بما يقدمه له أطراف الدعوى من أدلة، وإنما له سلطة وواجب عليه أن يبادر من تلقاء نفسه إلى اتخاذ جميع الإجراءات لتحقيق الدعوى والكشف عن الحقيقة الفعلية فيها، ذلك أن الحقيقة لا تظهر من تلقاء نفسها، وإنما في حاجة دوما إلى من يبحث وينقب عنها، وليس له أن يقتنع بما يقدمه إليه أطراف الدعوى فقط، وإنما عليه أن يبحث بنفسه عما يعتقد أنه مفيد في إظهار واكتشاف الحقيقة في كل نطاقها، ذلك أن الخطر أضحى عاما يهدد مصلحة المجتمع في أمنه واستقراره وسلامته، فكان من الضروري تسليم القاضي السلطات التي تمكنه من الوصول إلى الحقيقة الفعلية في الدعوى المنظورة أمامه.

أن دور القاضي الجزائي ليس دورا سلبيا كدور القاضي المدني– يقتصر على الموازنة بين الأدلة التي يقدمها الطرفان ثم يرجح أيهما أغلب– بل دوره إيجابي، فمن واجبه أن يتحرى وينقب عن الحقيقة باتخاذ الإجراء الذي يراه مناسبا ويقتنع به، وعليه فإن للقاضي الجزائي سواء بناء على طلبات الأطراف أو بموجب مقتضيات وظيفته، أن يأمر باتخاذ الإجراء الذي يراه مناسبا وضروريا للفصل في الدعوى[2].

تطبيقا على الجرائم المعلوماتية فإن القاضي الجزائي يستطيع من أجل الوصول إلى الحقيقة أن يوجه أمرا إلى مزود خدمة الأنترنت بتقديم بيانات معلوماتية متعلقة بمستخدم الأنترنت، كعناوين المواقع التي زارها وقت الزيارة والصفحات التي اطلع عليها والملفات التي جلبها والحوارات التي شارك فيها والرسائل التي أرسلها أو استقبلها وغيرها من المعلومات المتعلقة بكل أفعال المستخدم عندما يتصل بالشبكة، كما للقاضي الجزائي أن يأمر القائم بتشغيل النظام بتقديم

---

[1] – **فاضل زيدان محمد**، مرجع سابق، ص93.

[2] – تكمن العلة في الفرق بين دور كل من القاضي الجزائي والقاضي المدني في البحث عن الأدلة، إلى اختلاف طبيعة المصالح التي تحميها كل من الدعوى الجزائية والدعوى المدنية، فالأولى تحمى مصلحة عامة هي مصلحة المجتمع، أما الدعوى المدنية فإنها تحمى مصالح خاصة بأطرافها. **محمد زكي أبو عامر**، الإثبات في المواد الجنائية، الفنية للطباعة والنشر، الإسكندرية، 1985، ص 851.

المعلومات اللازمة لاختراق النظام والولوج إلى داخله، كالإفصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج المختلفة، أو تكليفه بحل رموز لبيانات مشفرة داخل ذاكرة الحاسب الآلي، كذلك للقاضي الجزائي سلطة الأمر بتفتيش نظم الحاسب الآلي بمكوناته المادية والمعنوية وشبكات الاتصال، متى ما قدر ضرورة وملاءمة هذا الإجراء[1].

من مظاهر الدور الإيجابي للقاضي الجزائي في البحث عن الدليل الإلكتروني كذلك، أن له سلطة الأمر باعتراض المراسلات السلكية واللاسلكية متى ما قدر فائدة الإجراء وجديته وملائمته لسير الدعوى.

أقوى مظاهر تعامل القاضي الجزائي مع الواقعة الإجرامية المعروضة، ندب الخبراء ليقدموا إيضاحات عن التقرير المقدمة منهم، لما للخبرة في مجال المساعدة القضائية من دور كبير[2].

ثانيا: الدور الإيجابي للقاضي الجزائي في قبول الدليل الإلكتروني

حسب المادة 307 من قانون الإجراءات الجزائية الجزائري إن الدور الإيجابي للقاضي الجزائي في توفير الدليل الإلكتروني، من حيث ماهيته، ومظاهره، وتبيين كيف أن القاضي الجزائي–على خلاف القاضي المدني– لا يجوز له أن يقنع بما يقدمه له الأطراف في الدعوى من أدلة، وإنما عليه أن يبحث بنفسه عن الأدلة ذات الأثر في تكوين عقيدته، وأن يستشير الأطراف إلى تقديم ما لديهم من أدلة.

تعد مرحلة قبول الدليل الإلكتروني الخطوة الثانية التي تلي البحث عن الدليل وتقديمه من قبل جميع الأطراف سلطة الادعاء، المتهم والقاضي.

تجدر الإشارة في هذا الصدد إلى أنه طبقا لمبدأ الشرعية الإجرائية التي يتحصل من خلالها الدليل بما يتضمنه من أدلة مستخرجة من رسائل إلكترونية كالكمبيوتر المحمول مثلا، لا يكون الدليل مقبولا في عملية الإثبات التي يتم من خلالها إخضاعها للتقدير، إلا إذا كان مشروعا، ذلك

---

[1] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 124.

[2] – أكدت المادة 143 من قانون الإجراءات الجزائية الجزائري سالف الذكر، على ذلك، حينما نصت على أنه: «لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة العامة وإما من تلقاء نفسها أو الخصوم... ».

أن القاضي لا يقدر إلا الدليل المقبول، ولا يكون كذلك إلا إذا كان مشروعا بأن تم البحث عنه وفقا لطرق مشروعة[1].

يخلص إلى أن مشكلة قبول الدليل الإلكتروني لا تثار في القانون الجزائري لأن هذا الأخير لا يعهد عنه سياسة النص على قائمة لأدلة الإثبات، فالأساس هو حرية الأدلة ولذلك فمسألة قبول الدليل الإلكتروني لا ينال منها سوى مدى اقتناع القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه للتقدير القضائي.

المطلب الثاني

إجتهاد القاضي الجزائي في مجال الإثبات في النظام الأنجلوسكسوني

يصعب في هذا النظام التمييز بين مراحل الدعوى الجزائية إلى أن تصل إلى المحاكمة، مما ينتج عنه صعوبة بروز الدور الإيجابي الذي يقوم به القاضي الجزائي في جمع الأدلة والتحري عن الحقيقة، وذلك لأنه نظام لصيق بالنظام الاتهامي القائم على الصراع بين خصمين متنازعين يتبادلان الاتهام والدفاع والقاضي حكم بينهما، حيث أن الإجراءات تمر بثلاث مراحل:

المرحلة التحضيرية: يقتصر دور القاضي هنا لمجرد الترخيص للشرطة في القيام ببعض الإجراءات الجبرية مثل التفتيش، إلا أنه لا يملك صلاحية اتخاذ أي إجراء من إجراءات التحقيق من تلقاء نفسه، وإنما تقتصر مهمته في مراقبة الإطار القانوني لأعمال البحث والتحقيق[2] حيث أن المشرع هو الذي يقوم بالدور الإيجابي في عملية الإثبات في الدعوى، فهو الذي ينظم عملية قبوا الأدلة للحكم بالأدلة أو الاستبعاد أدلة أخرى[3].

المرحلة المتوسطة: هي مقررة للنظر في مدى إمكانية إحالة المتهم إلى محكمة الجنايات في

---

[1] –راجع كل عن: **رشيدة بوكر**، مرجع سابق، ص317. **عائشة بن قارة مصطفى**، مرجع سابق، ص 125.

[2] – **عادل مستاري**، "التفتيش في الجرائم المعلوماتية"، مجلة الفكر الشرطي، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، دولة الإمارات العربية، المجلد الثاني والعشرون، العدد 86، 2013، ص 4.

[3] – إن القانون الأنجلوسكسوني Common Law ويسمى أحيانا القانون العام، هو المدرسة القانونية تستمد جذورها من التراث الإنجليزي، ومن أبرز سمات هذه المدرسة الاعتماد على السوابق القضائية كمصدر ملزم للتشريع.

Stephen J, Frunk SCHULHOFER, J BERNOCO, Berg GREEN, Rapport de Synthèse pour les pays de « common Law », La preuve en procédure pénale comparée, association internationale de droit pénal, RIDP 1992, p 33.

الجرائم المختلفة والخطيرة. والمرحلة الثالثة وهي مرحلة المحاكمة.

سيقسم هذا المطلب إلى الفرعين التاليين، أهم القواعد الخاصة التي تحكم النظام الانجلوسكسوني(الفرع الأول) والاستثناءات الواردة على القواعد التي تحكم النظام الأنجلوسكسوني(الفرع الثاني).

الفرع الأول

أهم القواعد الخاصة التي تحكم النظام الانجلو سكسوني

إن الدليل في النظام الانجلوسكسوني تحكمه قواعد خاصة لقبوله أمام المحاكم سواء تعلقت هذه القواعد بفحوى الأدلة أهمها استبعاد شهادة السماع، أو بكيفية تقديمها الأدلة أهمها قاعدة المحور الأصلي.

على ذلك يخلص أن هناك قاعدتين مهمتين تحكمان الإثبات الجنائي في النظام الانجلوسكسوني، قاعدة استبعاد شهادة السماع، وقاعدة الدليل الفضل.

أولا: قاعدة استبعاد شهادة السماع

يقصد بشهادة السماع أو التسامع عن الغير[1] بيان تقرير شفوي أو كتابي يحدث خارج المحكمة، كأن يأتي شخص يحكي ما سمعه من أشخاص آخرين عن وقائع القضية أو عن المتهم، ويتقدم إلى المحكمة من أجل إظهار الحقيقة أو بعبارة أخرى من أجل إثبات أمر حدث خارج الجلسة وكان صادقا [2].

---

[1] – تعرف شهادة السماع على أنها دليل يقدم من خلال شخص نقلا لعبارات أو سلوك صدر خارج المحكمة من شخص آخر، يؤكد أولا مسألة معينة لإثبات الحقيق، ويعتقد من يقدمه في صحته والفرق بين هذه التعاريف تجعل من الشهادة السماع دليل غير حازم لا يرقى لمستوى الدليل. بمعنى مجرد دلالة مثال عن شهادة السماع : « أن السيدة (س) قالت لي السيدة (ص) قد اغتصبها بعد الحفلة المدرسية الراقصة »، فهذا القول حدث خارج المحكمة، ولم يقدم من السيدة ذاتها، وأن السيدة (س) قدمته للمحكمة من أجل مسالة معينة في الدعوى يثار الجدل بشأنها، وهي أن الشخص "أ" شخص مغتصب. **رمزي رياض عوض**، حماية المتهم في النظام الانجلوأمريكي، دار النهضة العربية، القاهرة، 1998، ص 34.

[2] – يرى البعض من الفقهاء أن شهادة السماع نوع من الشهادة غير المباشرة، وليست هي شهادة السماع ذاتها، حيث تقسم الشهادة غير المباشرة إلى نوعين، "الشهادة السماعية" و"الشهادة بالتسامح"، وتعنى الأولى أن شخصا سمع من أخر معلومات عن الواقعة محل التحقيق، كما في الحالة التي يشهد فيها الشخص بأنه سمع من أخر أنه شاهد على ارتكاب المتهم للجريمة، أما الشهادة بالتسامع، فهي مجرد ترديد لإشاعة تتردد بين الناس بدون الجزم بصحتها، فقد تكون صادقة أو

مبدئيا القانون الإنجليزي لا يجيز شهادة التسامع، ويرجع السبب في ذلك إلى عدم الثقة في الشخص الذي يدلي به خارج المحكمة، فهو لا يؤدي يمينا أمام المحكمة، حيث يخضع لملاحظة القاضي أو المحلف وقت إدلائه أو كتابته، ومن ناحية أخرى فإن هذا السبيل لا يتيح للمتهم حقوقه الدستورية، خاصة حق المتهم في المواجهة[1].

أما بالرجوع إلى الدليل الإلكتروني، أصله يمثل شهادة سماع على أساس أنه يتكون من جمل وكلمات أدخلها شخص إلى جهاز الكمبيوتر، سواء تم معالجة تلك البيانات أو لم يتم ذلك، ومن شأن ذلك أن يثير اعتراضا على قبول المستندات المطبوعة التي يخرجها الحاسوب في الإثبات أمام القضاء الجنائي.

ثانيا: قاعدة المحور الأصلي أو الدليل الأفضل

هي تلك القواعد المتعلقة بكيفية تقديم الأدلة إلى القضاء وتحديد مدى قبولها كأدلة إثبات في المواد الجنائية ،تذهب قواعد الإثبات في التشريعات ذات الأصل الأنجلوسكسوني إلى تطبيق قاعدة الدليل الأفضل، فلأجل إثبات محتويات كتابة أو سجل أو صورة، فإن أصل الكتابة أو سجل أو صورة يكون مطلوبا[2]، بمعنى لا يجوز تقديم الصورة لإثبات محتوى الأصل، بصفة عامة حين يقدم أحد الأطراف تأييدا لدعواه، دليلا يستند إلى عدة دعائم فإن عليه أن يقدم أفضل نموذج، وهو ما يعني أن تكون الأدلة الواجب تقديمها أولية وليست ثانوية، أصلية لا بديلة، وأن يكون الدليل المقدم هو أفضل ما يتاح الحصول عليه بالنسبة لطبيعة وظروف القضية[1].

هناك تمييز حقيقي بين الأصالة في طابعها المادي وبين الأصالة في طابعها الإلكتروني، من حيث أن الأولى هي سوى تعبير وضعية مادية ملموسة، كما هو الشأن في الورق المكتوب أو بصمة الإصبع، فهذه كلها لها طابعها المادي المتميز، في حين أن الثانية ليست سوى تعداد غير

لا تكون، وترجع العلة في التمييز بين النوعين، في أن النوع الأول من الشهادة له قوة في الإثبات، ولكنها بدرجة اقل من النوع الثاني والتي لا تصلح أساسا كدليل لاستحالة التحقق من صحتها. راجع كل عن: **أمين مصطفي محمد**، حماية الشهود في قانون الإجراءات الجنائية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2008، ص 17. **فرج إبراهيم العدوي عبده**، سلطة القاضي الجنائي في تقدير الأدلة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1995، ص 205.

[1] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 128.

[2] – **عمر محمد بن يونس**، الإجراءات الجنائية عبر الأنترنت، مرجع سابق، ص 440.

محدود لأرقام ثنائية الصفر والواحد (1–0) فالصورة Image في العالم الرقمي مثلا ليس ذلك الوجود المادي الذي يعرف في شكل ورقي وغيره وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه.

تظل مشكلة أصالة الدليل الإلكتروني من المشكلات الكبرى، لاسيما أن الدليل الذي يتم استنباطه في هذا الإطار إنما هو دليل مستوحى من قاعدة مجهولة، أو خوادم غامضة، ليس من السهولة التوصل عليها، مثل خوادم الهكره التي يتم استخدامها برمجيات عالية التقنية تعمل على إخفائها في العالم الافتراضي كما هو الشأن في البرمجيات التي تقوم ببث عنوان خاطئ لهذه الخوادم، خاصة ان طبيعة هذا الدليل الذي يمكن إلغائه بأي شكل ويكون ما تبقى منه هو نسخة فقط تم التوصل إليها عن بعد مثلا بطريقة المراقبة الإلكترونية. فهل يكفي ناتج المراقبة الإلكترونية وحده للقول بأن الدليل هنا دليل أصلي وبالتالي يقبل طرحه على القضاء ليقول فيه كلمته بالإدانة[2]. ففي قضية سطو Burglary على أحد المصارف من قبل المدعو Pettigrew[3] رفضت محكمة الاستئناف في عام 1980 قبول مخرجات الحاسوب عبر الطابعة Print out التي عرضها بنك إنجلترا Bank of England كدليل يحتوي الأرقام المسلسلة للعملة المسروقة التي ضبطت مع المذكور، كانت حجة الرفض مبنية على معتقد المحكمة الذي صور هذا الدليل بكونه دليلا مستمدا من آلة مهامها القيام بإعداد تسلسل للأوراق المالية، وهو الأمر الذي يجعل مسألة التسلسل العملة أمرا طبيعيا ليس فيه ما يتم التعويل عليه في الإدانة. حتى أن الفقه استثارته هذه النقطة فاستفاض في إبراز قبول الدليل الإلكتروني المستمد من آلات غير ذكية، كما هو الشأن في كاميرات مراقبة السرعة ومراقبة المصارف وغيرها، وهي أدلة مقبولة أمام المحاكم، لذلك ومن الأولى يلزم قبول الدليل المستمد من الحاسوب.

---

[1] – **هشام محمد فريد رستم**، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص 171.

[2] – **فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، مرجع سابق، ص 636.

[3] – محمول من الموقع الإلكتروني التالي:http://e-lawresources.co.uk/Robbery.php تم الاطلاع عليه يوم: 2016/02/07.

ان الأصل في الدليل الإلكتروني مجرد إشارات إلكترونية، ونبضات ممغنطة، ليست مرئية للعين البشرية، مما لا تتيح للمحلفين أو للقاضي مناظرة أو وضع أيديهم على الدليل الأصلي، ومما يقدم إليهم من وثائق أخرجها الحاسوب سوى نسخ لأصول، مما يجعله دليلا ثانويا لا أصليا، فضلا عن ذلك أن النسخة لا تظهر جميع البيانات المتضمنة في الأصل، فعلى سبيل المثال الوثيقة المطبوعة من وثائق مايكروسفت لا تظهر جميع التعديلات والملاحظات في حالة ما إذا تم فيها تغيير الوثيقة الأصلية. بالإضافة إلى ذلك أن الأصول في بعض العمليات التي تجري عن طريق الحاسب قد لا تعود موجودة، وربما لم يكن لها وجود أصلا، كما في حالة التحليلات أو الإسقاطات المعالجة[1].

ان عملية الحصول على مخرجات الحاسوب والأنترنت بقصد تقديمها كدليل في المحكمة تعد من أولى الموضوعات التي تعرض لها الفكر القانوني سواء من حيث قابليتها القانونية أو من حيث منهجية الدليل الذي تم تخريجه، بحيث تعد هذه المخرجات أدلة أصلية على الرغم من كونها نسخ من دليل أصله موجود في العالم الافتراضي أو في الحاسوب، فتعامل هذه المخرجات على هذا النحو، والأمثلة الدارجة في هذا الإطار ممثلة في الأدلة الناجمة عن العدوان الإجرامي على حقوق الملكية الأدبية والفكرية، حيث تعد النسخ التي يتم تخريبها من المصنفات وطرحها في شكل ورقي أو تسجيلات أدلة أصلية، كذلك سجل الزيارات الذي يتم رصده في أغلب المواقع والصفحات عبر الأنترنت، حيث يكون هذا السجل معدا بطريق قاعدة البيانات فيعطي الفرصة الكاملة لصاحب الموقع في اختيار الكلمات المعدة للنشر وحذف ما عدى تلك غير اللائقة، إذ لا يكون للمعلومة وجود ما لم يكن لها أصل رقمي يتم بمقتضاه هيكلة المعلومة، فيقوم الخبير برصد قاعدة البيانات باستخدام الشفرة اللازمة وطباعة نسخة من مصنف أو عنوان مصنف أو علامة تجارية أو براءة اختراع أو غير ذلك تم العدوان عليه إجراميا وانتزاع حق المؤلف عنه وبالتالي عرضه كدليل على القضاء دون حاجة للتدقيق في مدى أصالتها ما دامت قد تم تخريجها من حاسوب غير معطوب أو مصاب بخلل برمجي.

[1]– **هشام محمد فريد رستم**، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص 173.

إن تطبيق قاعدة المحور الأصلي- التي يتبناها هذا النظام – من حيث المبدأ على الدليل الإلكتروني لكان مستبعدا كوسيلة إثبات في هذا النظام، وهو ما أدى إلى قلق رجال الضبط القضائي والمدعيين العموميين من أن مجرد مخرجات طابعة ملف إلكتروني مخزن على الحاسوب لا يعد أصليا[1].

الإشكال الذي ينبغي طرحه في هذا المقام هو: ما موقع الدليل الإلكتروني من هذه القواعد، فهل يتم رفضه ومن ثم استبعاده كدليل إثبات جنائي، أم يتم قبوله، وعلى أي أساس يكون هذا القبول؟ وهذا ما يحاول الإجابة عليه في الفرع الثاني.

الفرع الثاني

الاستثناءات الواردة على القواعد التي تحكم النظام الأنجلوسكسوني

يعتبر من أول وهلة بعد هذه المناقشة أن الدليل الإلكتروني، دليل غير مقبول، إلا أن الحقيقة غير ذلك، لأن المشرع في الأنظمة الأنجلوسكسونية وضع قائمة من الاستثناءات على هذه القواعد.

أولا: الدليل الإلكتروني مقبول استثناء من قاعدة استبعاد شهادة السماع

إن المشرع في الأنظمة الانجلوسكسونية وضع قائمة من الاستثناءات على قاعدة شهادة السماع ومن بينها البيانات والمعلومات التي يتم الحصول عليها من الكمبيوتر، حيث يكون هذا الأخير مقبولا في الإثبات شأنه شأن غيره من الأدلة.

أهم الحالات الاستثنائية التي يتم فيها قبول شهادة السماع كدليل في الدعوى الجنائية هي:

أقوال المجني عليه التي نطق بها قبل وفاته، اختبار أحد أعضاء الاتفاق الجنائي، التسجيلات الرسمية، البيانات والمعلومات التي يتم الحصول عليها من الكمبيوتر، تنكر الماضي بالوقائع، التقرير التلقائي، النطق بمفهوم الانطباعية[2].

هكذا يتبين أن الدليل الإلكتروني يدخل في طائفة الحالات الاستثنائية عن قاعدة شهادة السماع ليصبح هذا الدليل مقبولا في الإثبات الجنائي.

---

[1] – **عمر محمد بن يونس**، الإجراءات الجنائية عبر الأنترنت، مرجع سابق، ص 440.

[2] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 129.

إنّ قبول المشرع الإنجليزي للدليل الإلكتروني كدليل في الإثبات الجنائي وذلك خروجا من الأصل العام الذي يتبناه القانون الإنجليزي في عدم قبول الشهادة السماعية، يترتب عنه عدة شروط مهمة نصت عليها المادة 69 من قانون الشرطة والإثبات الجنائي لسنة 1984 وهو:

- عدم وجود أسباب معقولة للاعتقاد بأن البيان يفتقر إلى الدقة بسبب الاستخدام غير المناسب أو الخاطئ للحاسب.
- أن الحاسب كان يعمل في جميع الأحوال بصورة سليمة، إذا لم يكن كذلك، فإن أي جزء لم يعمل فيه بصورة سليمة أو كان معطلا عن العمل، لم يكن ليؤثر في إخراج المستند أو دقة محتوياته[1]، عليه فإن النيابة العامة إذا استندت على مستند إلكتروني في دعوى جنائية تعين عليها أن تقدم الدليل على أن الجهاز يعمل بطريقة صحيحة.

تجدر الإشارة إلى أن قانون الشرطة والإثبات الجنائي لسنة 1984 السالف الذكر لم يكتف بتحديد الشروط الواجب توافرها في مخرجات الحاسوب كي تكون الأدلة مقبولة أمام القضاء، بل تضمن توجيهات لكيفية تقدير قيمة أو وزن البيان المستخرج عن طريق الحاسب، فأوصت المادة 11 من الجزء 2 من الملحق 9 من القانون السالف الذكر وطبقا للمادة 69 من القانون نفسه، بوجه خاص على مراعاة المعاصرة، أي 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 الحاسوب، لديه دافع لإخفاء الوقائع أو تشويهها[2].

إن قبول الدليل الإلكتروني في الإثبات الجنائي في القانون الأمريكي معلق على شرطين:

- توافر الشروط اللازمة لصحة الشهادة السماعية.
- التأكد من عمل الجهاز نفسه على نحو صحيح حيث أن صحة الدليل الإلكتروني يتوقف على صحة برامج التشغيل الذي يعمل الكمبيوتر بحسب تعليماته، ومن حق المتهم أن تتاح له

[1] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 134.

[2] – **هشام محمد فريد رستم**، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص 178.

الفرصة لإثبات أن برنامج التشغيل يعمل بطريقة صحيحة ومنتظمة [1] ومن أجل ذلك قامت المحاكم الفيدرالية بتقسيم سجلات الحاسوب إلى ثلاثة أنواع:

النوع الأول: سجلات الحاسوب المخزنة computer stored records وهي التي تحتوي على بيانات بشرية مثل المخرجات من برامج الكتابة من الكمبيوتر word.

النوع الثاني: سجلات الحاسوب المتوالدة computer generated records، هنا الجهاز هو الذي يقوم بتدوين البيانات التي تصلح أن تقدم مباشرة إلى المحكمة.

النوع الثالث: سجلات تجمع بين التدخل الإنساني ومعالجة الكمبيوتر.

بعد استعراض الأنواع الثلاثة، فإنه فقط النوع الأول من سجلات الحاسوب الذي يعتبر شهادة سماعية مثلها في ذلك مثل الكلمات أو التقريرات التي يسجلها الإنسان على الأجهزة المختلفة، أما النوع الثاني فليست من قبيل شهادة السماع، وتتوقف قيمته الثبوتية ما إذا كان جهاز الكمبيوتر يعمل بطريقة صحيحة أم لا، أما بالنسبة للنوع الثالث، حتى وإن كان جزء منه يعتبر شهادة السماع وهو الصادر عن الإنسان، إلا أنه لا يعد هذا النوع من قبيل شهادة السماع.

-تطبيقات قبول الدليل الإلكتروني في الإثبات الجنائي:

يظهر قبول الدليل الإلكتروني في الإثبات الجنائي جليا في العديد من القضايا، ففي قضية (R.V Wood) [2] تم العثور في حيازة المتهم على بعض المعادن التي قد سرقت وكانت تركيبة المادة الكيمائية لهذه المعادن مسجلة في الكمبيوتر كدليل، والتساؤل الذي طرح في هذه القضية هو هل يمكن اعتبار هذه الورقة الناتجة عن الكمبيوتر دليلا سماعيا، وبالتالي لا يأخذ به؟

كان رد المحكمة أن الورقة الناتجة عن الكمبيوتر مقبولة وفقا للشريعة العامة وبالتالي لا تعد شهادة سماع وهي تصلح للإثبات.

---

[1] – **Cathy T.H. CHEN, Kai-Yuan Cheng, Sih-Yan LiN** – The Exploration of the Judge's Evaluation of Evidence through Inner Conviction on Whether Internet Messages Can be Evidence for Adultery in the Criminal Law---An Explication by Legal Positivism and Philosophical Theory,p 05,in ; http://www.academic-pub.org/ojs/index.php/IJCSE/article/view/498.consulté le: 21/02/2015

[2] – **شيماء عبد الغني**، مرجع سابق، ص 391.

أيضا قضت محكمة الاستئناءات في إنجلترا بالاتجاه نفسه بقبول الدليل المستخرج من الكمبيوتر في قضية R.V Pettigrew لسنة 1980[1]، والتي تلخص وقائعها في أنه وجد في حيازة المتهم الذي قام بالسطو على البنك أرقام النقود المسروقة والتي كانت مسجلة في كمبيوتر البنك في إنجلترا.

وردت قضية في القضاء الأمريكي تخلص وقائعها في أن " 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 هذا الجهاز بناء على إذن بذلك، وقد تم ضبط ملفات تحتوي على أسماء المتعاملين مع المتهم الأول، دفع أحد هؤلاء المتعاملين بعدم صحة إجراءات الضبط وذلك لسهولة العبث بالبيانات وتغييرها وسهولة إدخال اسمه من طرف المتهم الأول، ومع ذلك رفضت المحكمة هذا الدفع مستندة إلى أنه لا يشترط لصحة إجراءات ضبط بيانات الكمبيوتر أن يتم من جانب الخبير[2].

هكذا إن موقف القضاء الأمريكي جاء مؤكدا للشروط التي وضعها القانون الإنجليزي سالف الذكر.

ثانيا: الدليل الإلكتروني مقبول استثناء من قاعدة المحرر الأصلي

تقررت هذه القاعدة في القانون الأمريكي بموجب المادة 1002 من قانون الإثبات الأمريكي السالف الذكر، والتي جاء نصها الحرفي كالتالي: « باستثناء ما هو مقرر في هذا القانون، فإنه عند إثبات مضمون الكتابة والتسجيل والصورة فإنه يلزم توافر أصل الكتابة والتسجيل والصورة

---

[1] – Sur la recevabilité des imprimés d'ordinateur dans les procédures pénales https://www.lccsa.org.uk/r-v-pettigrew-r-v-newark-1980/. Consulté le 29/01/2015 .

[2] – أدخلت الحكومة الأمريكية طباعة وثائق الحاسوب كدليل، وحكم القضاء بالسجن على جيفت مستندا في ذلك على سجلات الكمبيوتر التي تمت طباعتها من طرف مكتب التحقيقات الفدرالية والتي كان يستعملها الجاني لتتبع معاملات المخدرات.

USA. V. Whitaker, 127F. 3d, 595 ,602 (7th, cir 1997), in ;
https://www.leagle.com/decision/1997722127f3d5951655. consulté le :23/04/2016.

»[1] وهكذا فأن حجية الكتابة أو التسجيل أو الصورة رهن بتقديم الأصل إلا إذا نص على خلاف ذلك.

توسع القانون الأمريكي أكثر حيث قام باعتماد مقياس القانون العام، وذلك في إطار الاعتراف بالنسخة طبق الأصل الفورية الصادرة عن الحاسوب، حيث تعرف المادة 1001(e) من القانون الإثبات الأمريكي النسخة طبق الأصل بأنها: « النسخة الطبق الأصل المنتجة لذات الأثر للنسخة الأصلية.... عن طريق إعادة تسجيلها ميكانيكيا أو إلكترونيا... أو عن طريق وسيلة تقنية أخرى مساوية التي تعيد إنتاجها بدقة كالأصل »[2].

كما جاء في المادة 1003 من القانون سالف الذكر " أن النسخة المطابقة للأصل تقبل إلا إذا:

- أثيرت حولها تساؤلات جدية تتعلق بجديتها وأصالتها.
- إذا كانت الظروف لا تسمح بقبول النسخة المطابقة للأصل لكي تحل محل الأصل.

استدعى الأمر مع كثرة المستندات الإلكترونية إلى تغيير هذه القاعدة لكي تتلاءم مع عصر المعلومات، واستجاب كل من القانون الفدرالي الأمريكي والقانون الإنجليزي حيث تم قبول صور المستندات أو جزء منها– المادة 27 من القانون العدالة الجنائية الإنجليزي لسنة 1988[3] – لهذه المستجدات، وقام بحسم هذه المسألة لصالح الدليل الإلكتروني.

من خلال تعديل قانون الإثبات الفدرالي الأمريكي لسنة 2011، الذي مس المادة 1001 منه، فأن تطور الذي حصل في مجال التشريع لا يقتصر فقط على القواعد الفدرالية للإثبات الأمريكي بل يشمل ذلك القوانين الخاصة بالولايات المتحدة كذلك القائمة في ولاية كاليفورنيا[4]

---

[1] - Rule 1002 of federal rules of Evidence : " To prove the content of a writing, recording, or photograph, the Original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of congress ".

[2] - Rule 1001(e) of Federal rules of Evidence, provides that:" A duplicate is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques. Which accurately reproduces the original"

[3] Section 27 of Criminal justice act 1988, in ;
https://www.legislation.gov.uk/ukpga/1988/33/section/27.

[4] – تنص المادة 1500-5 من قانون الإثبات الكالفورني، على أن: المعلومات المسجلة بواسطة الحاسب أو برامج الحاسب، أو نسخ أيهما لا يجب وصفها أو معاملتها على أنها غير مقبولة بمقتضى قاعدة أفضل الأدلة.
State of California Evidence Code , in ; http://www.clrc.ca.gov/pub/Printed-Reports/Pub064.pdf

وولاية أيْوَا[1]، لكي تشمل الدليل الإلكتروني بشكل موسع، فسمحت بالاعتراف بالمواد المكتوبة، والمسجلة والإلكترونية، لكي تحظى بذات الاهتمام الذي تحظى به الأدلة الأخرى في المحاكم، بالتالي قام المشرع الأمريكي باستخدام مدلول موسع للكتابة والتسجيلات ليشمل كل من الحروف أو الكلمات أو الأرقام أو ما يعادها، مكتوبة على اليد أو المنسوخة على الآلة الكاتبة أو مطبوعة أو تم تصويرها أو اتخذت شكل نبضات مغناطيسية بتسجيل ميكانيكي أو إلكتروني أو أي شكل آخر من تجميع المعلومات[2]، فتم اعتبار الكتابة الموجودة داخل الجهاز في صورة كهرومغناطيسية من قبيل النسخة الأصلية، كما ذهب القانون الأمريكي أبعد من ذلك حال توسعه في مدلول عرض الدليل الإلكتروني، إذ تنص المادة 3/1001 من قانون الإثبات الأمريكي، على أنه: إذا كانت البيانات مخزنة في حاسوب أو جهاز مماثل فان مخرجات الطابعة أو أية مخرجات أخرى يمكن قراءتها بالنظر إلى ما تم إظهارها وتبرز انعكاسا دقيقا للبيانات، تعد بيانات أصلية[3]، يفهم من خلال هذه المادة أن الدليل الإلكتروني المستخرج من الطابعة يعد دليل أصلي كامل.

[1] – جاءت المادة 716-16 من القانون الجديد لجريمة الحاسب لسنة 1984 لولاية أيوا بقاعدة إثبات جديدة تقضي: في أحوال الاتهام بمقتضى هذا الفصل، تكون مخرجات الحاسوب مقبولة كدليل على الكيان المنطقي أو البرامج أو البيانات التي يحتويها حاسب أو البيانات التي تؤخذ منه، بغض النظر عن تطبيق قاعدة الإثبات تقضي بغير ذلك.
Iowa Code §§ 715.1 to 715.8, in ; https://www.law.cornell.edu/cfr/text/12/715.8

[2] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 132.

[3] – roule 1001/3 of federal rule evidence, provides that : if data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original.

المبحث الثاني

القيود الواردة أمام قبول الدليل الإلكتروني

يعد نظام الأدلة المعنوية النظام السائد في التشريع الجزائري يعتمد عليه القاضي في قبول الأدلة المطروحة أمامه، وبمقتضاه يتمتع القاضي بحرية واسعة في تقديرها، حيث يوفر له استقلالا كاملا لتكوين قناعته القضائية بشأن قيمة الأدلة المعروضة عليه، إلا أن المشرع لم يترك هذه الحرية مطلقة بل قيدها وذلك بأن أورد عليها بعض الاستثناءات التي لا يملك القاضي إزاءها أي حرية في قبول الأدلة، لأن السلطة المطلقة مفسدة مطلقة، لذا كان من الضروري رسم ضوابط وأطر معينة يتعين أن تمارس هذه السلطة في نطاقها بحيث لا تنحرف عن الغرض الذي يرجوه المشرع من ورائها، وهو الوصول إلى الحقيقة الفعلية في الدعوى.

رغم عدم اتفاق فقهاء القانون الجنائي على أنواع هذه الضوابط، إلا أنها لا تخرج عن ضوابط تتعلق بمحل القبول وهو الدليل الذي يتأسس عليه اقتناع القاضي، وأخرى تتعلق ببعض الجرائم التي حددت أغلب التشريعات الأدلة التي تقبل في إثباتها، بحيث لا يوجز الإثبات بغيرها، كأدلة إثبات جريمة الزنا[1]، أو أدلة الإثبات الخاصة ببعض المسائل غير الجزائية التي يملك اختصاص النظر فيها بصفة التبعية للدعوى الأصلية والتي تكون أدلة إثباتها قانونية على عكس أدلة الإثبات الجزائية التي هي إقناعيه.

بالرجوع إلى إمكانية القاضي الجزائي الاستعانة بالدليل الإلكتروني للوصول إلى الحقيقة أو لإثبات وقوع الجريمة، هناك قيدا عاما يحد من حرية القاضي في قبول هذا الدليل، وهو قيد

[1]– الأصل أن جريمة الزنا كغيرها من الجرائم التي يجوز إثباتها بكافة طرق الإثبات، إلا أنه ولاعتبارات معينة فقد خص المشرع هذه الجريمة بقواعد إثبات خاصة، إذ حدد أدلة الإثبات وأوردها على سبيل الحصر، بحيث لا يجوز إثباتها إلا بالطرق التي حددها النص دون غيرها، وهذا ما أقرته المادة 341 من قانون العقوبات، وعلة هذا الاستثناء راجع إلى أن هذه الجريمة ذات طبيعة خاصة تميزها عن غيرها من الجرائم لما لها من تأثير سيء ومباشر على الأسرة التي هي أساس قيام المجتمع، ولذلك أراد المشرع أن يأتي بالأدلة عليها من أوراق غير معترض عليها وغير معرضة للتجريح أو الطعن فيها، دون تركها تخضع لقواعد الإثبات العامة، فحصر الأدلة حتى تقتصر الإدانة على الحالات التي لا يرقى إليها الشك وهذه الأدلة هي:

- محضر قضائي يحرره أحد رجال الضبط القضائي عن حالة التلبس.
- إقرار وارد في رسائل ومستندات صادرة من المتهم.
- إقرار قضائي، أي اعتراف المتهم أمام القضاء بأنه قام فعلا بارتكاب جريمة الزنا.

المشروعية، حيث يشترط لكي يتمكن القاضي من الاعتماد على دليل معين في الإدانة أن يكون قد تم الحصول عليه بطريقة مشروعة.

على ضوء ما تقدم، سيتم تبيان القيود المتعلقة بمحل الاقتناع (المطلب الأول)، ثم دراسة القيود المفروضة بمقتضى نصوص قانونية محددة (المطلب الثاني).

المطلب الأول

القيود المتعلقة بمحل القبول

إن قبول القاضي الجزائي بالأدلة الإلكترونية يؤسس على ضابطين، يتمثل الأول في ضرورة أن يكون الدليل إلكتروني مشروع، أما الثاني، فينبغي أن يكون الدليل من الأدلة الوضعية، أي مطروحة أمامه في الجلسة ضمن أوراق الدعوى لكي يتاح للخصوم إمكانية مناقشة هذا الدليل والرد عليه.

سيحاول تناول في الفرعين التاليين، مشروعية الدليل الإلكتروني (الفرع الأول) ووضعية الدليل الإلكتروني (الفرع الثاني).

الفرع الأول

مشروعية الدليل الإلكتروني

تقوم الخصومة الجنائية على ضمان حرية المتهم لا على مجرد إثبات سلطة الدولة في العقاب، بالتالي يتعين على القاضي ألا يثبت توافر هذه السلطة اتجاه المتهم إلا من خلال إجراءات مشروعة تحترم فيها الحريات وتؤمن فيها الضمانات التي رسمها القانون[1].

إن مبدأ المشروعية يحكم الدولة القانونية، يلزم أجهزتها الإدارية والقضائية سواء بسواء باحترام القواعد العامة التي حددها القانون لضمان احترام الحريات الفردية وحياة الأفراد في المجتمع[2].

---

[1]– **Jean François RENUCCI**, "La loyauté dans la reconnaissance de la preuve", RSC, 2007, p 895.

[2] – **عبد الفتاح عبد اللطيف حسين الجبارة**، الإجراءات الجنائية في التحقيق، الحامد للنشر والتوزيع، عمان، 2015، ص 198.

ان شرط مشروعية الدليل لقبوله من طرف القاضي، لا يقصد به أن يكون الدليل صريحا ومباشرا في الدلالة على ما يستخلص منه، فالقاضي له أن يكون عقيدته عن الصورة الصحيحة لواقعة الدعوى واستظهار الحقائق القانونية المتصلة بها من جميع العناصر المطروحة عليه[1] بطريقة الاستنتاج والاستقراء وكافة الإمكانيات العقلية، ولا يعيب الحكم استناده على دليل غير مباشر، فالقانون يترك للقاضي الجزائي الحرية في أن يستمد اقتناعه من أي دليل وبأية وسيلة يراها موصلة إلى الحقيقة، إلا أن هذه الحرية لا تعني أن القاضي الجزائي يمكنه أن يبني عقيدته على أي دليل يظفر به مهما كان مصدره ووسيلة البحث عنه، بل هو ملزم بضرورة أن يكون الدليل الذي يستند إليه في حكمه مقبولا في الدعوى ولن يكون كذلك إلا بعد تيقنه من مراعاة الدليل لقاعدة المشروعية[2] باتفاقه مع النظام القانوني في جملته، ويستبعد سائر الأدلة غير المقبولة، لأنها لا يمكن أن تدخل عنصرا من عناصر تقديره[3] بل مخالفة هذا الشرط قد يهدر قيمة الدليل ويبطله.

يقصد بمبدأ مشروعية الدليل ومن ثم قبوله في الإثبات –بما يتضمنه من أدلة مستخرجة من وسائل إلكترونية كالكمبيوتر مثلا– إجراء عملية البحث عنه والحصول عليه وإقامته أمام القضاء في إطار أحكام القانون واحترام قيم العدالة وأخلاقياتها التي يحرص على حمايتها، وإذا كان المشرع يلقي على كاهل المحقق مهمة كشف الحقيقة بجمع أدلة الجريمة فإن عمله مشروط بأن يتم في رحاب المشروعية باحترام حقوق الأفراد وعدم المساس بها إلا في الحدود التي يقررها القانون كذلك يجب أن تكون طريقة الحصول على الدليل لا تتعارض مع القواعد الجوهرية للإجراءات الجزائية والمبادئ القانونية العامة فإن تجاوز المحقق هذه الحدود، وتمكن من الحصول على دليل يثبت وقوع الجريمة وجب طرح هذا الدليل وعدم قبوله في الإثبات[4]، وذلك تماشيا مع التوصية رقم 18

---

[1] – ضمن القيود التي ترد على مبدأ حرية القاضي في الاقتناع أن يكون الدليل أصل في أوراق الدعوى . **جميل عبد الباقي الصغير**، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص 19.

[2] – راجع كل عن: **عائشة بن قارة مصطفى**، مرجع سابق، ص 138.

Geoffroy HILGER, Droit pénal général, édition Ellipses,2017,p29

[3] – **أنس كيلاني**، موسوعة الإثبات في القضايا الجزائية، دار الأنوار للطباعة، دمشق، 1991، ص 144.

[4] –**Djavad FOUROUTANI**, Le fardeau de la preuve en matière pénale essai d'une théorie générale, thèse pour obtenir le grade de docteur, Paris 2, 1977, p 26.

للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات[1]. وما يجب التطرق إليه في هذا الصدد مسألتين، الأولى قيمة الدليل الإلكتروني غير المشروع في الإثبات الجنائي، الثانية مدى إمكانية قبول دليل إلكتروني غير مشروع وذلك حماية للمصلحة العامة على حساب المصلحة الخاصة للأفراد.

أولا: قيمة الدليل غير المشروع

يميز في ذلك بين نوعين من الأدلة، دليل الإدانة، دليل البراءة.

أ- بالنسبة لدليل الإدانة:

انطلاقا من قاعدة أن الأصل في الإنسان البراءة، فإن المتهم يجب أن يعامل على أساس أنه برئ في مختلف مراحل الدعوى إلى أن يصدر بحقه الحكم النهائي، وهذا يقتضي أن تكون الأدلة التي يؤسس عليها حكم الإدانة مشروعة سواء كانت أدلة تقليدية ناجمة عن الوسائل الإلكترونية بصفة عامة، ومن أمثلة الطرق غير المشروعة التي يمكن أن تستخدم في الحصول على الأدلة الناتجة عن الجرائم المعلوماتية الإكراه المادي والمعنوي في مواجهة المتهم المعلوماتي من أجل فك شفرة نظام من النظم المعلوماتية أو الوصول إلى دائرة حل التشفير أو الوصول إلى ملفات البيانات المخزنة، أو التحريض على ارتكاب الجريمة المعلوماتية من قبل العضو المتسرب، كالتحريض على الغش أو التزوير المعلوماتي أو التجسس المعلوماتي والاستخدام غير المصرح به للحاسوب والتصنت والمراقبة الإلكترونية عن بعد[2]، فأي دليل يتم الحصول عليه بطريقة غير

---

[1] – أوصى المؤتمر الدولي الخامس العاشر للجمعية الدولية للقانون العقوبات الذي عقد في ريو دي جانيرو بالبرازيل 4-9 سبتمبر 1994، في مجال حركة إصلاح إجراءات الجزائية وحماية حقوق الإنسان بمجموعة من التوصيات منها التوصية 18، التي تنص على أن: كل الأدلة التي تم الحصول عليها عن طريق انتهاك حق أساسي للمتهم والأدلة الناتجة عنها تكون باطلة ولا يمكن التمسك بها أو مراعاتها في أي مرحلة من مراحل الإجراءات، وقد أشار المؤتمر إلى ضرورة احترام مبدأ المشروعية عند البحث عن الدليل في الجرائم المعلوماتية وألا ترتب عليه بطلان الإجراء فضلا عن تقرير المسؤولية الجزائية لرجل السلطة العامة الذي انتهك القانون.

congrès international de droit pénal, 15ème, Rio De Janeiro, cité précédemment.

[2] – **علي حسن طوالبه**، "مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي دراسة مقارنة"، مقال مقدم إلى مركز الإعلام الأمني، البحرين، 2009، ص 7، محمول من الموقع الإلكتروني التالي: http://www.policemc.gov.bh/mcms-store/pdf/ تم الاطلاع عليه يوم: 2016/02/23.

مشروعة يتم إبطاله بما في ذلك الدليل الإلكتروني، وعدم إنتاج الإجراء الباطل للآثار التي تترتب عليه مباشرة، لم يتضمن قانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أية أوضاع خاصة وترك الأمر للقواعد العامة، ومنها أن الأصل في الأدلة مشروعية وجودها ومن ثم فإن الدليل الإلكتروني سيكون مشروعا من حيث الوجود اصطحابا للأصل.

حدد قانون الإجراءات الجزائية الجزائري وذلك في نص المادتين 157-1 والمادة 191 أن الإجراء الباطل يمتد بطلانه إلى الإجراءات اللاحقة له مباشرة حيث إذا أوجب القانون مباشرة إجراء معين قبل آخر، بحيث يصبح الأول بمثابة السبب الوحيد للإجراء الذي تلاه كان الإجراء الأول شرطا لصحة الإجراء التالي له، فإذا بطل ترتب عليه بطلان الإجراء الذي بني عليه [1].

ان قانون الإجراءات الجزائية الفرنسي في إطار مشروعية الأدلة الإلكترونية، ورغم أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة، إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية أم في مجال التنقيب في الجرائم المعلوماتية، كان المحققون يستخدمون طرقا معلوماتية في أعمال التنصت على المحادثات الهاتفية، ويشير رأي فقهي فرنسي إلى أن القضاء قد قبل استخدام الوسائل العلمية الحديثة في البحث والتنقيب عن الجرائم تحت تحفظ أن يتم الحصول على الأدلة الجنائية خاصة منها المعلوماتية بطريقة مشروعة ونزيهة[2]، أما مضمون قاعدة مشروعية الدليل في النظام الأنجلوسكسوني، فهناك فروق بين القانونين الإنجليزي والأمريكي حول مدى قبول أو استبعاد الدليل غير المشروع[3].

---

[1] – **أحمد فتحي سرور**، نظرية البطلان في قانون الإجراءات الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1959، ص 382.

[2] – راجع كل عن: **هلالي عبد اللاه أحمد**، حجية المخرجات الإلكترونية، مرجع سابق، ص 121- 122. **على حسن الطوالبة**، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، مرجع سابق، ص9.

[3] – **Henri LECLERC**, « L'intime conviction du juge, norme démocratique de la preuve »,p207, in ; https://www.u-picardie.fr/curapp-revues/root/35/henri_leclerc.pdf_4a081ebec92b4/henri_leclerc.pdf, Consulté le :10/03/2016.

ان القاعدة الأساسية في النظام الإنجليزي هي متى كان الدليل منتجا في الإثبات فهو مقبول، أيا كانت الطريقة التي تم الحصول عليها من خلالها، أي حتى ولو كان ذلك بطريقة غير مشروعة[1].

صدر قانون الشرطة والإثبات الجنائي في سنة 1984 الذي تم العمل به منذ 1986، جاء ليعالج اختصاص الشرطة وقواعد الإثبات الجنائي على نحو يحقق ضمانات إجرائية هامة تفيد منها إدارة العدالة الجنائية، وقد تضمن هذا القانون أحكام تنظم استبعاد الأدلة غير المشروعة، إلا أنه لم يوجد أي معيار محدد يوضح متى تكون الإجراءات نزيهة أو غير نزيهة، بل كل ما بينه هو ألا يؤثر الدليل على نزاهة الإجراءات، وحسب المادتان 76 و78 منه تبقى السلطة التقديرية للقضاة في استبعاد الدليل[2] حيث للقاضي السلطة في عدم قبول الدليل إذا كانت القواعد الخاصة بالقبول ستؤدي إلى نتيجة غير عادلة ضد المتهم، فإذا تم تحصيل بعض الوثائق من المتهم بطريقة الخداع لاستخدامها كدليل ضده، لا شك أن القاضي له أن يستبعدها[3]، قامت الشرطة البريطانية بتركيب جهاز تصنت على خط هاتف إحدى الشاكيات بناء على موافقتها، وبعد ذلك أجرت الشاكية عدة مكالمات هاتفية مع الشخص المشكوك فيه، لكن القاضي استبعد كل هذه التسجيلات لأنها تمت من خلال شرك خداعي[4].

تضمن القانون السالف الذكر تحديد الشروط الواجب توفرها في مخرجات الحاسوب، لكي تقبل أمام القضاء وتضمن كذلك توجيهات في كيفية تقدير قيم البيان المستخرج عن طريق الحاسب، فأوصت المادة 11 منه على مراعاة كل الظروف عند تقييم البيانات الصادرة عن الحاسب لقبولها في الإثبات بوجه خاص مراعاة المعاصرة أي ما إذا كان قد تم تزويد الحاسوب بالمعلومات في وقت معاصر أم لا، وذلك طبقا للمادة 69 من القانون نفسه[5] والتي نصت ثلاثة شروط أساسية وهي:

---

[1] – **أحمد عوض بلال**، قاعدة استبعاد الأدلة المتحصلة بطريقة غير مشروع في الإجراءات الجنائية المقارنة، مرجع سابق، ص 41.

[2] – مأخوذ عن: **عماد عوض عدس**، التحريات كإجراء من إجراءات البحث عن الحقيقة، دار النهضة العربية، القاهرة، 2007، ص 401–402.

[3] – مرجع نفسه، ص 394.

[4] – **هلالي عبد اللاه احمد**، حجية المخرجات الكمبيوترية في المواد الجنائية، مرجع سابق، ص 132.

[5] – **Police and criminal evidance Act 1984**, in ;
http://www.legislation.gov.uk/ukpga/1984/60/pdfs/ukpga_19840060_en.pdf.

- يجب ألا يوجد أساس معقول للاعتقاد أن البيان خاطئ أو غير دقيق.
- يجب أن تكون جميع المكونات المادية للحاسوب تعمل بدقة وعلى نحو متوافق.
- إن أيا من الشروط المحددة المتعلقة بالموضوع يجب أن تخضع لتقدير المحكمة.

أما في القانون الأمريكي فالتطبيق القضائي الأمريكي لقاعدة الاستبعاد أكثر وضوحا من التطبيق القضائي الإنجليزي، ذلك أن نظرية " فاكهة الشجرة المسمومة يجب أن لا تؤكل " تجد لها مكانا مقبولا في التطبيق القضائي الأمريكي دون الإنجليزي، بحيث أن الأصل في القضاء الأمريكي هو التطبيق المطلق للقاعدة والاستثناء هو التطبيق التخييري لها[1].

تأكيدا على ذلك، خصص المشرع الأمريكي مبحثا خاصا وهو المبحث الخامس في المرشد الفدرالي الأمريكي لتفتيش وضبط الحاسوب وصولا إلى الدليل الإلكتروني، يتعلق بـ "علاج انتهاكات قانون المراقبة وقانون التسجيل والتقصي"، ويقصد به علاج بطلان الإجراءات غير المشروعة في الحصول على الدليل الإلكتروني، حيث نص في ذلك على انه يجب على رجال الضبط القضائي والمدعين العموميين سلوك أوامر الباب الثالث – قانون المراقبة – وقانون التسجيل والتقصي، عند التخطيط للمراقبة الإلكترونية، إذ يمكن أن تفسر الانتهاكات عن غرامات وجزاءات مدنية أو جزائية[2].

ب- بالنسبة لدليل البراءة:

تعددت الاتجاهات حول مدى اشتراط المشروعية بوجه عام في قبول دليل البراءة، وتلخص أهم هذه الاتجاهات فيما يلي:

•الاتجاه الأول:

يرى مؤيدي هذا الاتجاه بانه من الضروري التفرقة ما بين إذا كان دليل البراءة قد تم الحصول عليه نتيجة سلوك يعد جريمة أو ما إذا كان قد تم الحصول عليه نتيجة سلوك يشكل

[1] – حددت المحكمة العليا الأمريكية أربعة حالات لا يتم فيها الاستبعاد وهي: توافر حسن النية لدى رجال الشرطة – أن تكون الصلة بين العمل الإجرائي المخالف ضعيفة مع الدليل – قد يتم الحصول على الدليل بصورة مستقلة عن العمل الإجرائي المخالف، أن لا يمكن اكتشاف الدليل إلا بالخروج عن السبيل القانوني الصحيح. **عائشة بن قارة مصطفى**، مرجع سابق، ص 145.

[1]- Rules 103 and 402Federal Rules of Evidence act, 1975, in; www.uscourt-gov/sites/default/Rules%20of20%Evidence

مخالفة لقاعدة إجرائية، فإذا كان الأول وجب إهدار الدليل وعدم الاعتداد به، لأن القول بغير ذلك هو إباحة بعض الجرائم، أما إذا كان الحصول على الدليل يخالف قاعدة إجرائية، فهنا يصح الاستناد إلى هذا الدليل في تبرئة المتهم، لأن البطلان شاب وسيلة التوصل إلى الدليل، ولا يصح أن يضار المتهم بسبب لا دخل له فيه.

•الاتجاه الثاني:

يرى أصحاب هذا الاتجاه، ان شرط المشروعية واجب التطبيق دون النظر إلى الغاية من مجود الدليل البراءة أو الإدانة وبالتالي إثبات البراءة كالإدانة لا يكون إلا من خلال سبل مشروعية ولا يصح أن يتلف إثبات البراءة من قيد المشروعية الذي هو شرط أساسي في جميع التشريعات[1].

•الاتجاه الثالث:

حسب هذا الاتجاه فإن شرط المشروعية هو شرط وجوبي واجب التحقق في الدليل الإدانة دون البراءة، وذلك حسب هذا الاتجاه أن المحكمة لا تحتاج إلى اليقين في إثبات البراءة بل يكفي في ذلك الشك وهو ما يمكن الوصول إليه من خلال أي دليل ولو كان غير مشروع، وحسب هذا الاتجاه فإن تطلب مشروعية دليل البراءة يعرقل حق المتهم في الدفاع عن نفسه، إذ أن له الحرية الكاملة في اختيار وسائل دفاعه[2].

يستنتج أن بدا مشروعية الأدلة لا يجب أن يطغى على مبدأ افتراض البراءة، حيث أي دليل يفيد في إثبات هذا المبدأ الأخير، وجب الأخذ به دون الالتفات لأي اعتبار آخر، لان العدالة تضار بقدر اكبر في حالة إدانة بريء على إفلات مجرم من القضاء.

ثانيا: المصلحة الأولى بالحماية والرعاية

لا يزال هذا العصر ينادي بمبادئ سامية لحماية المتهم والأخذ بالضمانات الكافية أثناء مراحل الخصومة كلها "الاتهام، التحقيق، المحاكمة"، وأصبح من الواجب إتباع وسائل جديدة

[1] – **محمود نجيب حسني**، شرح قانون الإجراءات الجزائية، الطبعة الثانية، دار النهضة العربية، القاهرة،1988، ص 437.

[2] – **محمود محمود مصطفى**، شرح قانون الإجراءات الجنائية، مرجع سابق، ص 424.

تتلاءم مع التطور الجديد بارتكاب الجريمة وأساليبها الحديثة[1]، والتي تحتاج إلى وسائل جديدة لمكافحتها، ولدراسة شخصية المجرم، ووضع أنماط تأهيلية وضمانات حريته الشخصية، وهذا بالفعل ما شغل العلماء والفقهاء، وخصصت له الدراسة والأبحاث وانعقدت من أجله المؤتمرات الدولية، من قبل الهيئات الدولية، ومراكز الدفاع الاجتماعي.

ان للمعلومة الإلكترونية صلة وثيقة بالحق في السرية والخصوصية، ذلك أن هذا المستند قد يحوي بيانات ومعلومات لا يحق للآخرين الاطلاع عليها، وحماية المعلومة الإلكترونية في هذه الحالة تنطوي على حماية الحق في السرية والحق في الخصوصية[2]، يدرج على سبيل المثال نص قانون التخلص من الأوراق الحكومية الأمريكي لسنة 1998 (GPEA) [3] على أن الهيئات الحكومية أن تتخذ الإجراءات اللازمة لحفظ المعلومات الإلكترونية أو تسليمها أو الكشف عنها، كلما كان ذلك ممكنا كبديل للمستندات الورقية؛ كما نص هذا القانون كذلك على وجوب اتخاذ الإجراءات الكفيلة باستخدام وقبول التوقيع الإلكتروني كلما كان ذلك ممكنا، وقد حدد الشارع الأمريكي ميعادا لإنجاز هذه الإجراءات هو الأول من أكتوبر سنة 2003.

يثور التساؤل من ناحية القانون الجزائي الإجرائي حول مدى جواز حرية الإثبات اللجوء إلى الوسائل العلمية خاصة انه قد يترتب على استخدامها اعتداء على حقوق أساسية للإنسان، وبإمكان الملاحظ أن يلحظ التنامي حالياً في اتجاه كثير من الدول نحو الرفع من شأن ضرورة إثبات الجريمة، وإن تتطلب ذلك التجاوز عن بعض المبادئ التي حكمت تقليدياً البحث عن الدليل، فازدياد نسبة الجرائم، وارتفاع حجم خطورتها، كتلك التي تحمل اعتداءً شاملاً على مصالح المجتمع، مثل الإرهاب أو الاتجار بالمخدرات أو غيرها من الجرائم العابرة لحد ود الدول، والتي تمثل عاملاً حاسماً، دفع في

---

[1] - **Jacques BUISSON**, "Captation d'images, application de principe de légalité dans l'administration de la preuve", RSC 2008, p 655.

[2]- **Louis Edmond PETTITI**, « Les écoutes téléphoniques et la protection de la vie privée », RSC 1998, p 829.

[3] - **Governement Paper Work Elimination Act** , Sec. 1702, in ; https://ocio.nih.gov/ITGovPolicy/Documents/Paperwork_Elimination_Act_Public_Law_105-277.pdf.

اتجاه تنامي الفكرة التالية :ضرورة الوصول إلى الحقيقة تسمح بالتجاوز عن بعض المبادئ الإجرائية التي تعتبر ضمن المعايير التي يقوم عليها مفهوم المحاكمة العادلة[1].

إذا تم التسليم بالقول بأن هناك تعدي على حريات الأفراد فإنه تعدي ضئيل جدا للغاية، ومما يتعين الاعتداد به هو مدى خطورة العدوان أو المساس بالنظام الاجتماعي، فلا يمكن استبعاد كل وسيلة لمجرد منافاتها للقواعد العامة دون دراسته أو تعمق لآثارها في المجتمع.

إذا كان البعض يشك في مشروعية الدليل الإلكتروني، باعتباره طريقة للتدخل في الحياة الخاصة للأفراد، لاسيما في مجال الجرائم الجنسية، حيث يكون السلوك الجنسي برضاء المشتركين فيه، إلا أن الاستعانة بالوسائل العلمية الحديثة كالأنترنت واستخدامه كدليل على وقوع جريمة الإعلان عن البغاء ونشر المطبوعات الفاضحة يستهدف المصلحة العامة، وحتى تتمكن الدولة من حماية النظام الاجتماعي حتى لا ينهار بسبب الاحترام المبالغ فيه للحقوق والحريات الخاصة ولا يمكن الاعتراض عليه بحجة عدم مشروعية الدليل الإلكتروني، فكل ما يسفر عنه العلم الحديث يجب أن يستخدم في تحقيق أمن المجتمع.

الفرع الثاني

وضعية الدليل الإلكتروني

ان اهم القواعد الأساسية في الإجراءات الجزائية أنه لا يجوز للقاضي أن يبني حكمه على أدلة لم تطرح لمناقشة الخصوم في الجلسة، وهو ما يعبر عنه بوضعية الدليل.

مقتضى ذلك أن يكون الدليل أصل ثابت في أوراق الدعوى، وغاية ذلك أن يكون الخصوم على بينة مما يقدم ضدهم من أدلة، وأن تتاح لهم إمكانية مناقشتها والرد عليها[2]، ولو لم يناقشوها بالفعل، إذ ليس من الضروري أن تحصل مناقشة علنية، بل يلزم أن تكون الأدلة في متناول الخصوم.

---

[1] – **معتصم خميس مشعشع**، "إثبات الجريمة بالأدلة العلمية"، مجلة الشريعة والقانون، تصدر عن مجلس النشر العلمي كلية القانون، جامعة الإمارات العربية المتحدة، عدد56، أكتوبر 2013، ص 5.

[2] -**CLÉMENT Stéphane,** Les droits de la défense dans le procès pénal : du principe de contradictoire à l'égalité des armes, thèse pour obtenir le grade de docteur, faculté de droit et de sciences politiques, université de Nantes, Nantes, 2007, p 14.

يعد هذا المبدأ أحد القواسم المشتركة بين التشريعات الإجرائية المعاصرة لوجوب أن تكون الجلسة علنية، ولم تزل تحرص الدول على دراستها، كضرورة لضمان حق المحاكمة العادلة.

أولا: علانية المحاكمة

يقصد بعلانية المحاكمة، السماح لجميع الأشخاص بشكل عام حضور جلسات المحاكم ومتابعة كل ما يدور من مناقشات ومرافعات وما يتخذ فيها من إجراءات وما يصدر من قرارات وأحكام، فالأصل في المحاكم هو العلانية والاستثناء هو السرية، بحيث تكون الجلسات، قد جعلت العلانية بالمحاكم، كضمانة أساسية في ضمانات العدالة لصالح المتهم، وترجع أهمية علانية الجلسات إلى بث الطمأنينة في نفوس المجتمع وتأكيد ثقتهم في عدالة القضاة والتزامهم بأحكام القانون.

أجازت اغلب التشريعات للمحكمة – مراعاة للنظام العام والمحافظة على الآداب – أن تأمر بسماع الدعوى كلها أو بعضها في جلسة سرية، أو تمنع فئات معينة من الحضور فيها، وعلة تقرير هذه السلطة هي الحد من مشكلات العلانية. يخضع استعمال هذه السلطة لعدة قواعد مثل أن يصدر القرار بجلسة سرية من المحكمة في كامل هيئه، فلا يجوز أن يصدر عن رئيسها وحده، ويتعين أن يصدر القرار علنا، ويكون مسببا، وتكفي الإشارة إلى أن مقتضيات سرية الجلسة تتطلب ذلك حفاظا على النظام العام أو الآداب العامة فلا يشترط تفصيلها[1]،العبرة لاعتراض المتهم وإذا طلب المتهم أو غيره تقرير السرية، فلا تلتزم المحكمة بإجابته إلى طلبه إذا لم تقتنع بسببه.

ثانيا: مبدأ شفوية إجراءات المحاكمة

يقصد به أن تجري إجراءات المحاكمة شفويا أمام الجمهور الحاضر في الجلسة، ويقوم الشهود والخبراء والمحامون وغيرهم بإدلاء أقوالهم أمام القاضي بالتفصيل شفويا، والأصل في الأحكام الجنائية أن تبنى على المرافعة التي تحدث أمام نفس القاضي الذي أصدر الحكم وعلى التحقيق الشفهي الذي أجراه بنفسه، إذ أساس المحاكمة الجنائية هي حرية القاضي في تكوين عقيدته من التحقيق الشفوي الذي يجريه بنفسه ويسمع فيه الشهود مادام سماعهم ممكنا، مستقلا في

[1] -**إيمان محمد علي الجابري**، يقين القاضي الجزائي، دار منشأة المعارف، الإسكندرية، 2005، ص 84.

تحصيل هذه العقيدة من الثقة التي توحي بها أقوال الشاهد، حتى تؤثر هذه الأقوال في نفس القاضي، وهو ينصت إليها مما يبنى عليه، وعلى المحكمة التي فصلت في الدعوى أن تسمع الشهادة من فم الشاهد إذا كان ممكنا ولم يتنازل المتهم أو المدافع عنه صراحة أو ضمنا. إنّ رؤية القاضي للشاهد الماثل أمامه يعينه على تقدير أقواله حق قدرها لأنه يتفرس في حالة الشاهد النفسية التي تنتابه وقت أداء الشهادة ومراوغاته أو اضطرابه، وغير ذلك.

يحق للمحكمة أن تعتمد على الأقوال والشهادات التي اتخذت في محاضر الجلسات أمام هيئة أخرى أو في التحقيقات الابتدائية أو في محاضر جمع الاستدلالات باعتبارها من عناصر الدعوى المطروحة على بساط البحث، وإذا لم تلتزم المحكمة بذلك، فإنّها تكون قد أخلت بمبدأ شفوية المرافعة وجاء حكمها مشوبا بالإخلال بحق الدفاع ويترتب على الإخلال بقاعدة شفوية المرافعة بطلان الحكم الذي يصدر بالدعوى.

أن الأدلة الإلكترونية سواء كانت مخرجات ورقية يتم إنتاجها عن طريق الطباعات أو الراسم، أو تكون مخرجات غير ورقية إلكترونية – كالأشرطة والأقراص الممغنطة وأسطوانات الفيديو وغيرها من الأشكال الإلكترونية غير التقليدية – أو عرض مخرجات المعالجة واسطة الحاسوب على الشاشة الخاصة به، أو الأنترنت بواسطة الشاشات أو وحدة العرض المرئي[1]، كل هذه ستكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات، يجب أن يعرض في الجلسة بصفة مباشرة أمام القاضي[2].

ان الحديث في هذه المسألة يجر إلى مناقشة مدى تأثير الأصالة الرقمية[3] الدليل الإلكتروني على مبدأ قبوله من طرف القضاء

---

[1] – **هلالي عبد اللاه أحمد**، حجية المخرجات الكمبيوترية في الإثبات الجنائي، مرجع سابق، ص ص 14،22.

[2] – **محمد فهمي طلبه**، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، مطابع المكتب المصري الحديث، القاهرة، 1991، ص 31.

[3] – هناك تمييز حقيقي بين الأصالة للدليل في طابعها المادي وبين الأصالة في طابعها الرقمي من حيث أن الأولى إن هي سوى تعبير عن وضعية مادية ملموسة كما هو الشأن في الورق المكتوب أو بصمة الأصبع أو الحدوث العيني للواقعة في حين أن الثانية ليست سوى تعداد غير محدود لأرقام ثنائية موحدة في الصفر الواحد . **سعيداني نعيم**، مرجع سابق، ص 227.

ثالثا: الأصالة الرقمية للدليل الإلكتروني

تبرز هذه المشكلة بصورة جلية عندما يقوم المتهم بإزالة الدليل الإلكتروني عن بعد، فيكون ما تبقى منه هو مجرد نسخة فقط يتم التوصل إليها عن بعد أيضا بطرق المراقبة الإلكترونية مثلا، ومن ثم فالسؤال هل يكفي ناتج المراقبة الإلكترونية وحده للقول بأن الدليل هو دليل أصلي وبالتالي يقبل طرحه على القضاء ومناقشته ضمن أدلة الدعوى؟ وذات السؤال ينطبق على حالة الدليل المسترد بعدما تم حذفه باستخدام خاصية الإلغاء.

ان مناقشة هذه المسألة من الناحية القانونية دفع بالتشريع المقارن أن يعتمد منطق افتراض أصالة الدليل الإلكتروني، حيث نص قانون الإثبات الأمريكي في المادة 1003-3 أنه إذا كانت البيانات المخزنة في حاسوب أو آلة مشابهة فإن أي مخرجات طابعة منها أو مخرجات مقروءة تبرز انعكاسا دقيقا للبيانات وتعد بيانات أصلية، وتبرز أهمية التسليم بمنطق افتراض الأصالة في الدليل الإلكتروني على المستوى القانوني ذلك أن الطبيعة التقنية للدليل الإلكتروني لا تعبر عن قيمة أصلية بمجرد رفع محتواه في النظام المعلوماتي إذ يبقى متواجدا في كل مكان يتم استدعاءه منه[1].

كل هذه ستكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات، يجب أن يعرض في الجلسة ليس من خلال ملف الدعوى في التحقيق الابتدائي، لكن بصفة مباشرة أمام القاضي، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحاسوب، وأيضا بالنسبة للشهود في الجرائم المعلوماتية الذين يكون قد سبق أن سمعت أقوالهم في التحقيق الابتدائي، فإنه يجب أن يعيدوا أقوالهم مرة أخرى من جديد أمام المحكمة، كذلك فإن خبراء الأنظمة المعلوماتية على اختلاف تخصصاتهم[2] ينبغي أن يمثلوا أمام المحاكم لمناقشة تقاريرهم التي حصلوا إليها لإظهار الحقيقة.

أرست هذا الضابط المادة 212-2 من قانون الإجراءات الجزائية الجزائري إذ تنص « ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت

[1] – **محمد بو بكر بن يونس**، الجرائم الناشئة عن استخدام الأنترنت، مرجع سابق، ص 973.

[2] – **محمد فهمي طلبه**، مرجع سابق، ص 31 .

المناقشة فيها حضوريا أمامه » ومن القواعد العامة المستقرة في القانون الجنائي عدم قبول البينة السماعية أمام المحاكم الجنائية، إلا في حالات استثنائية حصرها القانون بشروط مشددة، ويعزى عدم قبول البينة السماعية إلى استحالة استجواب ومناقشة الشاهد الأصلي بواسطة المحكمة والدفاع، وعلى سبيل المثال، لقد تضمنت القواعد الفدرالية الأمريكية نصا يعتبر السجلات والبيانات المنظمة بدقة بينة مقبولة أمام المحاكم الجنائية استثنائيا للبيئة السماعية، وبناء على تلك القواعد تعد التقارير والمعلومات والبيانات المحفوظة في أي شكل، وكذلك الوقائع والأحداث والآراء ونتائج التحاليل المنقولة بواسطة أصحاب المعرفة والخبرة في نطاق الأنشطة والممارسات المنظمة بيئة مقبولة أمام المحاكم الجنائية لكونها بيانات كأثر دقة ومحفوظة بأسلوب علمي يختلف عن غيرها من الأدلة السماعية، والأدلة الجنائية الإلكترونية من هذا القبيل بكونها معدة بعمليات حسابية دقيقة لا يتطرق إليها الشك ويتم حفظها كليا بأسلوب علمي[1].

إذا كان القاضي يلتزم بأن يستمد اقتناعه من الأدلة الإلكترونية التي طرحت في جلسات المحاكمة وأتيحت لأطراف الدعوى مناقشتها، فمن أهم النتائج التي تترتب على هذه القاعدة حتميا نتيجتان:

- النتيجة الأولى: هي عدم جواز قضاء القاضي استناد إلى معلومات الشخصية أو إلى رأي غيره.

يقصد بالعلم الشخصي للقاضي، معلوماته الشخصية التي يكون قد حصل عليها من خارج نطاق الدعوى المطروحة عليها والتي من الممكن أن تؤثر في تكوين قناعته عند تقديره لأدلتها[2].

لا يجوز للقاضي أن يبني اقتناعه على هذه المعلومات الشخصية، لأنها من جهة لم تكن موضع مناقشة شفوية بحضور أطراف الدعوى، بل تكون لهم في الحقيقة مفاجأة أن لم تناقش بمعرفتهم ولم يتم إثباتها في إطار إجراءات الخصومة، مما يؤدي إلى عدم احترام حقوق الدفوع،

---

[1] – **محمد الأمين البشري**، "الأدلة الجنائية الرقمية، مفهومها ودورها في الإثبات"، المجلة العربية للدراسات الأمنية والتدريب، تصدر عن جامعة نايف العربية للعلوم الأمنية، الرياض، المجلد 17، العدد 33، أبريل 2002، ص 129.

[2] – **نبيل إسماعيل عمر**، "قاعدة عدم القضاء بعلم الشخص للقاضي في الشريعة الإسلامية والقانون الوضعي"، مجلة الدفاع الاجتماعي، تصدر عن المنظمة العربية ***للدفاع الاجتماعي*** ضد الجريمة الرباط، المغرب، العدد الأول، 1984، ص 41.

ولان القاضي من جهة ثانية يكون قد جمع في شخصه صفتين متعارضتين صفة الشاهد وصفة القاضي، وهذا ما لا يجيزه القانون ويرتب عليه بطلان الحكم[1]، ويرجع السبب في ذلك: إلى أن من مستلزمات تقدير القاضي الجزائي للأدلة بصفة عامة والدليل الإلكتروني على الخصوص، خلو ذهنه من أي معلومات مسبقة بشأنه، فلا تتم عملية التقدير إلا من خلال طرحه وبيان موقف الخصوم منه، وعندئذ يستطيع القاضي من خلال هذه المناقشة الوصول إلى التقدير السليم، وفي هذا الخصوص يقول الفقيه الإنجليزي Sydney Fipson ليس للقاضي أن يتصرف على أساس من علمهما الخاص، لكن إن كان لديهما وقائع مادية يريدان الإدلاء بها، فيجب أن يحلف كشاهد وليس كقاضي[2]. أما المعلومات العامة المستسقاة من خبرة القاضي بالشؤون العامة المفروض إلمام الكافة بها، فهي لا تعد من قبيل المعلومات الشخصية الممنوعة على القاضي أن يبني حكمه عليها.

تجدر الإشارة في هذا المقام، إلى انه ليس للقاضي أن يبني اقتناعه على رأي غيره، إلا إذا كان هذا الغير من الخبراء وقد ارتاح ضميره إلى التقرير المحرر منه فقرر الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة عليه يكون متولدا من عقيدته هو وليس من تقرير الخبير[3].

- النتيجة الثانية: هي ضرورة التأهيل التقني والفني للقضاة لمواكبة المناقشة العلمية لأدلة الحاسوب والأنترنت بشكل يتماشى والتقارير التي تم تقديمها في المؤتمرات الخاصة بجرائم الحاسوب والأنترنت [4].

---

[1] – راجع كل عن: **جندي عبد المالك**، الموسوعة الجنائية، الجزء الأول، منشورات الحلبي الحقوقية، بيروت، 2010، ص 261. **رأفت عبد الفتاح حلاوة**، الإثبات الجنائي قواعده وأدلته، دار النهضة العربية، القاهرة، 2003، ص 62.

[2] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 178.

[3] – **عائشة بن قارة مصطفى**، مرجع نفسه، ص 178.

[4] – **رشيدة بوكر**، مرجع سابق، ص 323.

المطلب الثاني

القيود الواردة من نصوص القانونية خاصة

هناك قيود أخرى ترد على سلطة القاضي الجزائي في قبول الدليل الإلكتروني، وهي محدودة بنصوص قانونية خاصة، وتنحصر في نوعين من القيود، يتمثل الأول في التقيد بأدلة معينة في جريمة الزنا، أما الثاني فيتعلق بطرق الإثبات الخاصة بالمواد غير الجنائية.

سيحاول معرفة موقف الدليل الإلكتروني من هذه القيود، فهل تطبق عليه هذه القيود شأنه في ذلك شأن أي دليل جنائي تقليدي، أم يستثنى من هذه القيود من خلال الفرعين التاليين، قيد تحديد الأدلة في جريمة الزنا(الفرع الأول) وقيد إثبات المسائل غير الجنائية(الفرع الثاني).

الفرع الأول

قيد تحديد الأدلة في جريمة الزنا

خرج المشرع عن مبدأ حرية الإثبات من خلال تقييد إثبات جرائم معينة بأدلة يحددها، يتضمن قانون العقوبات الجزائري العديد من النصوص التي تقيد حرية الإثبات، كما هو الحال بالنسبة لإثبات جريمة الزنا.

المبدأ الذي يسود الإثبات الجنائي، هو عدم حصر الأدلة في نوع معين منها، فجميعها مقبولة في الإثبات إذا تحصلت بصورة مشروعة طبقا للقواعد الإجرائية الخاصة بتحصيلها، ولكن المشرع حدد الأدلة المقبولة في إثبات بعض الجرائم، حيث لا يجوز الإثبات بغيرها، كجريمة زوج الزوجة الزانية، بحيث تقبل فقط الأدلة المعدة للإثبات مسبقا[1].

---

[1] – Art. 324 du **Code pénal français de 1810**, in ;
http://www.koeblergerhard.de/Fontes/CodePenal1810.htm .
disait «Le meurtre commis par l'époux sur l'épouse, ou par celle-ci sur son époux, n'est pas excusable (...) Néanmoins, dans le cas d'adultère, prévu par l'article 336, le meurtre commis par l'époux sur son épouse, ainsi que sur le complice, à l'instant où il les surprend en flagrant délit dans la maison conjugale, est excusable.»

لكن في 1975 لم يعد الزنا مجرما جنائيا بمقتضى التعديل الذي ألغى جريمة الزنا في هذا القانون.

أولا: الأدلة المقبولة في جريمة الزنا

حصر قانون العقوبات الإنجليزي الأدلة المقبولة في جريمة الزنا في المواد116-138 التي تشمل الجنح المخلة بالآداب والأسرة، كالزنا واتخاذ الزوج خليلة له جهارا في أي مكان، والسفاح بين الأصول والفروع[1]، أما في الولايات المتحدة الأمريكية، لا تعد الزنا جريمة في أكثر من نصف عدد الولايات المتحدة.

نص المشرع الجزائري على هذه الجريمة في نص المادتان 339 و341 من قانون العقوبات الجزائري، فأوجب أن تكون الزوجة المزني بها في ظروف لا تترك مجالات للشك عقلا في أن جريمة الزنا قد ارتكبت فعلا، فإذا بين الحكم الوقائع التي ستظهر منها حالة التلبس وكانت هذه الوقائع كافية وصالحة لمعرفتها، فلا وجه للاعتراض على أن الأمر لا يعدو أن يكون شروعا في ارتكاب الزنا[2] لأن تقدير هذه الحالة يرجع لسلطة قاضي الموضوع ولا وجه للطعن عليه فيه. جعل القانون مجرد وجود رجل في المنزل المخصص للحريم دليلا على الزنا كونها جريمة تامة لا مجرد الشروع. كما أن عدم جواز إثبات التلبس بشهادة الشهود لم يقرره القانون إلا في باب الزنا، لأنه من المتفق عليه قانونا، ليس من الضروري أن يشاهد الشريك متلبسا بالجريمة بواسطة أحد ضباط الشرطة القضائية.

استناداً إلى هذه الحقيقة فإن قضاء محكمة النقض الفرنسية يذهب إلى أنه لا يترتب على تعيين المشرع أدلة محددة في إثبات جريمة معينة الامتناع عن استخدام أدلة أخرى في إثباتها، إلا في الحالة التي يمنع نص القانون ذلك صراحة[3]، وقد طبق القضاء الفرنسي هذا الاجتهاد في العديد من القضايا، ذهب في إحدى القضايا إلى استنباط النتيجة التالية :إن نص المشرع على إثبات الجريمة بواسطة الأدلة التي تعدها الضبطية القضائية بالنسبة للجرائم التي كلفوا بإثباتها بموجب أحكام القوانين الخاصة، فيمنع من إثبات هذه الجرائم من خلال أدلة أخرى تنظمها الضبطية القضائية[4].

---

[1] – **The Penal code and Subsidiary Legislation in England** , Revised Edition showing the law as at 1 January 2008,in ; http://agc.gov.ms/wp-content/uploads/2010/02/penal_code.pdf.

[2] –**عبد الحميد الشواربي**، جريمة الزنا في ضوء القضاء والفقه، دار المطبوعات الجديدة، الإسكندرية، 1985، ص 50.

[3] – Cass. Crim. 28 nov. 2001,n° 01-86.467, in; www.legifrance.gouve.fr/affichJuriJudi.do?idtext=JURITEXT000007068863 . consulté le 23/04/2016.

[4] – **S GUINCHARD, J BUISSON** , Procédure pénale, Litec, 2ème édi. , 2002, p.460

أورد المشرع الجزائري الأدلة التي تقبل وتكون حجة دون غيرها في إثبات جريمة الزنا، وذلك على سبيل الحصر لا المثال، وذلك في المادة 341 من القانون العقوبات الجزائري[1]، التي تنص على ان:" الدليل الذي يقبل عن ارتكاب الجريمة المعاقب عليها بالمادة 339 يقوم إما على محضر قضائي يحرره أحد رجال الضبط القضائي عن حالة تلبس وإما بإقرار وارد في رسائل أو مستندات صادرة من المتهم وإما بإقرار قضائي".

أكدت المحكمة العليا الجزائرية نص هذه المادة بأن جريمة الزنا المعاقب عليها في المادة 339 من قانون العقوبات لا تثبت إلا بالطرق التي أوردها المشرع على سبيل الحصر في المادة 341 من القانون نفسه، وأن قضاة الموضوع عندما أدنوا المتهمين بجريمة الزنا على قرائن لم تنص عليها المادة 341 من قانون العقوبات فإنهم بقضائهم كما فعلوا قد خرقوا القانون[2]

ثانيا: قبول الدليل الإلكتروني لإثبات جريمة الزنا

انطلاقا من المفهوم الحرفي للمادة 341 قانون العقوبات الجزائري، فإنه لا يجوز للقاضي الجنائي أن يقبل لإثبات الزنا أدلة أخرى ولو كان إلكترونيا سواء كان عبارة عن صور، فيديو أو رسائل مرسلة عن طريق الهاتف المحمول SMS أو عن طريق الأنترنت E-mail سواء تضمنت هذه الرسالة اعترافا صرحا أو ضمنيا بوقوع الزنا، أو فيها نوع من الكلام الذي يوحي بممارسة علاقة غير شرعية.

من أجل سد الفراغ التشريعي الواقع في أغلب التشريعات المعاصرة، تقوم بقياس الكتابة الإلكترونية المكاتيب والأوراق، خاصة وأن المشرع الجزائري في تعريف الكاتبة حيث نص في المادة 323 مكرر من القانون المدني[3]، بل أكثر من ذلك فقد سوى بين الكتابة والشكل الإلكتروني والكتابة على الورق وذلك بشرط إمكانية التأكد من هوية الشخص الذي أصدرها بالكتابة الإلكترونية خاصة وأن القانون لم يشترط في المكاتيب والأوراق التي تكون دليلا على فعل الزنا أن تكون موقعة من المتهم، طالما كان من الثابت صدورها منه، وتبقى للقاضي في الأخير

[1] – امر رقم 66–156 المؤرخ في مؤرخ في 18 صفر عام 1386 الموافق ل 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية عدد 49 بتاريخ 11 جوان 1966 المعدل والمتمم

[2] – قرار المحكمة العليا، غرفة الجنح، صادر بتاريخ 1989/07/02 ملف رقم 059100، المجلة القضائية، العدد الثالث، 1991، ص 112.

[3] – امر رقم 75–58 المؤرخ في 20 رمضان عام 1395 الموافق ل 26 سبتمبر 1975، المتضمن قانون المدني، الجريدة الرسمية للجمهورية الجزائرية عدد 78 بتاريخ 30 سبتمبر 1975، المعدل والمتمم.

السلطة التقديرية في تقدير قيمة هذه المكاتيب والأوراق مهما تجسدت في أي صورة، وينبغي على القاضي في هذه الحالة أن تكون له ثقافة معلوماتية واسعة حتى يستطيع دراسة هذا النوع المستحدث من الأدلة، لاسيما أنه قابل للتعديل وبإمكانه أي شخص أن يتقمص شخصية معينة وذلك للإضرار بالشريك أو غيره[1].

لذلك كان من الأجدر بالمشرع الجزائري أن ينص على الدليل الإلكتروني ضمن أدلة إثبات الزنا وذلك سدا للفراغ التشريعي الذي أصبح جليا في أغلب التشريعات خاصة العربية منها.

الفرع الثاني

قيد إثبات المسائل غير الجنائية

تطرح المحاكم الجنائية بعض القضايا، التي لا يمكن الفصل فيها مباشرة، بل لأجل ذلك، لا بد الفصل أولا في بعض المسائل غير الجنائية التي تكون مقدمة ضرورية للفصل في الدعوى الجنائية، يشترط في هذه المسائل الأولية غير جنائية أن تكون عنصرا مفترض في الجريمة، سابقة في وجودها على ارتكاب الفعل الإجرامي.

أولا: شروط تقيد القاضي الجزائي بقواعد الإثبات الخاصة غير الجنائية

إن إثبات المسائل غير الجنائية الأولية سواء كانت مدنية أو تجارية يخضع للقانون الخاص، وهذا لأن قواعد الإثبات ترتبط بالموضوع التي ترد عليه لا بنوع المحكمة.

يتقيد القاضي الجزائي بطرق الإثبات الخاصة بالمواد غير الجنائية بمعنى أنه قد تتكون عناصر الجريمة من فروع مدنية أو تجارية أو أحوال شخصية، فيتوجب على القاضي الجزائي الفصل في تلك المواد غير الجنائية –طالما أنها مرتبطة بالدعوى الجنائية– بطرق الإثبات الخاصة بها ومثالها عقد الإيجار في الجرائم المنصوص عليها في قانون إيجارات الأماكن، وإثبات عقود الأمانة في جريمة خيانة الأمانة.

يشترط لالتزام القاضي باتباع طرق الإثبات المقررة في القوانين الجنائية للدعوى المطروحة أمامه شرطين هما:

[1] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 148.

– ألا تكون الواقعة محل الإثبات هي محل التجريم، كخيانة الأمانة، فإنّ الجريمة ليست في العقد الذي حدث الإخلال به، وإنما هي في الإخلال والثقة، أي يتعلق الإثبات فيها بوصف المتهم المسلم إليه المال وتبديده، وبهذا يمكن للقاضي الجنائي إثبات هذا التصرف بكافة طرق الإثبات لأنه يعد هو السلوك الإجرامي الذي يعاقب عليه القانون.

– أن تكون الواقعة المتعلقة بالقوانين غير الجنائية لازمة للفصل في الدعوى الجزائية، فإذا كانت الواقعة المدنية يمكن أن تستدل المحكمة منها كقرينة على وقوع الجريمة، فلا يمنع القاضي من اتباع كافة وسائل الإثبات، كواقعة إتلاف السند وتزويره يمكن إثباتها بكافة طرق الإثبات فيها، أيا كانت قيمة السند، إذ ينصب الإثبات في هاتين الحالتين على واقعتين هما الإتلاف والتزوير، وبخصوص ذلك يمكن للقاضي اللجوء إلى اتباع أساليب الإثبات المقررة في المواد غير الجنائية.

ان المثال الواضح لذلك هو إثبات جريمة خيانة الأمانة، فهذه الجريمة تفترض وجود عقد أمانة بين الجاني والمجني عليه سواء كان عقد وكالة أو الإجارة، وهذا العقد مسألة مدنية وسابق عن وجود فعل الاختلاس أو التبديد الذي تقوم عليه الجريمة، وبالتالي فلتوقيع العقوبة على جريمة خيانة الأمانة يجب إثبات وجود أحد هذه العقود الخاصة التي تقوم عليها هذه الجنحة، فالقاضي الجزائي يلجأ بالضرورة إلى بحث مسبق حول قيام هذا العقد وعليه إثبات ذلك لما تمليه قواعد الإثبات في القانون المدني السالف الذكر، وعلى ذلك إذا زادت قيمة التصرف القانوني نصابا محددا، مثلا 100.000 دينار جزائري حسب المادة 333 من القانون رقم 05–10 المعدل والمتمم للقانون المدني[1] أو كان هذا التصرف غير محدد القيمة يلزم إثباته بالكتابة.

ثانيا: جواز القاضي الجزائي إثبات المسائل غير الجنائية بالدليل الإلكتروني

لربط المثال السابق بموضوع الدراسة يمكن تمثيل هذه الصورة في حالة ما إذا قام طرفا العقد إبرام هذا العقد عن طريق الأنترنت، بالتالي يتجسد العقد في شكل سند أو محرر إلكتروني.

[1]– قانون رقم 05–10 يعدل ويتمم الأمر رقم 75–58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني الجزائري، الجريدة الرسمية للجمهورية الجزائرية عدد 44 بتاريخ في 20 يونيو 2005.

التساؤل الذي يجب طرحه في هذا المقام، هل يجوز للقاضي الجنائي أن يلجأ للدليل الإلكتروني لإثبات هذا العقد الخاص بالأمانة أي لإثبات المسائل الأولية بوجه عام؟

إن الإجابة على هذا الإشكال تكون بالإيجاب وذلك أن المشرع نظم في مختلف الدول المقارنة المعاملات الإلكترونية وسبل إثباتها وأعطى للمحررات الإلكترونية حجية تامة شأنها في ذلك شأن المحررات الورقية بشرط اشتمالها الشروط الفنية والتقنية.

أصبح للدليل الإلكتروني دورا هاما خاصة في المعاملات المدنية والتجارية، وذلك نتيجة دخول العالم مجال تكنولوجيا المعلومات الذي يعتمد أسلوب غير ورقي، مرئي ومنقول عبر الشاشة الإلكترونية.

تم استبدال الملفات الورقية والمخططات بالأسطوانات الممغنطة والسندات الإلكترونية المحفوظة على أسطوانات ضوئية رقمية أو على أقراص ممغنطة، وهي تنقل من مكان إلى آخر بسهولة وسرعة خارقة من دون أي حاجة للورق. نتيجة لذلك، وحتى تواكب مختلف الدول هذه التطورات في مجال تكنولوجيا الاتصالات عن بعد وبالتالي تنمية وتشجيع التجارة الإلكترونية قامت بتوسيع تعريف الكتابة لتشمل في طياتها المحررات الإلكترونية، وذلك كالتشريع الفرنسي والجزائري، كما تم الاعتراف بالمحرر الإلكتروني كدليل لإثبات المعاملات الإلكترونية.

عرفت المادة 1365 من القانون المدني الفرنسي[1] الدليل الكتابي على أنه « ينتج من تتابع حروف أو خصائص مطبوعة أو أرقام أو كل إشارة أو رموز لها معنى مفهوم أيا كانت الدعامة المدونة عليها ووسيلة نقله »، وهو التعريف نفسه الذي أخذه المشرع الجزائري بموجب المادة 323 مكرر 1 قانون رقم 05-10[2] المؤرخ في 20 يونيو 2005 المعدل للقانون المدني الجزائري.

أقر المشرع الفرنسي التماثل بين الكتابة على الورق والكتابة الإلكترونية من حيث الحجية في الإثبات، فتنص المادة 1366-1 من القانون المدني الفرنسي على أية " تقبل الكتابة في شكل إلكتروني كدليل في الإثبات مثلها في ذلك مثل الكتابة على دعامة ورقية. ما دام الشخص

[1]-**code civil Français**, in ; https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070721.

[2]-قانون رقم 05-10، سالف الذكر.

المنسوب إليه هذه الكتابة قد تم تحديده علة وجه صحيح وقد تم إثبات هذه الكتابة والاحتفاظ بها في ظروف من شانها أن تضمن سلامتها.

أخذ المشرع الجزائري حرفيا بالنص السالف ذكره، 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.

ان المحرر الإلكتروني يتكون من عنصرين الكتابة والتوقيع، فمن غير المتصور أن يبقى شكل التوقيع على المحرر الإلكتروني تقليديا بخط اليد بل يجب أن يكون من نفس تقنية المحرر الإلكتروني بمعنى أن يكون توقيعا إلكترونيا، ونتيجة لذلك تبنى المشرع الفرنسي فكرة التوقيع الإلكتروني.

يستخدم التوقيع الإلكتروني في تأمين المعلومات من خلال إدخال أختام توقيت الإرسال في الرسائل المشفرة، فإذا ما حاول شخص ما، أن يزور المفترض كتابة أو إرسال الوثيقة فيه، سيكون هذا التزوير قابلا للكشف، وسوف يرد ذلك الاعتبار للقيمة الإثباتية للصور الفوتوغرافية والفيديوهية، ولقد أضاف علم التصوير للإثبات الجنائي قيمة علمية بما له من أثر في نقل صور صادقة للأماكن والأدلة إلى كل من يعنيه الأمر، اعتمادا على آلة التصوير التي لا تعرف الكذب. بيد أنه لا يمكن إنكار الآثار السلبية والخطيرة التي تنشأ عن استخدام هذه الوسائل، لما قد يحدثه في الحياة الخاصة إذا لم توضع له الضوابط الكافية[1] وتختلف حجية التوقيع الإلكتروني في الإثبات المدني عنه في الإثبات الجنائي، حيث يخضع في الإثبات المدني لقواعد شكلية، أما في الإثبات الجنائي فيخضع تقديره لمطلق سلطة القاضي الجزائي، كما أن وجود نظام تسجيل الدخول في شبكة الأنترنت يسمح بتحديد الأشخاص الذي دخلوا أو حاولوا الدخول بعد ارتكاب الفعل الجرمي.[2]

[1] – **عبد الحافظ عبد الهادي عابد**، الإثبات الجنائي بالقرائن – دراسة مقارنة، دار النهضة العربية، القاهرة، 1998، ص 463.

[2] – **على حسن طوالبه**، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، مرجع سابق، ص 15.

الفصل الثاني

يقينية الدليل الإلكتروني

إنّ أهم النتائج التي تترتب عن مبدأ حرية القاضي في تكوين اقتناعه، حرية القاضي في تقدير الأدلة بما في ذلك الدليل الإلكتروني وموازنتها وفقا لما يمليه عليه وجدانه، ومن دون أن يخضع في ذلك لرقابة المحكمة العليا، إلا أنه مع ذلك مقيد بضرورة تأسيس اقتناعه على الجزم واليقين، دون الظن والاحتمال، وأن يكون متوائما مع مقتضيات العقل والمنطق.

إن سلطة القاضي الجزائي في تقدير الدليل الإلكتروني يحكمه مبدأ الاقتناع القضائي الذي يؤدي إلي نتيجتين هما، حرية القاضي في قبول الأدلة وحرية القاضي في تقدير الأدلة.

يجوز للقاضي الجزائي الاستناد إلى الدليل الإلكتروني لإثبات الجرائم خاصة الجرائم المعلوماتية، حيث أن المشرع حسم هذه المسالة بتحديد النموذج القانوني للدليل الخاضع لتقدير القاضي، فمتى ما توافرت شروط هذا النموذج طبقا لمبدأ الشرعية الإجرائية، وجب على القاضي إخضاعه لعملية تقديره وهي مسألة موضعية محضة، للقاضي أن يمارس سلطته التقديرية فيها، بل هي المجال الطبيعي لهذه السلطة حيث أنها تتعلق بقيمة الدليل في الإثبات وصولا للحقيقة.

رغم منح القانون للقاضي الجزائي حرية واسعة في مجال تقدير الأدلة وفقا لاقتناعه الشخصي إلا انه أحاطه بسياج من القيود والضوابط التي تشكل في مجموعها شروطا لإعمال المبدأ بل وتطبيقه التطبيق الأمثل بما يضمن الوصول إلى الحقيقة الفعلية في الدعوى دون التعدي على الحقوق والحريات الشخصية.

تقتضي دراسة سلطة القاضي الجزائي في التقدير والتيقن من الدليل الإلكتروني أن تحدد حرية القاضي الجزائي في الاقتناع بالدليل الإلكتروني (المبحث الأول)، وتقييم الدليل الإلكتروني (المبحث الثاني).

المبحث الأول

حرية القاضي الجزائي في الاقتناع بالدليل الإلكتروني

أصبح الدليل الإلكتروني شأنه شأن الدليل بشكل عام يخضع للمبدأ العام في الإثبات الجزائي وهو حرية القاضي الجزائي في الاقتناع ما لم يتضمن المشرع الجزائري في هذا الصدد أية أوضاع خاصة في القانون رقم 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والقاضي في ظل هذا المبدأ حرية واسعة في تقييم عناصر الإثبات، ووزن الأدلة وتقديرها بالكيفية التي تمكنه من تكوين عقيدته في الدعوى المطروحة عليه ولا يخضع في ذلك إلا لصوت ضميره وما يقتنع به شخصيا، ولا يستشير في ذلك سوى وجدانه، فهو وحده الذي يملي عليه الحكم الذي يصدره والرأي الذي يتوصل إليه.

رغم ذلك إن المشكلات التي يثيرها هذا الدليل في مقابل نقص الثقافة المعلوماتية، تؤدي إلى إنقاص قيمته ونسبه الاستناد عليه في إثبات الجرائم المعلوماتية.

سيحاول دراسة أثر الطبيعة العلمية للدليل الإلكتروني على اقتناع القاضي الجزائي(المطلب الأول)، ثم التطرق إلى الضوابط التي تحكم الإقتناع القضائي بالدليل الإلكتروني(المطلب الثاني)

المطلب الأول

أثر الطبيعة العلمية للدليل الإلكتروني على اقتناع القضائي

يعد الدليل الإلكتروني تطبيقا من تطبيقات الدليل العلمي، فهل القاضي الجزائي يسلم به ويبني اقتناعه على أساس أن أمره محسوم علميا؟

لذلك كان وجوبا قبل الإجابة عن هذا التساؤل بيان مضمون مبدأ اقتناع القاضي في مجال الإثبات الجزائي(الفرع الأول)، ثم بيان تطبيق ذلك على الطبيعة العلمية للدليل الإلكتروني(الفرع الثاني).

الفرع الأول

مضمون مبدأ حرية الاقتناع القضائي

يعد مبدأ الاقتناع القضائي أحد أهم المبادئ التي تقوم عليها نظرية الإثبات في المواد الجزائية، وعنه تتفرع معظم القواعد التي تحكم هذا الإثبات.

يعد الاقتناع الشخصي للقاضي الجزائي من أهم النتائج المترتبة على القاعدة العامة للإثبات في القانون الجزائي، ومؤداه أن القاضي في المواد الجزائية يبني حكمه على اقتناعه الشخصي القائم على الترجيح بين الأدلة المقامة أمامه بما يستقر في ضميره من خلال حريته في موازنة الأدلة المعروضة عليه في الدعوى دون أن يخضع في ذلك لرقابة المحكمة العليا مادام أن الدليل الذي استند إليه متفقا مع الأدلة المقدمة في الدعوى ولا يتضمن إنشاء واقعة جديدة.

يتميز الاقتناع الشخصي للقاضي الجزائي بالذاتية لأنه إنتاج ضمير يتأثر بمدى قابلية الشخص واستجابته للدوافع والبواعث المختلفة، فهو عبارة عن نشاط عقلي لا يتدخل المشرع ليبين للقاضي كيفية ممارسته وترجمته إلى واقع منتج، ولا يرسم له كيف يشكل معادلاته الذهنية في مجال تقدير الأدلة ليصل من خلالها إلى الحقيقة[1].

هدف كل بحث هو اكتساب المعرفة الصحيحة الحقيقية للواقع، وأول عناصر البحث العلمي عن الحقيقة هو جمع المعلومات وتحليلها منهجيا من أجل وضع القرارات، والعنصر الثاني هو إعادة بناء كل شيء بالضبط بقدر الإمكان بالنسبة للحدث الذي يصفه تقريبا.

تهدف الخصومة الجزائية إلى معرفة الحقيقة المطلقة، ويقتضي ذلك أن يصدر حكم قضائي بالإدانة عن اقتناع يقيني بصحة ما ينتهي إليه من نتائج مستنبطة من الواقع والقانون.

ان الحقيقة التي يرغب القاضي في الحكم على أساسها بشكل عام، والحكم في الإدانة بشكل خاص، لا يمكن أن تقوم إلا على اليقين حقا، بعيدا عن الشك تماما ولا يكفي وجود مجرد الاحتمال والظن، فاستظهار الحقيقة الواقعية وإصدار الحكم بالإدانة وتوقيع الجزاء على الجاني لابدّ أن يبنى على اليقين، لأن الجزاء يتضمن خطورة خاصة تجعله أشد جسامة من الأحكام القانونية الأخرى، فمن الظلم جدا أن يصاب بريء.

[1] – **محمود نجيب حسني**، شرح قانون الإجراءات الجزائية، مرجع سابق، ص 774.

ان اليقين هو أساس الحقيقة القضائية، يولد الصدق للحكم والثقة في عدالة القاضي الذي يؤدي إلى تدعيم الثقة في عدالة القضاء ويعزز الثقة بأحكامه، والحقيقة القضائية التي يعلنها الحكم الجزائي يكون لها دورا أساسيا ثابتا في المجتمع والقانون، بحيث تكون قرينة البراءة هي المحور الذي ترتكز عليه وتنطلق منه سائر قواعد الإجراءات الجزائية.

يقصد بالموقف اليقيني تلك الحالة الذهنية أو العقلانية التي تؤكد وجود الحقيقة ولا يتوصل إلى هذه الصورة إلا بواسطة الاستنتاج، حتى يصل لإدراك القاضي من خلال مختلف الوقائع المطروحة أمامه، بحيث ينطبع في ذهنه تصورات واحتمالات مؤكدة لا تقبل الشك أو أي ريب لما تحويه من ثقة عالية نحو ما استدركه القاضي من الحقائق والمعلومات التي توصل إليها في حكمه، فإذا وصل القاضي لهذه المرحلة من مراحل اليقين، فإنّه يكون قد وصل إلى الحقيقة الواقعية وينطبق اليقين على الواقعة الإجرامية في ذهن القاضي، مما يولد حالة ذهنية أو عقلانية لديه محدثة انطباعا عن كيفية حدوث تلك الواقعة. يتوقف تكامل هذا اليقين في ضمير القاضي على قدرة الأدلة المطروحة على توصيل القاضي إلى هذه الدرجة ذهنيا، فإذا حدث ذلك يكون هناك تطابق لديه بين حالة الذهن والعقل مع حالة الواقع والحقيقة، ويكون تطبيق القانون عادلا، إذا بيّن القاضي الواقعة بيانا صحيحا وكافيا يؤدي هذا البيان في نهاية الأمر إلى استخلاص اليقين للواقعة.

هدف الإثبات هو البحث عن الحقيقة لتحقيق العدالة، وبدون ذلك لا تثبت الجريمة ولا تستطيع الدولة تطبيق حقها في العقاب، وهنا يأتي دور القاضي في معرفة الأسلوب الذي يعتمد عليه البحث وإظهار الحقيقة، ونسبتها إلى المتهم لينال عقابه. وتتكون الحقيقة الواقعية في الحكم الصادر بالإدانة من المعرفة القانونية والمعرفة العلمية والمنطقية[1].

أن للقاضي أن يستمد اعتقاده من أي دليل يطمئن إليه نفسه، دون أي قيد يقيده في ذلك، سواء في تلك الأدلة التي طرحت عليه من قبل النيابة العامة أو الخصوم أو التي يرى بنفسه تقديمها وهذه الحرية التي يتمتع بها القاضي الجزائي في هذا المجال ليست مقررة بهدف توسيع الإدانة أو البراءة وإنما هي مقررة له بالنظر إلى صعوبة الحصول على دليل في المواد الجزائية[2].

[1] – **كامل مصطفى**، مسائل عملية أمام المحاكم الجنائية، منشأة المعارف، الإسكندرية، ص 199.

[2] – **علي محمود علي حمودة**، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مرجع سابق، ص 44.

يستنتج أن اليقين والاقتناع والحقيقة عبارة عن سلسلة واحدة تدور في نسق واحد ذات علاقة تكامل، فكل نوع يحتفظ بخاصيته واستقلاله في مواجهة الآخرين، فوصول القاضي إلى درجة اليقين يتولد عنه قناعته الشخصية بالحقيقة، فاليقين يعتبر اللبنة الأولى التي تتولد وينبثق عنها اليقين الذي يتدرج من الضعف إلى القوة مع تقدّم إجراءات الدعوى الجزائية، مع العلم أن هذا التدرج من أجل الوصول إلى الحقيقة القضائية الذي يصاحب الاقتناع ينشأ عنه ما يسمى بالاقتناع اليقيني، وعليه أن هذه العناصر مترابطة فيما بينها ولا يمكن التخلي عن واحدة منها، بالتالي يمكن القول أن القاضي إذا استطاع الوصول إلى اليقين، بحيث إدراك الأدلة الإلكترونية، فإنّ حالة الذهن تتطابق مع العقل، وحالة الواقع والوصول إلى الحقيقة، أمّا إذا شك القاضي في قدرة الأدلة الإلكترونية، فإنّه يمكن القول بعدم قيام عنصر اليقين، وبالتالي تكون قناعة القاضي بعيدة عن الحقيقة، لكن هذا لا يعني التحكيم القضائي، فلا يجوز للقاضي أن يقضي وفقا لشعوره وتحليله، وإنما هو ملزم بتحدي المنطق الدقيق في تفكيره الذي قاده إلى اقتناعه وتقييد، بالأدلة اليقينية، فالأدلة يجب أن تقرب القاضي نحو الحقيقة الواقعية، فلا يقبل الشك.

لم يقتصر تطبيق هذا المبدأ على التشريعات اللاتينية فحسب، بل يمتد إلى التشريعات الأنجلوسكسوني مع اختلاف طفيف في الصياغة، فهي لا تعرف تعبير الاقتناع القضائي، وإنما تستخدم بدلا منه تعبير ثبوت الإدانة بعيدا عن أي شك معقول Proof beyond a reasonable doubt[1].

نص المشرع الفرنسي على هذا المبدأ في المادة 353 [2] قانون إجراءات جزائية فرنسي الحالي والتي تنص على ما يلي: « لا يطلب القانون من القضاة حسابا بالأدلة التي اقتنعوا بها، ولا يفرض قاعدة خاصة تتعلق بتمام وكفاية دليل ما، وإنما يفرض عليهم أن يتساءلوا في صمت

---

1 − **John SPENCER**, « La preuve en procédure pénale, droit anglais », RIDP, v 63, 1er et 2eme trim, 1992, p 101.

2 -art 353 du Code de procédure pénale Français , cité précédemment , dispose : « avant que la cour d'assises se retire, le président donne lecture de l'instruction suivante, qui est, en outre, affichée en gros caractères, dans le lieu le plus apparent de la chambre des délibérations : " sous réserve de l'exigence de motivation de la décision, la loi ne demande pas compte à chacun des juges et jurés composant la cour d'assises des moyens par lesquels ils se sont convaincus, elle ne leur prescrit pas de règles desquelles ils doivent faire particulièrement dépendre la plénitude et la suffisance d'une preuve ; elle leur prescrit de s'interroger eux-mêmes dans le silence et le recueillement et de chercher, dans la sincérité de leur conscience, quelle impression ont faite, sur leur raison, les preuves rapportées contre l'accusé, et les moyens de sa défense. La loi ne leur fait que cette seule question, qui renferme toute la mesure de leurs devoirs : " Avez-vous une intime conviction ? ".

وتدبر، وأن يبعثوا في صدق ضمائرهم أي تأثير قد أحدثته الأدلة الراجحة ضد المتهم ووسائل دفاعه... ».

أما المشرع الجزائري فإنه كرس مبدأ الاقتناع القضائي بموجب المادتين 307[1] قانون إجراءات جزائية والتي هي مستوحاة من نص المادة 353 القانون الإجراءات الفرنسي.

يجدر الإشارة في هذا المقام أن مبدأ الاقتناع القضائي العام يسري لدى أنواع المحاكم الجزائية كافة، سواء كانت محاكم الجنايات، الجنح أم المخالفات[2]، وإذ كان قد شرع أصلا لكي يطبق أمام قضاء الحكم، إلا أن ذلك لا يعني أبدا أن نطاق تطبيقه مصور على هذه المرحلة، بل هو يمتد كذلك ليشمل مرحلة التحقيق الابتدائي إذ أن هذا المبدأ ينطبق على قضاة التحقيق، ومع هذا ينبغي أن لا يغيب عن البال أن مرحلة الحكم تعد هي الميدان الأرحب والأوسع لتطبيقه.

الفرع الثاني

التطبيق على الطبيعة العلمية للدليل الإلكتروني

إنّ أهم السمات التي يتميز بها الدليل الإلكتروني كتطبيق من تطبيقات الدليل العلمي الموضوعية والحياد والكفاءة، إن مقدار اتساع مساحة الأدلة العلمية ومن بينها الدليل الإلكتروني ما يكون انكماش وتضاؤل دور القاضي الجزائي في التقدير، خاصة أمام نقص الثقافة الفنية للقاضي، وبالتالي فإن مهمته تصبح شبه آلية، إلا أن الحقيقة غير ذلك، فالدليل الإلكتروني كدليل علمي يخضع إلى تقدير القاضي الجزائي، وبالتالي إلى اقتناعه وفي هذا الخصوص ينبغي أن التمييز بين أمرين:

---

[1]– المادة 307 من قانون الإجراءات الجزائية الجزائري تنص: " يتلو الرئيس قبل مغادرة المحكمة قاعة الجلسة التعليمات التالية التي تعلق فضلا عن ذلك بحروف كبيرة في أظهر مكان في غرفة المداولة: ان القانون لا يطلب من القضاة حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم بها قواعد يتعين عليهم ان يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا انفسهم في صمت وتدبر، وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها، ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم. هل لديهم اقتناع شخصي؟".

[2] – ان المشرع الجزائري لم يحدد صراحة في المواد المقررة لهذا المبدأ، المواد 307، 212 من قانون الإجراءات الجزائية سالف الذكر، بخلاف المشرع الفرنسي حيث خصص المادة 353–1 من قانون الإجراءات، لتطبيق المبدأ أمام الجنايات، كما نصت المادة 427 من القانون نفسه على تطبيق هذا المبدأ في محاكم الجنح.

– **القيمة العلمية القاطعة للدليل،** تقدير القاضي لا يتناول هذا الأمر، لأن قيمة الدليل تقوم على أسس علمية دقيقة، فلا حرية له في مناقشة الحقائق العلمية الثابتة[1].

– **الظروف والملابسات التي وجد فيها الدليل،** والتي تدخل في نطاق التقدير الذاتي للقاضي، فهي من صميم وظيفته القضائية، بحيث يمكنه أن يطرح هذا الدليل رغم قطعيته إذا تبين أنه لا يتفق مع ظروف الواقعة وملابساتها، حيث تولد شبهة لدى القاضي، ومن ثم قد يقضي في إطار تسيير الشك لصالح المتهم، ذلك أن مجرد توافر الدليل العلمي لا يعني أن القاضي ملزم بالحكم بموجبه مباشرة سواء بالإدانة أم بالبراءة، دون بحث الظروف والملابسات فالدليل العلمي ليس آلية معدة ت لتقرير اقتناع القاضي بخصوص مسألة غير مؤكدة، بل هو دليل إثبات قائم على أساس من العلم والمعرفة، وللقاضي النظر إليه على ضوء الظروف والملابسات المحيطة[2].

يستنتج مما سبق أن مبدأ الاقتناع الذاتي للقاضي الجزائي هو حجر الزاوية في الأحكام الجزائية، وعلى هذا الأساس فإن ظهور الدليل الإلكتروني بكل خصائصه يجب أن لا يغير شيئا من هذا المبدأ .

إن الدليل الإلكتروني شأنه شأن الأدلة الجزائية بشكل عام لا يحظى أمام القاضي الجزائي بقوة حاسمة في الإثبات وإنما هو مجرد دليل لا تختلف قيمته ولا تزيد حجته عن سواه، وهذا أثر من آثار حرية القاضي الجزائي في الاقتناع، وعلى هذا الأساس يصح للقاضي أن يؤسس اقتناعه على الدليل الإلكتروني كما يصح أن يطرحه رغم قطيعته من الناحية العلمية وذلك عندما يجده لا يتسق منطقيا مع ظروف الواقعة وملابساتها ولو لم تكن في الدعوى أدلة سواه.

---

[1] – Marylou GARCIAS et Max CHOUZIER, "La preuve informatiques : Quelles nouveautés techniques pour quelles évolutions juridiques", Revue Lexbase, édition affaires n° 280 du 18 Janvier 2012 , p 3,in ; http://www.adij.fr/wp-content/uploads/2012/01/CompteRendu_PreuveInformatique.pdf. consulté le:22/12/2015.

[2] – راجع كل عن: جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص 23، عائشة بن قارة، مرجع سابق، ص 161.

المطلب الثاني

الضوابط التي تحكم اقتناع القضائي الجزائي بالدليل الإلكتروني

إنّ أهم النتائج التي تترتب عن مبدأ الاقتناع القضائي أي مبدأ حرية القاضي الجزائي في تكوين اقتناعه هو حرية القاضي في تقدير الأدلة بما في ذلك الدليل الإلكتروني وموازنتها وفقا لما يمليه عليه وجدانه، لذلك فإن تقدير كفاية أو عدم كفاية الدليل الإلكتروني في إثبات جريمة معلوماتية ونسبتها إلى فاعلها، أمر تستقل به محكمة الموضوع المعروض عليها هذا الدليل، ولا تخضع في ذلك لأية رقابة، إلا أنه ومع ذلك مقيد بضرورة تأسيس اقتناعه على الجزم واليقين دون الظن أو الترجيح والاحتمال، وأن يكون الاقتناع القضائي ملائما مع مقتضيات العقل والمنطق.

وبناء على ذلك يقسم المطلب إلى فرعين، اليقين القضائي واستثنائه من حالة البراءة (الفرع الأول) وبلوغ الاقتناع القضائي حد الجزم واليقين بما يتلاءم مع مقتضيات العقل والمنطق (الفرع الثاني).

الفرع الأول

اليقين القضائي واستثنائه في حالة البراءة

يفترض في كل إنسان أن يكون بريئا، بالرغم من قوة الشكوك التي تحوم حوله، طالما أن مسؤوليته الجزائية لم تثبت بعد، ولهذا السبب يجب أن يعامل المتهم بأنه بريء، حتى يصدر ضده حكم جنائي صحيح من القضاء المختص. وتعد قرينة البراءة ضمانة هامة للحرية الشخصية لكل إنسان، ضد تعسف السلطة أو انتقام المجني عليه من المتهم[1].

أولا: قرينة البراءة

يتطلب افتراض البراءة في المتهم عدم مطالبته بتقديم أي دليل على براءته، فله أن يتخذ موقفا سلبيا تجاه الدعوى القائمة ضده، وعلى النيابة العامة تقديم الدليل على ثبوت التهمة المنسوبة عليه، بل عليها أن تقدم للمحكمة الأدلة الصادقة التي تفيد في كشف الحقيقة سواء كانت في صالح المتهم أو ضده فوظيفة النيابة هي إثبات الحقيقة، وليس الاقتصار على جمع الأدلة قبل

[1] – **إيمان محمد على الجابري**، مرجع سابق، ص 190.

التهم[1]، فإذا توافرت أدلة تفيد صحة الاتهام كان من حق المتهم تقديم ما لديه من الأدلة لدحض ما توافر ضده، وإذا عجزت النيابة عن جمع أدلة أخرى ضد المتهم فإن هذا الأخير لا يلتزم بتقديم أي دليل على براءته، لأن الأصل فيه هي البراءة.

تتضمن قرينة البراءة افتراضا، وهو أن المتهم بريء حتى تثبت إدانته بحكم قضائي بات وهذا الحكم البات يفترض أنه قد استبعد كل فرض للشك في ثبوت الجريمة ونسبتها إلى الجاني دون تسرع أو خلط بين السببية والوقت الزمني، وهنا يتوصل القاضي إلى اليقين القضائي التام، ومما لاشك فيه أن التوصل لهذه النتيجة يتطلب من القاضي جهدا كبيرا، وهو يعد في غاية الصعوبة، ذلك لأن الوقائع كلما تنتسب للماضي يصعب إثباتها بأدلة حقيقية[2].

يلتزم القاضي الجزائي بتطبيق هذه القاعدة، لأن المتهم بريء حتى تثبت إدانته وفق إجراءات وحكم مبنٍ على اليقين الذي ينفي أصل القاعدة وهو البراءة، وكلما ثار الشك لدى القاعدة توجب عليه قاعدة تفسير الشك لصالح المتهم، فإذا ما خالف ذلك وقضى بالإدانة كان حكمه باطلا[3].

الدليل القانوني لقرينة البراءة هو أن الاتهام يدعي خلاف الأصل وهو البراءة، فإذا لم ينجح في إثبات ادعائه إثباتا قاطعا تعين الإبقاء على الأصل.

تعد قرينة البراءة ركيزة أساسية للشرعية الدستورية[4] في قانون العقوبات، وهي شرعية الجرائم والعقوبات، يتمثل في ضمان أصل البراءة لكل متهم[5]، كل شك في إثبات الجريمة يجب أن يفسر لمصلحة المتهم سواء أكان هذا الشك من أركان الجريمة أم من دليل إثباتها، وبهذا الشك يجب أن تطرح أدلة الإدانة وتتأكد براءة المتهم[6]. لهذا فإن الأحكام الصادرة بالإدانة، يجب أن تبنى على

---

[1] – **أحمد فتحي سرور**، الوسيط في قانون الإجراءات الجزائية، مرجع سابق، ص 767.

[2] – **سعيد عبد اللطيف حسن**، الحكم الجنائي الصادر بالإدانة، دار الفكر العربي، القاهرة، 1989، ص 579.

[3] – **محمد عيد الغريب**، حرية القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام، دار النهضة العربية، القاهرة، 2008، ص 19.

[4]– المادة 56 من الدستور الجزائري 2016، سالف الذكر.

[5] – **أحمد فتحي سرور**، القانون الجنائي الدستوري، دار أشرف، القاهرة، 2001، ص 251.

[6]– وهذا ما نصت عليه المادة 2 من قانون رقم 17–07 مؤرخ في 28 جمادى الثاني لعام 1438 الموافق 27 مارس سنة 2017 يعدل ويتمم الأمر رقم 66–155 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966 والمتضمن قانون لإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية عدد 20 بتاريخ 29 مارس 2017، "...ان كل شخص يعتبر بريء ما لم تثبت إدانته...أن يفسر الشك في كل الأحوال لمصلحة المتهم..."

حجج قطعية الثبوت تفيد الجزم واليقين، لا مجرد الظن والاحتمال، وكل شك في أدلة الإدانة يجعل الحكم بالعقوبة على خير أساس، متى كان الدليل الذي ساقه الحكم قد عول عليه في إدانة المتهم دليلا ضنيا مبنيا على مجرد الاحتمال، غير أن الأحكام الجزائية الصادرة بالإدانة لا تبنى إلا على حجج الثبوت، تفيد الجزم واليقين، فإن الحكم يكون معيبا مستوجبا للاستئناف. وتم بموجب المادة 6 من قانون رقم 17-07 المعدل والمتمم ويتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، التي عدلت المادة 248 استحداث محكمة جنايات ابتدائية ومحكمة جنايات استئنافية، مقرهما على مستوى المجلس القضائي، تختصان بالفصل في الأفعال الموصوفة بالجنايات وكذلك الجنح والمخالفات المرتبطة بها.

بناء على هذه النتيجة يكفي في المحاكمة الجزائية أن يتشكك القاضي في صحة إسناد التهمة إلى المتهم لكي يقضي بالبراءة، إذ مرجع الأمر في ذلك إلى ما يطمئن إليه في تقدير الدليل ما دام الظاهر من الحكم أنه إحاطة بالدعوى عن بصر وبصيرة، كما أن الخطأ القانوني في الحكم القاضي بالبراءة لا يعيبه.

ان الشك المؤدي إلى تبرئة المتهم له ضوابط ومعايير، وإلا كثيرا من المجرمين يفلت من العقاب بمجرد كلمة الشك، ولتفادي ذلك كان لمحكمة الموضوع أن تقضي بالبراءة متى تشككت في صحة إسناد التهمة إلى المتهم أو لعدم كفاية أدلة الثبوت عليه، إلا أن ذلك مشروط بأن تلتزم بالحقائق الثابتة بالأوراق وأن يشتمل حكمها على ما يفيد أنها محصت الدعوى وأحاطت بظروفها وبأدلة الثبوت التي قام الاتهام عليها عن بصر وبصيرة ووازنت بينها وبين أدلة النفي فرجحت دفاع المتهم أو داخلتها الريبة في صحة عناصر الإثبات، أما إذا كان الدليل الذي ساقه الحكم وعول عليه في إدانة المتهم هو دليل ظني مبني على مجرد الاحتمال والأحكام الصادرة بالإدانة يجب ألا يبنى على حجج قطعية الثبوت تفيد الجزم واليقين.

يترتب على افتراض البراءة في المتهم وجوب معاملة المتهم على أساس أنه برئ في جميع المراحل التي تمر بها الدعوى الجزائية سواء في مرحلة جمع الاستدلالات أو التحقيق أو مرحلة المحاكمة.

نظرا لأن الأصل في المتهم البراءة، فإن المتهم بريء حتى تثبت إدانته[1]، ومن ثم فإن من حقه إذا نسب إليه ارتكاب فعل يؤثمه القانون أن يدفع هذا الاتهام عن نفسه، كما أن له مطلق الحرية في اختيار وسائل دفاعه، وهذا ما عرف بحق المتهم في الدفاع عن نفسه.

تأكيدا لضمان حق المتهم، أحاط الاستجواب بضمانات تكفل للمتهم حقوقه كاملة، وتجعله بمنأى عن التعسف، وللمتهم أن يمتنع عن الإجابة أو الاستمرار لأسئلة المحقق. ولا يجوز تحليف المتهم اليمين حين استجوابه وإلا توجب بطلانه، ولا يجوز أن يعد السكوت دلالة على إدانة المتهم، بحيث يتم تعذيبه جسديا أو معنويا لحمله على الكلام. وهذا ما تقرر في قانون الإجراءات الجزائية[2]، كذلك أوصت به المؤتمرات الدولية ومنها المؤتمر الدولي السادس لقانون العقوبات المنعقد في روما سنة 1953 الذي أوصى بأنه لا يجبر المتهم على الإجابة[3].

ثانيا: اليقين القانوني

اليقين هو كل معرفة لا تقبل الشك ومنه حدسي كاليقين ببعض الأوليات، أو استدلالي غير مباشر يتنبأ إليه المرء بعد البرهة، ومنه ذاتي يسلم به المرء ولا يمكنه نقله إلى غيره، أو موضوعي يفرض نفسه على العقول كاليقين العلمي والعلم اليقيني هو الذي ينكشف فيه العلوم انكشافا لا يبقى معه ريب ولا غلط أو وهم.

أما اليقين القانوني فهو عبارة عن اقتناع مستند إلى حجج ثابتة وقطعية، عبارة عن حالة ذهنية أو عقلانية تؤكد وجود الحقيقة[4]، ويتم الوصول إليه عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى وما ينطبق في ذهنه من تصورات ذات درجة عالية من التوكيد.

---

[1]– المادة 2 من قانون رقم 17–07، سالف الذكر.

[2] – فتوح عبد الله الشاذلي، قواعد الأمم المتحدة لتنظيم قضاء الأحداث، دار المطبوعات الجامعية، الإسكندرية، 2014، ص 77.

[3]– Congrès international de droit pénal, 6ème , Rome, 27 septembre– 3 octobre 1953, paragraphe 105. P 21.

[4]– **رشيدة بوكر**، مرجع سابق، ص324.

عندما يصل القاضي لهذه المرحلة من اليقين، فإنه يصبح مقتنعا بالحقيقة، فاليقين هو وسيلة الاقتناع أو بعبارة أخرى فإن الاقتناع ثمرة اليقين، وليس اليقين ذاته.

متى تكامل اليقين بأن وصل القاضي إلى درجة القطع ينشأ ما يسمى بالاقتناع اليقيني، وهو أساس الحقيقة القضائية التي ينشدها القاضي في حكمه.

يترتب على لزوم بلوغ الاقتناع بالإدانة درجة اليقين أنه إذا لم يدرك القاضي هذه الدرجة من الاقتناع كان مع ذلك أن اقتناعه يتأرجح بين ثبوت التهمة ومسؤولية المتهم عنها وبين عدم ثبوتها وعدم مسؤولية المتهم عنها، وهذا الاقتناع المتأرجح يعني الشك في ثبوت التهمة، مما يستوجب على القاضي أن يحكم بالبراءة أخذا بقاعدة أساسية أن الأصل في الإنسان البراءة حتى تثبت إدانته، وما دام هذا الأخير شرط حين الحكم بالإدانة، فبمفهوم المخالفة تستثنى حالة البراءة من هذا الشرط.

إنّ شرط اليقين في أحكام الإدانة شرط عام سواء كانت الأدلة تقليدية أو مستحدثة كالدليل الإلكتروني، وتكمن العلة من وراء هذا القيد في أن الحكم بإدانة شخص أمر جد خطير، يترتب عليه آثار جسيمة، ويمكن أن ينال من حريته أو شرفه أو ماله، بل قد يكون حقه في الحياة[1].

إذا كان الأصل في الإنسان البراءة، فإنه يجب لإدانته أن يقوم الدليل القاطع على ارتكابه الجريمة سواء كانت تقليدية أو مستحدثة ونسبتها للمتهم، أما فيما يتعلق الحكم بالبراءة يكفي أن يشكك القاضي في صحة إسناد التهمة إلى المتهم حتى يقضي بالبراءة، وذلك إعمالا بمبدأ تفسير الشك لمصلحة المتهم.

الفرع الثاني

بلوغ الاقتناع القضائي حد الجزم والاقتناع بما يتواءم مع مقتضيات العقل والمنطق

ان الوقت الذي يعود فيه لقاضي الموضوع تقدير الأدلة وموازنتها وفقا لما يمليه عليه وجدانه ومن دون أن يخضع في ذلك للرقابة، إلا أنه مقيد بضرورة تأسيس قناعته على الجزم والاقتناع الكامل لا على الظن والترجيح، وذلك لاستبعاد قرينة البراءة اللاصقة بكل إنسان، استنادا إلى أن

[1] – **محمد علي السالم عياد الحلبي**، "حرية القاضي الجنائي في الاقتناع في قوانين مصر، الأردن والكويت"، مجلة الحقوق الكويتية، تصدر عن كلية الحقوق، جامعة الكويت، العدد الثالث، السنة الحادية والثلاثون، سبتمبر 2007، ص 376.

الأصل في الإنسان البراءة يلزم القاضي أن يبني اقتناعه على سبيل اليقين والجزم، والمطلوب عند الاقتناع ليس اليقين الشخصي فحسب، وإنما هو اليقين القضائي الذي يمكن أن يصل إليه الكافة لاستقامته على أدلة تحمل بذاتها معالم قوتها في الإقناع[1]، والأمر لا يختلف بالنسبة للدليل الإلكتروني، إذ يشترط أن يكون هو الآخر يقينيا حتى يمكن الحكم بالإدانة.

أولا: الجزم بإدانة أو براءة المتهم استنادا على الدليل الإلكتروني

يتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من أدلة إلكترونية، وهكذا يستطيع القاضي من خلال ذلك وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة إليها أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة – الجرائم المعلوماتية– إلى شخص معين من عدمه، وبهذا المفهوم يقوم اقتناع القاضي على عنصرين:

- شخصي يلخص في ارتياح ضمير القاضي واطمئنان نفسه إلى إدانة المتهم على سبيل الجزم واليقين، بالاستناد إلى : المعرفة الحسية، التي تدركها الحواس، والمعرفة العقلية التي يتوصل إليها القاضي بعد التحليل والاستنتاج من خلال الربط بين هذه المخرجات والملابسات التي أحاطت بها[2].
- موضوعي: يلخص في ارتكاب هذا الارتياح والاطمئنان على أدلة من شأنها أن يفض لذلك وفقا لمقتضيات العقل والمنطق، بحيث لا يكون عمل القاضي ابتداعا للوقائع وانتزاعا من الخيال[3].

إن الجزم بوقوع الجريمة المعلوماتية ونسبتها إلى المتهم المعلوماتي تتطلب نوعا جديدا من المعرفة وهي المعرفة العلمية للقاضي بالأمور المعلوماتية لاسيما وأن القاضي الجزائي يلعب دورا إيجابيا في الإثبات، وقد يؤدي الجهل في بعض الأحيان إلى التشكيك في قيمة الدليل الإلكتروني ومن ثم يقضي بالبراءة، لاسيما أن الشك يستفيد منه المتهم المعلوماتي في مرحلة المحاكمة وهذا ما يؤدي إلى إفلات المجرمين من تطبيق القانون.

---

[1]– **أحمد فتحي سرور**، الوسيط في قانون الإجراءات الجنائية، مرجع سابق، ص 475.

[2]– مرجع نفسه، ص 181.

[3] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 180.

أن اتباع القاضي الجزائي لطرق الإثبات لا يشكّل استثناء على سلطته التقديرية للأدلة الخاصة بإثبات الوقائع غير الجزائية، لأن مجالها ليس الإثبات الجزائي، الذي هدفه هو أن تحول الشك إلى يقين، لأن الاتهام يتشكّل في صورة شك ليأتي القاضي ويمحص الأدلة ويتحرى من وقائعها، وفي النهاية يتحول الشك إلى يقين، فيدان المتهم، أو يبقى الشك الذي يكون لصالح المتهم.

عملا بمبدأ حرية القاضي في الاقتناع، لا يلزم لصحة الحكم أن يكون الدليل الذي يستند إليه القاضي صريحا ومباشرا في الدلالة على ما يستخلصه منه، بل له أن يكوّن عقيدته من صورة صحيحة للواقعة وإظهار الحقيقة القانونية المرتبطة بها، ثم يستخلص العناصر المطروحة بطريق الاستقراء والاستنتاج العقلي.

ثانيا: شروط تكوين القاضي لعقيدته

يجوز للقاضي أن يكون عقيدته كما يشاء ولكن وفقا لعدة شروط وهي:

– استهداف إظهار الحقيقة كأساس لإقامة الحق، واستخلاص الحقيقة عن طريق استقصائي مشروع، يقرّه القانون، وعدم التعويل في كشف الحقيقة على علم شخصي لا أصل له في أوراق الدعوى.

– يجب أن يكون هناك حد تقف عنده حرية القاضي الجزائي في الاقتناع لا يتخطاه وهو مشروعية الدليل، فالحكم الصادر بالإدانة يعتمد على مجموعة من الإجراءات الجزائية التي لابدّ منها حتى يتولد لدى القاضي اليقين لإصدار الحكم، بشرط أن يتم الحصول على هذه الأدلة بطريق مشروع، فإذا شاب هذه الأدلة أثر عيوب إجرائية، فسيؤدي ذلك إلى بطلان الحكم لمخالفتها النصوص القانونية. بذلك أراد المشرع حماية الحقوق والحريات التي يتمتع بها أطراف الخصومة الجزائية، فنص على ذلك في الدستور والتشريع، ولا يمكن المحافظة على كرامة الإنسان والدفاع عنه إذا أقمنا الدليل على حساب حريته، لأن ذلك سوف يتعارض مع حقوق المتهم كونه اعتداءً على الكيان الإنساني ومصالحه، ولا يمكن المحافظة على مشروعية الأدلة إلا من خلال احترام القانون وتنفيذه كما هو.

–يملك قاضي الموضوع كامل الحرية في أن يختار من طرق الإثبات ما يراه موصلا إلى كشف الحقيقة، ليزن قوة الإثبات النابعة من ضميره ووجدانه بمحض إرادته، فيأخذ ما يطمئن إليه

ويطرح ما لا يطمئن إليه، وهو في كل ذلك لا يسأل لماذا اختار هذه الوسيلة بالضبط، ولا يناقش في تقديره لهذه الأدلة، ولكنه من جهة أخرى يأتي استنتاجه متوافقا مع حكم المنطق السائغ عقلا.

-إذا استقرت لدى القاضي فكرة واضحة مستخلصة من دليل واضح ليسند منطوق الحكم بها، بحيث يكفي لاقتناعه يقضي قضاءه بالإدانة أم بالبراءة، ويجب أن يكون هذا الدليل خاليا من الغموض ولا تناقض فيه. إن تحديد طبيعة الدليل يتطلب بيان صوره وأشكاله، ثم عرض أنواعه، وذلك لضرورة إدراج الدليل في الحكم.

- وجوب ذكر الدليل بالحكم بشكل كافٍ وواضح وليس بالاكتفاء بالإشارة الموجزة إليه بل يجب سرد مضمونه بأسلوب وافٍ، ويبنى مدى تأييده للوقائع التي اقتنعت المحكمة بها.

التناقض الذي يعيب الحكم هو أن تكون الأسباب متهدمة متساقطة لا شيء فيها، ولا يمكن أن يعد قواما لمنطوق الحكم. فالتناقض في أسباب الحكم الذي يترتب عليه اعتباره غير مسبب هو الذي تتماحى به الأسباب بحيث لا يبقى بعدها ما يمكن حمل الحكم عليه، له وجهان أحدهما: يقع في أسباب الحكم نفسه بحيث لا يمكن معه أن يفهم على أي أساس قضت المحكمة، فيصبح كأنه خال من الأسباب ويجوز نقضه ومن ثم إبطاله، أما التناقض بين أسباب حكم تمهيدي صادر في الدعوى، وأسباب حكم آخر قطعي فيها، فلا يصح التحدي به. أما الآخر: صدور الحكم على خلاف حكم سابق ولكن يشترط في هذه الحالة أن يكون الحكم السابق حكما نهائيا فاصلا في الموضوع المتنازع فيه بين الطرفين، مثال التعارض بين الأدلة هو عدم التعرض للخلاف بين الدليلين القولي والفني، مما يزيل التعارض بينهما، فإنّ الحكم يكون قاصرا قصورا يعيبه، ومن صور التناقض أيضا، تخاذل الأسباب التي تعيب الحكم بحيث تكون دلالة بعضها غير مناسبة مع دلالة بعضها البعض، فهو تناقض غير ظاهر، ويلاحظ أيضا أن التناقض في التدليل في الحكم يختلف عن التدليل الوهمي المسبب لبطلان الحكم، وهو عبارة عن أدلة لا مصدر لها في أوراق الدعوى التي أثبتت في الحكم، وبهذا الشكل لا يمكن الاعتداد به كدليل استندت إليه المحكمة بعكس الحقيقة، كأن يسند الحكم أقوال شاهد لم يقلها أو يذكر اعتراف إلى متهم لم يصدر منه، والخطأ في الإسناد الذي يعيب الحكم، هو الذي يؤثر في عقيدة القاضي الذي خلص إليها.

المبحث الثاني

تقييم الدليل الإلكتروني

يشترط في الأدلة المستخرجة من البيئة المعلوماتية والأنترنت أن تكون غير قابلة للشك حتى يمكن الحكم بموجبها بالإدانة، ذلك أنه لا مجال لدحض قرينة البراءة أو افتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين.

خاصة أن الدليل الإلكتروني يثير العديد من المشكلات تتعلق بطبيعته التكوينية من جهة وبإجراءات الحصول عليه من جهة أخرى وهذه المشكلات تعود عليه بالسلب، حيث تضعف من قيمته في مجال الإثبات الجزائي.

يتحقق اليقين للأدلة الإلكترونية أكثر بإخضاعها للتقييم الفني بالوسائل الفنية من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته وكذا صحة الإجراءات المتبعة في الحصول عليه من أجل تفادي تلك العيوب التي قد تشوبه، فمثلما يخضع الدليل الإلكتروني لقواعد وإجراءات معينة تحكم طرق الحصول عليه فإنه يخضع لقواعد أخرى للحكم على قيمته التدليلية من الناحية العلمية وذلك راجع للطبيعة الفنية لهذا الدليل[1].

ستكون دراسة تقييم الدليل الإلكتروني من خلال التعرض إلى أهم المشكلات التي قد تؤثر على قيمته(المطلب الأول)، والموقف الدولي والوطني اتجاه هذه المشكلات (المطلب الثاني).

المطلب الأول

الإشكالات التي تؤثر على تقييم الدليل الإلكتروني

ان العالم مزدحم بشبكات اتصالات دقيقة ومتطورة تنقل وتشغل المعلومات والبيانات من مناطق متباعدة باستخدام تقنيات لا تكفل لها أمنا كاملا، ويتاح في ظلها التلاعب عبر الحدود بتلك المعطيات المنقولة أو المخزنة، مما قد يسبب لبعض الدول، الأفراد أو الشركات أضرارا فادحة، يغدو التعاون الدولي واسع المدى في مكافحة الجرائم المعلوماتية أمرا محتما، خاصة أن

[1]– **خالد عباد الحلبي**، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، عمان، 2011، ص 249.

الدليل الإلكتروني الذي يمكن استخلاصه من أجل إثبات وقوعها ونسبتها إلى مرتكبيها، قد تقل قيمته لإشكالات موضوعية وإجرائية عديدة.

رغم ضرورة هذا التعاون والمناداة به، إلا أنه ثمة صعوبات ومعوقات تقف دون تحققه وتجعله صعب المنال.

من خلال هذا المطلب سوف يحاول إبراز أهم هذه المعوقات في الفرعين التاليين، الإشكالات الموضوعية(الفرع الأول) والإشكالات الإجرائية (الفرع الثاني)

الفرع الأول

الإشكالات الموضوعية للدليل الإلكتروني

غالبا ما تتعلق بطبيعة الدليل ذاته، وذلك بسبب الخصائص الفيزيائية التي يتكون منها هذا الدليل.

أولا: أهم الإشكالات الموضوعية

أ- **التعدي على الخصوصية:** إن الدليل الإلكتروني دليل غير مرئي عبارة عن سجل كهرومغناطيسي مخزن في نظام حاسوبي في شكل ثنائي وبطريقة غير منظمة، فعلى سبيل المثال تتضمن الأقراص الصلبة مزيجا بين بيانات مختلفة فيما بينها والتي لن تكون كلها ذات صلة بالمسألة المطروحة، بمعنى أن هناك اختلاطا بين الملفات البريئة مع تلك المجرمة التي تعد موضوعا للدليل الإلكتروني مما يؤدي إلى التعدي على الخصوصية[1].

ب- **غياب الآثار المادية:** ينتج عن الجرائم التقليدية آثار مادية تسهل على رجال العدالة إثباتها بعكس الجرائم المعلوماتية حيث يكون ذلك في منتهى الصعوبة، بل الدليل الإلكتروني فيها عبارة عن نبضات إلكترونية مكونة من سلسلة طويلة من الأصفار، لا تفصح عن شخصية معينة، وهذه المشكلة تظهر بصفة جلية مع شبكة الأنترنت حيث تسمح لمستخدميها الاتصال دون كشف عن أسمائهم الحقيقية كإرسال رسائل البريد الإلكتروني مجهولة المصدر، فضلا عن ذلك غالبا ما يكون الدليل الإلكتروني مشفرا، كما يمكن تعديله والتلاعب فيه، مما يقطع الصلة بين المجرم

[1] - **عائشة بن قارة مصطفى**، مرجع سابق، ص 162.

وجريمته، وتحول دون كشف شخصيته، وبذلك يشكل هذا الدليل عائقا أمام رجال التحري والتحقيق خاصة أنهم اعتادوا على الإثبات المادي للجرائم.

ج- **صعوبة تعقب الدليل الإلكتروني وضبطه:** ينتقل الدليل الإلكتروني عبر شبكات الاتصال بسرعة ديناميكية فائقة بمعنى إمكانية تخزين المعلومات أو البيانات في الخارج بواسطة شبكة الاتصال عن بعد ويترتب على ذلك صعوبة تعقب الأدلة الإلكترونية وضبطها، لأنه يستلزم القيام بأعمال إجرائية خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها، مثل معاينة مواقع الأنترنت المخالفة، تفتيش نظم الحاسب الآلي، ضبط الأقراص الصلة التي تحتوي على مواد غير مشروعة كالصور الإباحية مثلا، وهذا كله يصطدم بمشاكل الحدود والولايات القضائية، ويرجع السبب في ذلك إلى أن هذه الإجراءات تمثل مساسا بسيادة الدولة التي عبر من خلالها نشاط المجرم وهو في طريقه للهدف، أو حيث قد توجد أدلة الجريمة، وهو ما ترفضه الغالبية من الدول[1].

اضف إلى ذلك مشكلة طلبات الإنابة القضائية الدولية التي تعد من أهم صور المساعدات القضائية الدولية في المجال الجزائي أن تسلم بالطرق الدبلوماسية وهذا بالطبع يجعلها تتسم بالبطء والتعقيد، والذي يتعارض مع طبيعة الأنترنت وما تتميز به من سرعة، وهو الأمر الذي انعكس أدلة الإثبات في الجرائم المعلوماتية. كذلك من الصعوبات الكبيرة في مجال المساعدات القضائية الدولية المتبادلة التباطؤ في الرد، حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد على الطلب سواء بسب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة وغيرها من الأسباب . فكم هو محبط شطب قضية لعدم تلبية طلب بسيط في الوقت المناسب[2].

---

[1] – **عائشة بن قارة مصطفى**، مرجع سابق، ص 163.

[2] – **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، ص 55، محمول من الموقع الإلكتروني التالي: www.minshawi.com/vb/attachment.php?attachmentid=337&d.jl
تم الاطلاع عليه يوم: 2016/07/23.

د- **مدى الاعتداد بالنسخ:** يستخرج الدليل الإلكتروني من الكمبيوتر في شكل نسخة وليس أصل، حيث أن الأصالة في هذا الدليل الإلكتروني لها طابع افتراضي لا يرتقي إلى مستوى الأصالة في الدليل المادي، فهذا الأخير يعبر عن وضعية مادية ملموسة، كما هو الشأن في الورق المكتوب أو بصمة الأصبع، في حين أن الدليل الإلكتروني عبارة عن تعداد غير محدود لأرقام ثنائية موحدة في الصفر والواحد (0-1) فالصورة مثلا في العالم الرقمي ليس لها ذلك الوجود المادي كما في الشكل الورقي، وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه، فكل شيء في العالم الرقمي يتكون من الصفر والواحد، وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة.

هـ- **عدم وجود نموذج موحد للنشاط الإجرامي المعلوماتي**[1]: بنظرة متأنية للأنظمة القانونية القائمة في الكثير من الدولة لمواجهة الجرائم المعلوماتية، عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الأنترنت الواجب تجريمها، فما يكون مباحا في أحد الأنظمة قد يكون مجرّما وغير مباح في نظام آخر. ويمكن إرجاع ذلك إلى عدة أسباب وعوامل كاختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لآخر، وهذا الخلل ينجم عنه أشكال أخرى مثل عدم وجود التجريم المزدوج والذي يعد من أهم الشروط الخاصة بنظام تسليم المجرمين فهو منصوص عليه في أغلب التشريعات الوطنية والصكوك الدولية المعنية بتسليم المجرمين، وبالرغم من أهميته، إلا انه قد يكون عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية، بالإضافة إلى أنه من الصعوبة تحديد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بشبكة الأنترنت أو لا، الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المتعلقة بالأنترنت . بالتالي اختلاف السياسة التشريعية من مجتمع لآخر[2] يوثر سلبا على الجانب الإجرائي، فعدم وجود نموذج موحد للجريمة المعلوماتية يؤثر كذلك على دليل إثباتها.

---

[1] - **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، مرجع سابق، ص102.

[2] - **جميل عبد الباقي الصغير**، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 1998، ص 91.

و- **تنوع واختلاف النظم القانونية الإجرائية:** إن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها، كما هو الحال بالنسبة للمراقبة الإلكترونية، والتسليم المراقب، والعمليات المستترة، وغيرها من الإجراءات الشبيهة، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى، وبالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنقاذ القانون في الدولة الأخرى على استخدام ما تعتبره هي أنه أداة فعّالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق تري هذه الدولة أنها طرق غير مشروعة، حتى وإن كان هذا الدليل تم الحصول عليه في اختصاص قضائي وبشكل مشروع[1].

ز- **عدم وجود أو نقص قنوات اتصال:** أهم الأهداف المرجوة في مجال الجريمة والمجرمين، الحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لزاما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العملية التي غالبا ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين.

ثانيا: الحلول لمواجهة الإشكالات الموضوعية

حتى لا تبقى الإشكالات السالفة الذكر عقبة أمام القاضي حين قيامه بتقييم الدليل الإلكتروني، وبالتالي تكوين اقتناعه، كان لا بد من إيجاد حلول بشأنها في سبيل إرساء العدالة.

أ- إن نقص الثقافة المعلوماتية للقاضي الجزائي قد يحتم وكواجب قضائي عليه الاستعانة في هذه المسائل بوسائل الخبرة كنهج ليس من أجل استقاء الدليل فحسب، بل لبحث مصداقيته في مجال المعالجة الآلية للمعلومات وتحقيق اليقينية لهذا الدليل.

[1]- **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص53.

غالبا ما يتم اللجوء إلى الخبرة في مجال التعامل مع أي ظاهرة فنية، لاسيما في مجال تكنولوجيا المعلومات والأنترنت، فهي تؤدي دور لا يستهان به إزاء نقص معرفة رجال القانون للجوانب التقنية في الجرائم المعلوماتية.

للتأكد من سلامة الدليل الإلكتروني من التبديل والتغيير وذلك في حالة عدم الحصول على النسخة الأصلية يستعمل الخبير التقني عدة أنظمة يذكر منها:

- استعمال الدليل المحايد: وهو نوع من الأدلة الإلكترونية المخزونة في البيئة الافتراضية لا علاقة له بموضوع الجريمة، ولكنه يساعد في التأكد في مدى سلامة الدليل الإلكتروني المقصود من حيث عدم حصول أي تعديل عليه في النظام الكمبيوتري.
- التحليل التناظري الإلكتروني: يتم من خلاله مقارنة الدليل الإلكتروني المقدم للقضاء بالأصل المدرج بالآلة الإلكترونية، ومن ثم يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا، ويستعان في ذلك باستخدام علم الكمبيوتر الذي يلعب مهما في تقديم المعلومات الفنية التي تساهم في فهم مضمون ووجود الدليل الإلكتروني، وهذا العلم يستعان به أيضا في كشف مدى التلاعب بمضمون هذا الدليل[1].

كما أن الأمر يحتم إخضاع مجموعة الإجراءات الفنية إلى اختبارات كوسيلة للتأكد من سلامتها من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات، ويتبع في ذلك مجموعة من الخطوات أهمها:

- إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج ويكون ذلك بإتباع اختبارين أساسيين يتم التأكد من خلالهما أن الأداة المستخدمة عرضت كل المعطيات المتعلقة بالدليل الإلكتروني وفي الوقت ذاته لم يضف إليها أي بيان جديد، وهو ما قد يعطي للنتائج المتقدمة مصداقية في التدليل على الوقائع، ويتمثل هذان الاختباران في:

[1] – **سعيداني نعيم**، مرجع سابق، ص 225.

– اختبار السلبيات الزائفة ومفادها أن تخضع الأداة المستخدمة في الحصول على دليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الإلكتروني، وأنه لم يتم إغفال معطيات مهمة عنه.

– اختبار الإيجابيات الزائفة ومفاده إخضاع الأدلة المستخدمة في الحصول على الدليل الإلكتروني لاختبار يمكن من التأكد من أن هذه الأداة لا تعرض معطيات إضافية جديدة[1].

تجدر الإشارة إلى أن هذه الخبرة تشكل عبئا ثقيلا على العدالة الجنائية بالنظر إلى حجم ومقدار المصاريف التي يتم إنفاقها في سبيل الحصول على الدليل الإلكتروني، وإن كان الإنفاق يتفاوت حسب ما إذا كانت الدولة تأخذ بالنظام الإتهامي أو بنظام التنقيبي[2] غير أن الإشكال الأساسي لا يتعلق بطبيعة النظام الإجرائي المتبع في كل دولة، وإنما ينحصر في طبيعة الدليل الإلكتروني وما يتطلب إثباته من تكاليف باهظة، خاصة أمام غياب منظمات متخصصة كالجامعات والمعاهد لاسيما في الدول العربية، حيث يتطلب الأمر اللجوء إلى شركات أجنبية في الخارج مما يجعل التكاليف تخضع للسعر العالمي المقرر في اللوائح المالية لتلك المنظمات.

ب– إنّ البحث في موضوع الأصالة على المستوى القانوني جعل المشرع المقارن يعتمد منطق افتراض أصالة الدليل الإلكتروني، وقد تضمن قانون الإثبات الأمريكي في الولايات المتحدة الأمريكية نصا صريحا في القاعدة 1001 بند 3 وقانون البوليس والإثبات البريطاني لسنة 1984 حتى تتحقق بتقنية الأدلة الإلكترونية أن تكون البيانات دقيقة وناتجة عن الحاسوب بصورة سليمة حيث يسمح استثناء بقبول الدليل الإلكتروني باعتباره مستندا أصليا ما دام أن البيانات مطبوعة أو مسجلة على دعامات أخرى ومقروءة للعين المجردة وتعبر عن البيانات الأصلية بشكل دقيق.

ج– أما فيما يتعلق بعدم وجود نموذج موحد للنشاط الإجرامي فإن الأمر يقتضي توحيد هذه النظم القانونية، ولاستحالة هذا الأمر فإنه لا مناص من البحث عن وسيلة أخرى تساعد على إيجاد تعاون دولي يتفق مع طبيعة هذا النوع المستحدث من الجرائم ويخفف من غلو الفوارق بين الأنظمة العقابية الداخلة، وتتمثل هذه الوسيلة في تحديث التشريعات المحلية المعنية بالجرائم

[1] – **سعيداني نعيم**، مرجع سابق، ص 226.

[2] – **عمر محمد أبو بكر بن يونس**، الجرائم الناشئة عن استخدام الأنترنت، مرجع سابق، ص 987.

المعلوماتية وإبرام اتفاقيات خاصة يراعي فيها هذا النوع من الجرائم.

د- بالنسبة لتنوع واختلاف النظم القانونية الإجرائية، فالصكوك الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة، الشيء الذي يخفف من غلو واختلاف النظم القانونية والإجرائية ويفتح المجال أمام تعاون دولي فعّال، مثلا المادة 34 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[1] أما المادة 20 منها تشير في هذا الصدد إلى التسليم المراقب، والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة[(2)]، والتي تعتبر من أهم التقنيات المستخدمة في التصدي للجماعات الإجرامية المنظمة المحنكة بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها وتجميع المعلومات وأدلة الإثبات لاستخدامها فيما بعد في الملاحقات القضائية المحلية منها أو الدولية في دول أطراف في سياق نظم المساعدة القانونية المتبادلة.

هذا ما أكدت عليه اتفاقية بودابست حيث نصت المادة 29 على سرية حفظ البيانات المعلوماتية المخزنة وأجازت لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكاني لذلك الطرف الآخر والتي ينوي الطرف طالب المساعدة أن يقدم طلباً للمساعدة بشأنها بغرض القيام بالتفتيش أو الدخول بأي طريقة مماثلة، وضبط أو الحصول أو الكشف عن البيانات المشار إليها.

---

[1]- **اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية** المعتمدة من طرف الجمعية العامة لمنظمة الأمم المتحدة يوم 15 نوفمبر 2000، صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 02-55 ممضي في 05 فبراير 2002، يتضمن التصديق بتحفظ عليها، الجريدة الرسمية للجمهورية الجزائرية، عدد 9 بتاريخ 10 فبراير 2002.

[2] - المادة 11 من **اتفاقية الأمم المتحدة لمكافحة الإتجار غير المشروع بالمخدرات والمؤثرات العقلية** الموافق عليها في فيينا بتاريخ 20 ديسمبر 1988، صادقت عليها الجزائر بموجب مرسوم تشريعي رقم 94-02 ممضي في 05 مارس 1994، يتضمن الموافقة عليها مع تحفظ، الجريدة الرسمية للجمهورية الجزائرية، عدد 12 بتاريخ 06 مارس 1994.

المادة 50 من **اتفاقية الأمم المتحدة لمكافحة الفساد**، المعتمدة من قبل الجمعية العامة للأمم المتحدة بنيويورك يوم 31 اكتوبر 2003، صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 06-128 من عام 1425 الموافق ل 19 ابريل 2006، يتضمن التصديق بتحفظ عليها، الجريدة الرسمية للجمهورية الجزائرية، عدد 26 بتاريخ 25 ابريل 2006.

أضافت المادة 30 من ذات الاتفاقية على الكشف السريع عن البيانات المحفوظة حيث نصت على: أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة والمتعلقة باتصال خاص تطبيقاً لما هو وارد في المادة 29 فإن الطرف المساند إذا اكتشف وجود مؤدي خدمة في بلد آخر قد شارك في نقل هذا الاتصال فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة حتى يمكن تحديد هوية مؤدي الخدمة هذا والطريق الذي تم الاتصال من خلاله.

أشارت المادة 31 من هذه الاتفاقية إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش أو أن يدخل بأي طريقة مشابهة وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني لذلك الطرف والتي يدخل فيها أيضاً البيانات المحفوظة وفقاً للمادة 29، ويجب الاستجابة لمثل هذا الطلب بأسرع ما يمكن في الحالات الآتية: إذا كانت هناك أسباب تدعو للاعتقاد أن البيانات المعنية عرضة على وجه الخصوص لمخاطر الفقد أو التعديل، أو أن الوسائل والاتفاقات والتشريعات الواردة في الفقرة 2 تستلزم تعاوناً سريعاً.

أن المادة 32 من ذات الاتفاقية سمحت بالدخول للبيانات المخزنة خارج نطاق الحدود بشرط أن يكون ذلك بموجب اتفاق، أو أن تكون هذه البيانات متاحة للجمهور.

أيضا نصت المادة 33 على تعاون الدول الأطراف فيما بينها لجمع البيانات في الوقت الحقيقي عن التجارة غير المشروعة، والمرتبطة باتصالات خاصة على أرضها تتم بواسطة شبكة معلومات، وفي إطار ما هو منصوص عليه في الفقرة الثانية، وينظم هذا التعاون الشروط والإجراءات المنصوص عليها في القانون الداخلي، ويمنح كل طرف تلك المساعدة على الأقل بالنسبة للجرائم التي يكون جمع المعلومات بشأنها في الوقت الحقيقي متوافر في الأمور المشابهة على المستوى المحلي.

هناك أيضا المادة 34 من الاتفاقية ذاتها والتي نصت على التعاون في مجال التقاط البيانات المتعلقة بمضمون الاتصالات النوعية التي تتم عن طريق إحدى شبكات المعلومات.

يلاحظ مما سبق أن اتفاقية بودابست أوجدت بعض الحلول التي من شأنها التغلب على مشكلة اختلاف النظم الإجرائية أمام التعاون الدولي لمواجهة الجرائم المتعلقة بشبكة الأنترنت .

للحد من ظاهرة عدم وجود قنوات اتصال بين جهات إنفاذ القانون فنلاحظ أنه غالبا ما تشجع الصكوك الدولية الدول إلى التعاون فيما بينها وتدعوها إلى إنشاء قنوات اتصال بين سلطاتها المختصة ووكالاتها ودوائرها المتخصصة بغية التيسير في الحصول على هذه المعلومات وتبادلها[1]، ومن الأمثلة على هذه الصكوك الدولية اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في المادة 27 منها، والمادة 9 من اتفاقية 1988، والمادة 48 من اتفاقية الأمم المتحدة لمكافحة الفساد، والبند الثاني من المادة 27 من الاتفاقية الأوربية بشأن الإجرام المعلوماتى، والمادة35 من ذات الاتفاقية الأوربية والتي أوجبت على الدول الأطراف فيها ضرورة تحديد نقطة اتصال تعمل لمدة 24 ساعة يومياً طوال أيام الأسبوع لكي تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشبكات، أو استقبال الأدلة ذات الشكل الإلكتروني، وهذه المساعدة تشمل تسهيل أو، إذا سمحت الممارسات والقوانين الداخلية بذلك، تطبيق الإجراءات التالية بصفة مباشرة؛ – إسداء النصيحة الفنية –حفظ البيانات وفقاً للمواد 29، 30 –جمع الأدلة وإعطاء المعلومات ذات الطابع القضائي وتحديد أماكن المشتبه فيهم .

كما أوجبت ذات المادة على الدول الأطراف ضرورة أن تتمكن نقطة الاتصال من الاتصال السريع بنقطة اتصال الطرف الآخر، وأن يعمل كل طرف على أن يتوافر لديه الأفراد المدربين القادرين على تسهيل عمل الشبكة.

هـ– لأجل القضاء على مشكلة التجريم المزدوج والذي يعد من أهم الشروط الخاصة بنظام تسليم المجرمين ركزت الاتجاهات والتطورات التشريعية الخاصة بتسليم المجرمين على تخفيف التطبيق الصارم لهذا الشرط، وذلك بإدراج أحكام عامة في المعاهدات والاتفاقيات المعنية بتسليم المجرمين وذلك إما بسرد الأفعال والتي تتطلب أن تجرم كجرائم أو أفعال مخلة بمقتضي قوانين الدولتين معا أو بمجرد السماح بالتسليم لأي سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة[2].

---

[1] – **توصية المجلس الأوربي رقم (R95)13** بشأن مشاكل الإجراءات الجزائية المتعلقة بتكنولوجيا المعلومات، سالفة الذكر.

[2] – **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص60.

و- ان الصعوبات الخاصة بالمساعدات القضائية الدولية والتباطؤ في الرد فان الحاجة ملحة إلى إيجاد وسيلة أو طريقة تتسم بالسرعة تسلم من خلالها طلبات الإنابة كتعين سلطة مركزية مثلا أو السماح بالاتصال المباشر بين الجهات المختص في نظر مثل هذه الطلبات لنقضي على مشكلة البطء والتعقيد في تسليم طلبات الإنابة. وهذا بالفعل ما أوصي به مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية والذي انعقد في بانكوك في الفترة من 18-2005/4/25[1] حيث أكد على ضرورة تعزيز فعالية السلطات المركزية المعنية الضالعة في أعمال المساعدة القانونية المتبادلة وإقامة قنوات مباشرة للاتصال فيما بينها بغية ضمان تنفيذ الطلبات في الوقت المناسب، والشيء نفسه في البند الثاني من المادة 27 من اتفاقية بودابست، والمادة35 من ذات الاتفاقية الأوربية والتي أوجبت على الدول الأطراف فيها ضرورة تحديد نقطة اتصال تعمل لمدة 24 ساعة يومياً طوال أيام الأسبوع لكي تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشبكات، أو الاستقبال الأدلة في الشكل الإلكتروني عن الجرائم. كما أوجبت المادة ذاتها على الدول الأطراف ضرورة أن تتمكن نقطة الاتصال من الاتصال السريع بنقطة اتصال الطرف الآخر. وأن يعمل كل طرف على أن يتوافر لديه الأفراد المدربين القادرين على تسهيل عمل الشبكة.

أما بالنسبة للرد على طلبات التماس المساعدة فإنه من الضرورة بمكان الاستجابة الفورية والسريعة على هذه الطلبات، لأجل ذلك تنص غالبية المعاهدات والاتفاقيات الخاصة بالمساعدات القضائية المتبادلة على ضرورة الاستجابة الفورية والسريعة على طلبات التماس المساعدة. وهذا ما أكدت عليه الفقرة الثالثة من المادة 25 من اتفاقية بودابست حيث نصت على أنه يمكن لكل طرف، في الحالات الطارئة أن يوجه طلباً للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل الاتصال السريعة مثل الفاكس أو البريد الإلكتروني على أن تستوفي هذه الوسائل الشروط الكافية المتعلقة بالأمن وصحتها مع تأكيد رسمي لاحق إذا اقتضت الدولة المطلوب منها المساعدة في ذلك. وتقوم الدولة بالموافقة على هذا الطلب والرد عليه عن طريق إحدى وسائل الاتصال السريعة.

---

[1] - Congrès des nations Unies , 11ème , pour la prévention du crime et la justice pénale, 18 – 25 Avril 2005, Bangkok (Thaïlande),in ; www.11uncongress.org. Consulté le :04/02/2012.

الفرع الثاني

الإشكالات الإجرائية للدليل الإلكتروني

سبق الحديث على أن الدليل الإلكتروني يتم الحصول عليه بإتباع جملة من الإجراءات الفنية والتي من الممكن أن يعتريها الكثير من الإشكالات نظرا للطبيعة التكوينية للدليل الإلكتروني.

أولا: أهم الإشكالات الإجرائية

أ- **مشكلة الاختصاص في الجرائم المعلوماتية:** الجرائم المعلوماتية من أكبر الجرائم التي تثير مسألة الاختصاص على المستوى الدولي ولا توجد أي مشكلة بالنسبة للاختصاص على المستوى الوطني أو المحلى حيث يتم الرجوع إلى المعايير المحددة قانونا لذلك[1]، أما على المستوى الدولي ان اختلاف التشريعات والنظم القانونية والتي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المعلوماتية التي تتميز بكونها عابرة للحدود. فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجزائي للدولة الأولى استنادا إلى مبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبيه، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية[2]. كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الاطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة.

ب- **مشكلة الخبرة والتدريب في الجرائم المعلوماتية:** إن الطبيعة الخاصة للدليل الإلكتروني في مجال الجريمة المعلوماتية انعكس على عمل الجهات المكلفة بالتحقيق والمحاكمة حيث يتطلب الكشف عن هذه الجرائم وإثباتها إتباع استراتيجيات خاصة تتعلق باكتسابهم مهارات خاصة على نحو يساعدهم على مواجهة تقنيات الحاسب الآلي وشبكاته.

---

[1] – هذه المعايير الثلاثة هي مكان القبض على المتهم، مكان وقوع الجريمة أو محل إقامة المتهم.

[2] – **جميل عبد الباقي الصغير**، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، مرجع سابق، ص 73.

أنه من المتصور أن تجد الجهات المكلفة بالقبض والتحقيق نفسها غير قادرة على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذه النوعية من الجرائم، فكثيرا ما تفشل جهات التحقيق في جمع الأدلة الإلكترونية، بل إن المحقق نفسه قد يدمر الدليل بخطأ منه أو بإهمال، بحيث تتعقد التقنيات المرتبطة بارتكاب تلك الجرائم لذا يجب استخدام تقنيات تحقيق جديدة لتحديد نوعية الجريمة المرتكبة وشخصية مرتكبيها وكيفية ارتكابها مع الاستعانة بوسائل جديدة لضبط الجاني والحصول على أدلة إدانته[1].

إن بعض الدول لا ترى في التدريب دور إيجابي في تطوير العمل من خلال تطبيق ما تعلمه المتدربون في الدورات التدريبية وما اكتسبوه من خبرات. ومن الصعوبات أيضا والتي قد تهدد التعاون في مجال التدريب ما يتعلق بالفوارق الفردية بين المتدربين وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدي مختلف الأفراد المتدربين، لاسيما في مجال تكنولوجيا المعلومات وشبكات الاتصال حيث أنه يوجد بعض الأشخاص ممن لا يعي في هذا المجال شيء، وعلى النظير يوجد أشخاص آخرين على درجة كبيرة من المعرفة والثقافة في هذا المجال[2].

إضافة إلى أن نظرة المتدرب إلى الدورة التدريبية على أنها مرحلة تدريبية أو عبء لا طائل منه تهدد العملية التدريبية برمتها وبالطبع نسف التعاون الدولي في هذا المجال.

أيضا من الصعوبات التي قد تؤثر على العملية التدريبية ما يتعلق بالملامح العامة المميزة للبيئة التدريبية وعدم قدرتها على تمثيل الواقع العملي لبيئة العمل الطبيعية تمثيلا تاما ومتقنا، من حيث ما يدور بها من وقائع وملابسات وإجراءات، وما يتم فيها من نشاطات لا تبلغ حد التطابق مع طبيعة المهام التي سيؤديها المتدربون في بيئة العمل الطبيعية.

ثانيا: الحلول لمواجهة الإشكالات الإجرائية

بالنسبة لمشكلة الاختصاص في الجرائم المعلوماتية، ثمة حاجة ملحة إلى إبرام اتفاقيات

---

[1]– **Sassi BEN HALIMA**, op.cit, p 610.

[2] – **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص56.

دولية - ثنائية أو جماعية- يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي خاصة بالنسبة للجرائم المعلوماتية[1] بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرائية بما يتناسب التطور الكبير التي تشهده تكنولوجيا المعلومات والاتصالات.

أما فيما يتعلق بالصعوبات المتعلقة بمجال التدريب من اجل اكتساب الخبرة فإنه يمكن التغلب عليها بإجراء المزيد من الحملات التوعوية للتنبيه بمخاطر الجرائم المعلوماتية والأضرار التي تسببها وبأهمية تدريب رجال العدالة الجزائية على مواجهتها، كما أنه وبمزيد من التنسيق بن الأجهزة المعنية بتدريب رجال تنفيذ القانون إيجاد برامج تدريبية مشتركة تناسب جميع الفئات، هذا بالإضافة إلى القيام ببعض العمليات المشتركة والتي من شأنها صقل مهارات القائمين على مكافحة تلك الجرائم وتقريب وجهات النظر بشأنها.

لذلك يجب أن تخصص كل دولة إدارة متخصصة بهذا النوع من القضايا، ذلك لتلقي البلاغات وملاحقة المجرم الإلكتروني والبحث عن الأدلة ضدهم وتقديمهم للمحاكمة[2].

المطلب الثاني

الموقف الدولي والوطني أمام إشكالات الدليل الإلكتروني

إنّ القضاء على إشكاليات الدليل الإلكتروني لا يكون إلا بمواجهة الجريمة المعلوماتية، فإن البعد الدولي للجريمة المعلوماتية وصعوبة ضبط الأدلة الإلكترونية الناجمة عنها يفرض على المجتمع الدولي تقوية وسائل الإثبات الجزائية بما يتناسب مع الجانب التقني لهذه الجريمة، كما يفرض البحث عن وسائل أكثر ملائمة لطبيعة هذه الجرائم لتضييق الثغرات القانونية التي برع مرتكبوها في استغلالها للتهرب من العقاب ولنشر نشاطهم الإجرامي في مناطق مختلفة من العالم.

لقد أثبت الواقع العملي أن أي دولة لا تستطيع بجهودها المنفردة القضاء على الجريمة المعلوماتية، خاصة مع التطور الملموس والمذهل في الاتصالات وتكنولوجيات المعلومات.

---

[1]– على سبيل المثال المادة 22 من الاتفاقية بودابست سالفة الذكر .

[2]– **رأفت رضوان**، "شرطة الأنترنت"، مجلة مركز بحوث الشرطة، تصدر عن أكاديمية مبارك للأمن، القاهرة، العدد 26، يوليو 2004، ص 111.

يمكن ارتكاب الجريمة المعلوماتية من أقصى بقاع الأرض بنفس سهولة ارتكابها من أقرب مكان، كما أن رسالة واحدة تعزز ارتكاب جريمة معلوماتية يمكن تمريرها من خلال الكثيرين من مقدمي الخدمات في بلدان مختلفة لها نظم قانونية مختلفة، كما أن الآثار الرقمية التي يمكن تتبعها تكون ضعيفة أو سريعة الزوال، ولذا تستلزم اتخاذ إجراء سريع، وهذا تحديداً حين يسعى المرء إلى منع ارتكاب جريمة في مرحلة التنفيذ، مثل شن هجوم إلكتروني على بنية أساسية حرجة، أيضاً حين يسعى المرء إلى جمع أدلة تتصل بجريمة ارتكبت مؤخراً، وتصبح المهمة بالغة الصعوبة حين تعبر الهجمة اختصاصات قضائية متعددة ذات نظم مختلفة في حفظ الأدلة، وهكذا لم تعد تكفي الوسائل التقليدية لإنفاذ القانون.

إنّ بطء الإجراءات الرسمية يجازف بفقدان الأدلة، وقد تكون بلدان متعددة متورطة في الأمر، لذا تشكل متابعة وحفظ سلسلة الأدلة تحدياً كبيراً، بل حتى الجرائم المحلية قد يكون لها بعد دولي، وربما تكون هناك حاجة إلى طلب المساعدة من جميع البلدان التي مرت الهجمة من خلالها.

إذا كانت هناك جريمة واضحة تستحق التحقيق بالفعل، فقد تكون هناك حاجة إلى مساعدة من السلطات في البلد الذي كان منشأ الجريمة، أو من السلطات في البلد أو البلدان التي عبر من خلالها النشاط المجرَّم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة.

يمثّل التعاون الدولي أحد جانبي العلاقات الدولية حيث يقابله في الجانب الآخر الصراع الدولي، فالمتأمل في التاريخ يرى أنّ النظام العالمي يعيش منذ ظهوره حالة من التأرجح، والتعاون الدولي في مكافحة الجريمة يمثل أحد صور التعاون الدولي بمفهومه الشامل، وقد اختلفت صوره عبر الزمان، كما اختلفت أشكاله وأساليبه وآلياته، وكذا اتساع مجالاته وطموحاته نتيجة تطور الجريمة ومناهج الإجرام كانعكاس التطوّر الحضاري والتكنولوجي لاسيما في مجال المواصلات والاتصالات والمعلومات، كان من الضروري أن تتطوّر خطط ومناهج التصدي لها.

إذا كان من الضروري أن تمتلك الدول الإمكانيات التشريعية والقضائية والفنية لضبط والتعامل مع الأدلة الناتجة عن الجرائم المعلوماتية فإنه من الأهم أن تكون تلك القوانين متوائمة ومتجانسة بين مختلف الدول، إذ هي تحمي مصلحة مشتركة.

التعاون الدولي في مكافحة الجريمة المعلوماتية يأخذ مظهران[1]، الأول يتعلق بتداخل الاختصاصات القضائية المتعددة ذات النظم القانونية المختلفة، ويتمثل في التعاون القضائي، والثاني يتعلق بالسعي إلى اتخاذ الإجراءات والآليات ذات الطبيعة التقنية والفنية.

سوف يدرس فيما يلي مظاهر التعاون الدولي القضائي (الفرع الأول)، والتعاون الفني الدولي (الفرع الثاني).

الفرع الأول

التعـاون القضائــي الدولي

يعد التعاون القضائي الدولي من أسمى مظاهر التعاون الدولي في مكافحة الجريمة، إذ يوفّق بين استقلال كل دولة في ممارسة اختصاصها الجزائي على حدود إقليمها، وبين ضرورة ممارسة حقها في العقاب، وبدون هذا التعاون، فلا يمكن للدولة أن تمارسه.

التعاون القضائي الدولي في مواجهة الجريمة المعلوماتية يعد الآلية الرئيسية للكفاح ضد ها فإن فعالية التحقيق والملاحقة القضائية غالبا ما تقتضي الحاجة إلى مساعدة من السلطات في البلد الذي كان منشأً للجريمة، أو من السلطات في البلد الذي عبر من خلاله النشاط المجرم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة، فقد يكون مرتكب الجريمة المعلوماتية من جنسية دولة ما مستعملا في جريمته حواسيب موجودة في دولة أخرى وتقع آثار جريمته في دولة ثالثة فمن البديهي أن يقف مبدأ السيادة ومشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها، لذا فإن التحقيقات في الإجرام السيبراني ومتابعة مرتكبيها قضائيا تؤكد على أهمية المساعدة القضائية المتبادلة بين الدول.

ان أهم صور التعاون القضائي الدولي، المساعدة القضائية الدولية وتسليم المجرمين.

[1]– وهذا ما أكدت عليه **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 14–252 ممضي في 08 سبتمبر 2014، يتضمن التصديق عليها، الجريدة الرسمية للجمهورية الجزائرية عدد 57 بتاريخ 28 سبتمبر 2014.

أولا: المساعدة القضائية الدولية

لا بد من أن يكون هناك تعاون دولي قضائي يتفق مع طبيعة الجريمة المعلوماتية، يسمح هذا التعاون الدولي بسهولة الاتصال المباشر بين أجهزة القضاء في الدول المختلفة.

يعد التعاون القضائي الدولي الآلة الرئيسية لمكافحة الجريمة المعلوماتية، فمن البديهي أن يقف مبدأ السيادة ومشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجريمة ومعاقبة مرتكبيها، لذا فإن التحقيقات في الجرائم المعلوماتية ومتابعة مرتكبيها قضائيا تؤكد على أهمية المساعدة القضائية المتبادلة بين الدول[1].

تعرف المساعدة القضائية الدولية بأنها كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم[2] .

نص المشرع الجزائري على المساعدة القضائية الدولية في مجال الإجرام المعلوماتي في المادة 16 الفقرة الأولى من قانون 09-04 والتي تنص على:" في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني". وتضيف الفقرة الثانية من نفس القانون "يمكن في حالة الاستعجال ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها"، بذلك جعل المشرع الجزائري مبدأ المساعدة القضائية الدولية المتبادلة في إطار التحريات والتحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

---

[1] المادة 32 من **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات**، سالفة الذكر.

[2] – Congrès des nations Unies, 11ème, pour la prévention du crime et la justice pénale, cité précédemment , p5

ان فعالية التحقيق والملاحقة القضائية في الجرائم المعلوماتية غالبا ما تقتضي تتبع أثر النشاط الإجرامي من خلال مجموعة متنوعة من مقدمي خدمات الأنترنت أو الشركات المقدمة لتلك الخدمات مع توصيل أجهزة الحاسب الآلي بالأنترنت، وحتى ينجح المحققون في ذلك فعليهم أن يتتبعوا أثر قناة الاتصالات بأجهزة الحاسب الآلي المصدرية والجهاز الخاص بالضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات وسطاء في بلدان مختلفة، ولتحديد مصدر الجريمة غالبا ما يتعين على أجهزة إنفاذ القانون الاعتماد على السجلات التاريخية التي تبين متى أجريت تلك التوصيلات ومن أين ومن الذي أجراها، وفي أحيان أخرى قد يتطلب إنفاذ القانون تتبع أثر التوصيل ووقت إجرائه، وعندما يكون مقدمو الخدمات خارج نطاق إقليم الدولة، وهو ما يحدث غالبا فإن أجهزة إنفاذ القانون تكون بحاجة إلى مساعدة من نظرائها في دول أخرى، بمعنى الحاجة إلى ما يسمي التعاون القضائي الدولي.

يمتد أثر الجرائم المعلوماتية ذات الطابع الدولي لأكثر من دولة، فتتلخص وقائع قضية شخصين مقيمين في ملبورن بأستراليا بإرسال ما بين ستة إلى سبعة ملايين رسالة إلكترونية على عناوين في أستراليا والولايات المتحدة الأمريكية بالإضافة إلى قيامهما بوضع عدة رسائل على لوحات الرسائل لدى الشركات الرئيسية المقدمة لخدمات الأنترنت، ذلك كله بهدف التشجيع على شراء أسهم إحدى الشركات الأمريكية التي كانت تباع أسهما في الولايات المتحدة الأمريكية في الرابطة الوطنية للأسعار المؤتمنة للمتاجرة بالأوراق المالية "بورصة"NASDAQ، وكانت هذه الرسائل تبشر على غير الحقيقة بزيادة سعر أسهم الشركة بنسبة 900%، ونتيجة لذلك وبعد فترة قصيرة حدثت زيادة في حجم تداول أسهم تلك الشركة لتصل إلى عشرة أمثالها وبالتالي تضاعف سعر السهم، ولقد اعترف أحد المتهمين وهو مساهم في الشركة أنه قدم معلومات زائفة وغير صحيحة وعندما ارتفعت الأسعار باع أسهمه في الشركة محققا بذلك ربحا كبيرا[1]،أن الشخصين قد انتهكا القانون الأسترالي والأمريكي بالإضافة إلى التلاعب في الأسواق المالية ناهيك عن تعطل أجهزة الحاسب الآلي في كلا البلدين بسبب الكم الهائل من الرسائل الإلكترونية.

[1] – **سالم محمد سليمان الاوجلي**، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، 1997، ص 425.

يلاحظ من خلال المثال السابق أن ملاحقة مرتكبي هذه الجرائم وتقديمهم للعدالة من أجل توقيع العقاب عليهم يستلزم القيام بإجراءات إجرائية خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها، من هذه الإجراءات معاينة مواقع الأنترنت في الخارج أو ضبط الأقراص الصلبة أو تفتيش نظم الحاسب الآلي وهذا كله قد يصطدم بمشاكل الحدود والولايات القضائية، ولأن كان كذلك فلا مناص من تقديم المساعدة القانونية المتبادلة، وهذا ذاته ما حصل في الواقعة السابقة حيث كان هناك تعاون بن السلطات الأسترالية والسلطات الأمريكية.

ان المشرع الجزائري في المادة 17 من القانون 09-04[1]، بين إجراءات الاستجابة لطلبات المساعدة، فجاء في نص المادة: " تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل"، وأضافت المادة 18 فقرة 2" يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب"، أما المادة 18 فقرة 1 من نفس القانون فبينت حالات رفض المساعدة القضائية الدولية، فنصت على:" يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام." وتتخذ المساعدة القضائية في المجال الجزائي صور عدة منها:

أ- تبادل المعلومات:

يشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة معينة[2]، عن الاتهامات التي وجهت إلى رعاياها في الخارج

[1] – قانون09-04، سالف الذكر.

[2]– صرح عميد الشرطة مصطفاوي عبد القادر بخصوص أول قضية تمت معالجتها مع دول أجنبية كانت قضية ذات بعد دولي وقعت في نهاية سنة 2009 على إثر بلاغ من مكتب التحقيقات الفدرالية أف. بي. أي، وتنقل ممثلين عنهم لتقديم بلاغ إلى السلطات الجزائرية بسبب تعرّض شركة أمريكية إلى عملية قرصنة بخصوص بيانات بنكية، وتبيّن من التحقيق أنها منظمة إجرامية تنشط في مجال الاختراق والقرصنة ولها شريك في الجزائر، وبعد وصول البلاغ الأجنبي تم توجيه الملف إلى مصالح مديرية الشرطة القضائية فشكلنا فوج للتحقيق متكون من ثلاثة عناصر، ورفعنا التحدي، حيث أسفرت التحريات المكثفة عن تحديد مكان وهوية الشخص الذي اتضح أنه يقطن بإحدى ولايات الشرق الجزائري، تمكنا من إثبات كفاءة الشرطة الجزائرية بتحديد هويته وتقديمه للعدالة. **مجلة السلام**، المصلحة المركزية للجريمة الإلكترونية في مواجهة مجرمي العالم الإفتراضي، 13/02/2016 ،محمول من الموقع الإلكتروني التالي:
http://www.essalamonline.com/ara/permalink/52564.html تم الاطلاع عليه يوم: 2017/06/15.

والإجراءات التي اتخذت ضدهم، وقد يشمل التبادل السوابق القضائية للجناة، بحيث يسمح بالاتصال المباشر بين الأجهزة القضائية والأمنية في الدول المختلفة من أجل تبادل المعلومات المتعلقة بالجريمة والمجرمين[1].

ان هذه الصورة من صور المساعدة القضائية الدولية صدى كبيراً في كثير من الاتفاقيات، أهمها ما ورد في المادة الثالثة والثلاثون من المعاهدة العربية لمكافحة جرائم تقنية المعلومات لتبادل المساعدة في المسائل الجزائية هذه المعاهدة باتفاق أطرافها على أن يقدم كل منهم للآخر أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات أو إجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلا في اختصاص السلطة القضائية للدولة طالبة المساعدة، وكذا ما ورد في البند الثالث والرابع والخامس من المادة الثامنة لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة الوطنية لسنة 2000[2]، إذ أوجبت على الدول الأطراف تيسير تبادل المعلومات المتعلقة بكافة جوانب النشاط الإجرامي.

كذلك ما ورد في الفقرة الثانية من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجزائية[3].

جاء في قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، المادتان 13 و14 منه على إنشاء هيئة وطنية للوقاية من الجرائم المعلوماتية، وتتولى هذه الهيئة خصوصا المهام التالية:

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشان الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

---

[1] – **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص12.

[2]– **اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية**، سالفة الذكر.

[3]- Traité type d'entraide judiciaire en matière pénale, A/RES/45/117 68e séance plénière 14 décembre 1990, in ; https://www.unodc.org/documents/corruption/Publications/Model_Treaties_MLA_FR.pdf. consulté le: 14/05/2016

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

أما المادة 17 من القانون نفسه تنص على أن الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل.

كما جاء في نص المادة 11 من المرسوم الرئاسي 15–261 المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته[1] بتكليف مديرية المراقبة الوقائية واليقظة الإلكترونية على الخصوص بتنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم.

ب– نقل الإجراءات:

يقصد به قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معينة[2] من أهمها التجريم المزدوج الذي يقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات. بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة، وأيضا من الشروط الواجب توافرها أن تكون الإجراءات المطلوب اتخاذها من الأهمية بمكان بحيث تؤدى دورا مهما في الوصول إلى الحقيقة.

أقرت العديد من الاتفاقيات الدولية والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية كاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية عام 2000 في المادة 21 منها.

---

[1] – مرسوم رئاسي 15–261 المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، سالف الذكر.

[2] – **سالم محمد سليمان الأوجلي**، مرجع سابق، ص 427.

ج- الإنابة القضائية الدولية:

إنّ من أجل تسهيل الإجراءات الجزائية بين الدول والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، كالسماع إلى الشهود، إجراء التفتيش أو غيرها من الإجراءات، وجدت الإنابات القضائية الدولية التي بموجبها يمكن للدولة الطالبة – وذلك لضرورة الفصل في مسالة معروضة لدى سلطاتها القضائية– أن تتقدم بطلب اتخاذ إجراء قضائي من الإجراءات الجزائية إلى الدولة المطلوب منها لتعذر قيامها بهذا الإجراء بنفسها[1].

من الوقائع العملية في هذا الصدد، فقد عقد مؤتمر حول مرض الإيدز في هولندا عام 1989، قام أحد الأشخاص المشتركين في هذا المؤتمر بتوزيع أسطوانات على باقي المشتركين تتضمن معلومات عن فيروس الإيدز، ولكن كان يجب على كل مشترك أن يدفع قيمة هذه الأسطوانة، في اجل محدد في حساب معين في احد البنوك، ونظرا لان مجموعة من الأشخاص لم يقوموا بالوفاء، قام الجاني بغلق الأنظمة الخاصة بهم، الأمر الذي يشكل جريمة. عندما تم تحريك دعوى جنائية ضد الجاني في الخارج، قامت هولندا بإمداد السلطات الإنجليزية والأمريكية بمعلومات عن الجاني وعن مغادرته إقليم هولندا، وهذا ساعد على الإمساك به ومحاكمته[2].

في إحدى قضايا الغش المعلوماتي، أسفر البحث عن وجود طرفية حاسب Computer terminal في ألمانيا متصلة بشبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها، فلما أرادت سلطات التحقيق الألمانية الحصول على هذه البيانات، لم يتحقق لها ذلك إلا من خلال التماس المساعدة المتبادلة وبمعرفة المختصين الفنيين[3].

عادة يتم إرسال طلب الإنابة القضائية عبر القنوات الدبلوماسية[4]، فمثلا طلب الحصول

---

[1]- راجع كل عن: **عكاشة محمد عبد العال**، الإنابة القضائية في نطاق العلاقات الخاصة الدولية، الدار الجامعية، بيروت، 1992، ص 13. **جميل عبد الباقي الصغير**، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، مرجع سابق، ص83

[2]- **على حسن الطوالبة**، التعاون القضائي الدولي في مجال مكافحة الجرائم الإلكترونية، ص 12، محمول من الموقع الإلكتروني التالي: https://www.policemc.gov.bh/mcms-store/pdf، تم الاطلاع عليه يوم :2017/02/21.

[3]- **هلالي عبد الله أحمد**، حجية المخرجات الكمبيوترية في المواد الجنائية، مرجع سابق، ص 79.

[4]- Art. 2 du Traité type d'entraide judiciaire en matière pénale. cité précédemment.

على دليل إثبات وهو عادة من شأن النيابة العامة تقوم بتوثيقه المحكمة الوطنية المختصة في الدولة الطالبة ثم يمرر بعد ذلك عن طريق وزارة الخارجية إلى سفارة الدولة متلقية الطلب لتقوم هذه الأخيرة بإرساله بعد ذلك إلى السلطات القضائية المختصة في الدولة متلقية الطلب، وما أن يتم تلبية الطلب ينعكس الاتجاه الوارد في سلسلة العمليات[1]، إلا أنه وسعيا وراء الحد من الروتين والتعقيد والبطء التي تتميز بها الإجراءات الدبلوماسية يحدث وبدرجة متزايدة أن تشترط المعاهدات والاتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن تعين سلطة مركزية – عادة ما تكون وزارة العدل – ترسل إليها الطلبات مباشرة بدلا من الولوج إلى القنوات الدبلوماسية والتي من شأنه تسريع الإجراءات التي قد تأخذ وقتا طويلا فيما لو تم عبر تلك القنوات[2].

هناك عنصران أساسيان للمساعدة الدولية في مكافحة الجريمة: المساعدة غير الرسمية من محقق لآخر، والمساعدة الرسمية المتبادلة.

تكون المساعدة غير الرسمية أسرع إنجازاً، وهي الوسيلة المفضلة للنهج حين لا تكون هناك حاجة إلى صلاحيات إلزامية (أي أوامر تفتيش أو طلب تسليم المجرم)، وهي تقوم على وجود علاقات عمل جيدة بين أجهزة شرطة البلدان المعنية، وتولد نتيجة الاتصالات التي جرت مع الوقت في مسار المؤتمرات وزيارات المجاملة والتحقيقات المشتركة السابقة.

أما المساعدة الرسمية المتبادلة تكون أكثر إرهاقاً يتم اللجوء إليها عادة عملاً بترتيبات معاهدات بين البلدان المعنية وتشمل تبادل الوثائق الرسمية، وهي تشترط في الغالب الأعم أن تكون الجريمة المعنية على درجة معينة من القسوة وأن تشكل جريمة في كل من البلدان الطالبة والموجه إليها الطلب، ويشار إلى هذا الأمر الأخير باعتباره "تجريماً مزدوجاً".

نظرا لأن عامل السرعة يعتبر من العوامل الرئيسية والهامة في مكافحة الجرائم المعلوماتية، ولكون غالبية هذه الاتفاقيات صدرت في وقت لم تكن شبكة الأنترنت قد ظهرت، أو كانت موجودة ولكنها محدودة، فإن تعديل هذه الاتفاقيات التقليدية للتعاون القضائي الدولي أصبح ضرورة ملحة

[1] – **حسين بن سعيد بن سيف الغافري**،"الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص58

[2] – art 3 du Traité type d'entraide judiciaire en matière pénale ,cité précédemment.

خاصة مع التطور الكبير في تكنولوجيا المعلومات والاتصالات[1]، ولأجل ذلك أبرمت العديد من الاتفاقيات الجديدة التي ساهمت في تقصير الوقت واختصار الإجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق، مثال ذلك الاتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفويا في حالة الاستعجال[2]، والفقرة 13 من المادة 46 من اتفاقية الأمم المتحدة لمكافحة الفساد.

ثانيا: تسليم المجرمين

استقر فقه القانون الدولي على اعتبار تسليم المجرمين شكلا من أشكال التعاون القضائي الدولي في مكافحة الجريمة والمجرمين وحماية المجتمعات من المخلين بأمنها واستقرارها وحتى لا يبقى أولئك العابثين بمنأى عن العقاب منتشرين في الأرض فسادا.

يعرّف تسليم المجرمين بأنه" أحد مظاهر التضامن الدولي لمكافحة الجريمة تقوم بموجبه دولة ما بتسليم شخص مقيم في إقليمها إلى دولة أخرى تطلبه لتحاكمه عن جريمة انتهك بها حرمة قوانينها أو لتنفيذ فيه حكما صادرا عليه من إحدى محاكمها ".

يعد تسليم المجرمين أحد مظاهر التعاون الدولي لمكافحة الجريمة وكذا الأركان الأساسية التي يقوم عليها وجود طرفي في التسليم دولتين أو أكثر، إلاّ أنّ هذا النظام في التسمية غير دقيق ويعود ذلك إلى أن التسليم هو عمل تقوم به الدولة المطلوب منها التسليم أما عمل الدولة الطالبة للتسليم فهو الاستيراد أو الاستلام. أما كلمة المجرمين فتعوزها الدقة في التعبير عن الشخص محل التسليم فهي بقدر ما تنطبق على وصف المحكوم عليهم، فهي تتعارض وغير المحكوم عليهم (المتابعين) وذلك إعمالا بمبدأ المتهم برئ حتى تثبت إدانته، إلا أنه ينبغي العمل بالتسمية المتعارف عليها – تسليم المجرمين – رغم عدم دقتها للتعبير عن النظام المرجو منه[3].

هذا النوع من التعاون القضائي الدولي هو نتيجة طبيعية للتطورات التي حدثت في كافة المجالات منها مجال الاتصالات وتقنية المعلومات، حيث لم تعد الحدود القائمة بين الدول تشكل

---

[1] – **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص 15.

[2] – **جميل عبد الباقي الصغير**، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، مرجع سابق، ص86.

[3] – **جمال ماهر**، اتفاقيات التعاون القانوني والقضائي في تسليم المجرمين، ص 2، محمول من الموقع الإلكتروني التالي: http://montada.echoroukonline.com/showthread.php?t=84558 الاطلاع عليه يوم: 2017/02/28.

حاجزاً أمام مرتكبي الجرائم كما أن نشاطهم الإجرامي لم يعد قاصرا على إقليم معين بل أمتد إلى أكثر من إقليم، بحيث بات المجرم منهم يشرع في التحضير لارتكاب جريمته في بلد معين ويقبل على التنفيذ في بلد آخر ويرتكب الفرار إلى بلد ثالث للابتعاد عن أيدي أجهزة العدالة، فالجريمة إذاً أصبح لها طابع دولي والمجرم ذاته أصبح مجرما دوليا، وهذا بالفعل ما ينطبق على الجرائم المتعلقة بالأنترنت.

أن أجهزة إنفاذ القانون لا تستطيع تجاوز حدودها الإقليمية لممارسة الأعمال القضائية على المجرمين الفارين، كان لا بد من إيجاد آلية معينه للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية فوق إقليمها، ولكي يتم ذلك ويكون هناك تعاون دولي ناجح في مجال تحقيق العدالة كان لزاما تنظيم هذا النوع من التعاون الدولي تشريعيا وقضائيا وتنفيذيا، فالدولة ما دامت عضوا في المجتمع الدولي لا بد لها من الإيفاء بالالتزامات المترتبة على هذه العضوية ومن ضمنها الارتباط بعلاقات دولية وثنائية تتعلق باستلام وتسليم المجرمين.

يقوم نظام تسليم المجرمين على أساس أن الدولة التي يتواجد على إقليمها المتهم بارتكاب أحد الجرائم العابرة للحدود ومنها الجرائم المعلوماتية عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك، وإلا كان عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة. فهو إذاً يحقق مصالح الدولتين الأطراف في عملية التسليم، فهو يحقق مصلحة الدولة الأولى في كونه يضمن معاقبة الفرد الذي أخل بقوانينها وتشريعاتها، ويحقق في الوقت ذاته مصلحة للدولة الثانية المطلوب إليها التسليم كونه يساعدها على تطهير إقليمها من فرد خارج عن القانون ومن شأن بقائه فيها تهديد أمنها واستقرارها.

لأن كان كذلك فقد حرصت معظم الدول على سن التشريعات الخاص بتسليم المجرمين، بالإضافة إلى عقد العديد من الاتفاقيات الإقليمية والدولية والثنائية التي تعنى بعملية التسليم، من هذه الدول الجزائر، فهذه الأخيرة نظمت موضوع تسليم المجرمين من خلال قانون الإجراءات الجزائية في المواد من 694 إلى 720 منه.

انّ الجزائر على غرار باقي الدول، ولتنظيم التسليم فإنها سنت موادا في قانون الإجراءات الجزائية، بالإضافة إلى نصوص الاتفاقات الدولية الثنائية منها والمتعددة بشأن التعاون القانوني

والقضائي، فما هو النظام الذي اعتمدته الجزائر بخصوص تسليم المجرمين ؟.

والرجوع إلى أحكام المواد704 إلى 710من قانون الإجراءات الجزائية فإنّ الإجراءات المتعلقة بالاستجواب والقبض المؤقت، الفصل في طلب التسليم بالقبول أو الرفض كله يعود إلى الجهة القضائية – الغرفة الجنائية بالمحكمة العليا، حتى أنّ إقرار الشخص المطلوب قبوله بالتسليم دون اتخاذ الإجراءات القانونية اللازمة، فإنه وجوبا يخضع لإثباته من طرف القضاء.[1]

كما أنّ الفصل في طلب التسليم بالقبول أو الرفض يتميّز بالطابع النهائي الذي لا يقبل الطعن فيه بأي طريق[2].

استخلاصا فإن المشرّع الجزائري أخذ بالنظام القضائي في التسليم واعتبر التسليم عمل قضائي وكل ما يتعلق به مرجعه القضاء من حيث فحص الشروط والإجراءات وكذا قبوله أو رفض، وما على السلطة التنفيذية إلا تنفيذ الأحكام القضائية بوسائلها القانونية[3] المتوفرة لديها.

دراسة موضوع تسليم المجرمين يقتضي بداية بيان ماهيته ثم معرفة شروطه وإجراءاته، وأخير بيان لمظاهر التعاون الدولي في مجال التسليم.

أ- ماهية نظام تسليم المجرمين

أصبح المجرم المعلوماتي بالتبعية مجرما دوليا، ولكون أنه لا يمكن لأي دولة أن تجاوز حدودها الإقليمية لممارسة أعمالها القضائية على المجرمين الفارين، كان لابد من إيجاد آلية معينة للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية فوق إقليمها، تتمثل في تسليم المجرمين الفارين لها[4]. هذا الإجراء يقوم أساسا على قيام دولة ما (الدولة المطلوب منها التسليم) بتسليم

---

[1]- المادة 708 قانون الإجراءات الجزائية الجزائري، سالف الذكر.

[2]- المادة 710 من نفس القانون.

[3]- وزير العدل يقوم بإصدار مرسوم بالإذن بالتسليم يبلغه إلى حكومة الدولة الطالبة. المادة 711 من قانون الإجراءات الجزائية الجزائري، سالف الذكر.

[4]- ان تسليم المجرمين يختلف عن مفاهيم أخرى قد تخلط به فهو لا يعد من قبيل الإبعاد الذي يعد عملا إداريا تستقل باتخاذه الجهة الإدارية في حالات لا يمكن حصرها، ولا يعتبر كذلك من قبيل الطرد التي تمارسه الدولة بما لها من سيادة على إقليمها متى ما رأت أن بقاء الشخص على إقليمها من شأنه أن يؤثر على وجودها أو أمنها. راجع كل عن: **سراج الدين محمد الروبي**، الإنتربول وملاحقة المجرمين، الدار المصرية اللبنانية، القاهرة، 1998، ص 40. **جميل عبد الباقي الصغير**، الجوانب الإجرائية الجرائم المتعلقة بالأنترنت، مرجع سابق، ص 88.

شخصا موجودا في إقليمها إلى دولة أخرى (الدولة طالبة التسليم) بناء على طلبها بغرض محاكمته عن جريمة نسب إليه ارتكابها أو لتنفيذ حكم صادر ضده من محاكمها[1]، بمعنى آخر تسليم دولة لدولة أخرى شخصا منسوبا إليه اقتراف جريمة ما أو صدر ضده حكما بالعقاب كي تتولى محاكمته أو تنفيذ العقاب عليه. إن الدولة التي يتواجد على إقليمها المتهم بارتكاب جريمة معلوماتية عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك، وإلا كان عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة، فهو يحقق بذلك مصلحة الدولتين الأطراف في عملية التسليم، إذ يحقق مصلحة الدولة الأولى في كونه يضمن معاقبة الفرد الذي أخل بقوانينها وفي الوقت ذاته يحقق مصلحة الدولة الثانية المطلوب إليها التسليم كونه يساعدها على تطهير إقليمها من فرد خارج عن القانون[2].

الواضح أن فكرة نظام التسليم تقوم من جهة على وجود علاقة بين دولتين: الأولى تطالب بأن يسلم إليها مرتكب الجريمة لتتخذ بحقه الإجراءات اللازمة لإيقاع العقوبة اللازمة عليه، والثانية يوجه إليها طلب التسليم لتقرر بعد ذلك إما الاستجابة له إذا كان متوافقا مع تشريع نافذ المفعول فيها أو معاهدة أو اتفاق يربط بينها وبين الدولة الطالبة، وإما الرفض لعدم وجود ذاك التشريع أو تلك الاتفاقية، من جهة أخرى فهو يشمل طائفتين من الأشخاص، طائفة الأشخاص المتهمين الذين تسند إليهم ارتكاب جرائم إلا أنه لم يصدر بحقهم أحكام بعد، والفرض هنا أن شخصا ما اقترف جريمة ما في دولة معينة، وقبل أن يلقى القبض عليه يفر هاربا إلى دولة أخرى، عندها تطلب الدولة المرتكب على إقليمها الفعل الإجرامي من الدولة التي فر المتهم هاربا إليها أن تسلمه لها لمحاكمته عما ارتكب من جرم، وطائفة الأشخاص المحكوم عليهم الذين صدر بحقهم حكمٌ بالإدانة إلا أنه لم ينفذ بعد نتيجة لفرارهم إلى دولة أخرى، والفرض هنا أن الشخص المتهم بارتكاب جريمة ما قد لوحق جزائيا من قبل قضاء الدولة التي ارتكب فيها الفعل الإجرامي، وصدر بحقه حكما قضائيا إلا أنه وقبل البدء في التنفيذ يفر هاربا إلى دولة أخرى فتطلب الدولة التي ارتكب فيها الجريمة استلامه من الدولة التي فر إليها.

---

[1]– راجع كل عن: **أحمد بن بخيت الشنفري**، "التعاون الدولي في مجال تسليم المجرمين"، مجلة الأمانة الدورية، تصدر عن مجمع البحوث والدراسات بأكاديمية السلطان قابوس لعلوم الشرطة، مسقط، سلطنة عمان، العدد16، يناير2005، ص155. **جميل عبد الباقي الصغير**، الجوانب الإجراءات للجرائم المتعلقة بالأنترنت، مرجع سابق ص 88.

[2]– **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص18، 19

تتنوع أنظمة تسليم المجرمين وتختلف كل دولة في الطريقة التي تبحث بها طلب التسليم بحسب نوع النظام التي تأخذ به، وهناك ثلاثة أنظمة متبعة في تسليم المجرمين هي:

التسليم الإداري: يتم بموجب هذا النظام الفصل في طلبات التسليم على مستوى السلطة التنفيذية، إذ يحال طلب التسليم من وزارة الخارجية إلى وزارة العدل التي تبت في الطلب قبولا أو رفضا والتي ترد به إلى وزارة الخارجية لتبليغه للمثل الدبلوماسي للدولة طالبة التسليم ويبرر أنصار هذا النظام بأن إناطة مهمة الفصل في طلب التسليم إلى السلطة التنفيذية كونه يعتبر من أعمال السيادة، كما أنه قد يثير مسائل سياسية تكون السلطة التنفيذية كفيلة بمعالجتها.

رغم ما يتميز به هذا النظام من بساطة الإجراءات، إذ يكفي لدراسة ملف التسليم التأكد من مطابقة الهوية الواردة في الطلب مع الشخص الموقوف قيد التسليم وأن الجريمة المتابع بها من الجرائم القابلة للتسليم.

إلا أنه يعاب على هذا النظام أنه لا يوفر للشخص المسلم الضمانات القانونية الكافية إذ يسلم الشخص دون أخذ رأيه أو الاعتراض على قرار التسليم، كما أن الإجراءات القانونية المتخذة من السلطة التنفيذية قد تتأثر بالاعتبارات السياسية مما يشوبها عيب الدقة وبالتالي فقد تؤدي إلى خلاف ما يقتضيه التسليم.

التسليم القضائي: يقوم هذا النظام على أساس احترام حقوق الأفراد وصيانة حرياتهم، لذا تعتبر السلطة القضائية هي الجهة الوحيدة المختصة بإصدار قرار التسليم، ولا دخل للنيابة العامة في إصدار هذا القرار وإنما يقتصر عملها أو دورها على تلقي طلب التسليم من الجهة المختصة وتعد أوراق الموضوع للعرض على المحكمة المختصة لتتولى الأخيرة عملية إصدار القرار النهائي حول هذا الطلب.

أن الدول التي تأخذ بهذا النظام تختلف في النظر في طلبات التسليم، ففي فرنسا مثلا: يكتفي القضاء بمراقبة وجود الوثائق كالأمر بالقبض والتحقق من هوية الشخص وكذا تطابق النصوص القانونية مع الوثائق المتابع بها.

في حين في الدول الأنجلوسكسونية التي تأخذ بهذا النظام ترى أنه يجب أن تكون الأدلة المقدمة كافية لإدانة الشخص المطلوب تسليمه، يقصد بكفاية الأدلة هو ثبوت الجريمة ظاهريا مما يبعث

في المحكمة بأن الشخص المطلوب تسليمه قد ارتكب فعلا الجريمة المطلوب لأجلها.

يرجح اتجاه الدول الأنجلوسكسونية لضرورة توفر أدلة الاتهام لقبول التسليم يعود لعدم ثقة هذه الدول بالقضاء الأجنبي، لذا لا يكفي صدور أحكام منها أو أوامر بالقبض، بل يشترط كفاية أدلة الاتهام حتى يقبل التسليم كونها تجيز تسليم رعاياها بعد التأكد من ثبوت الجريمة وتوفر أدلتها يأخذ المشرع الجزائري بالنظام القضائي للفصل في طلب التسليم طبقا لما جاء في نص المواد من 702 إلى 709، فقبل النظر في طلب التسليم فإنه يكون قد فحص من قبل وزير الخارجية أولا ثم من طرف وزير العدل، ليحال الملف على القضاء، ويستجوب المقبوض عليه من النائب العام لدى المحكمة العليا ويحرر محضر بذلك خلال 24 ساعة ترفع المحاضر والمستندات إلى الغرفة الجنائية للمحكمة العليا وتحدد له جلسة في أجل أقصاه 08 أيام تبدأ من تاريخ تبليغ المستندات كما يجوز أن تمدد هذه المدة إلى 08 أيام إضافية إذا ما طلب ذلك الشخص المطلوب أو النيابة العامة وللشخص المطلوب أن يستعين بمحام معتمد لدى المحكمة العليا للدفاع عنه كما تجري المحاكمة في جلسة علنية مالم يتقرر خلاف ذلك، بناءا على طلب النيابة العامة أو طلب الشخص المطلوب تسليمه.

إذا تنازل الشخص المطلوب تسليمه عن تلك الإجراءات فإنه يتعين إثبات ذلك الإقرار من طرف المحكمة، عندما تصدر المحكمة رأيها في طلب التسليم في شكل قرار بالرفض لعدم توفر الشروط القانونية فإنه يشترط أن يكون قرارها مسبب والذي يكون نهائيا وملزم للسلطة التنفيذية أما إذا أصدرت قرار بقبول التسليم أو بإقرار المطلوب تسليمه بتنازله عن الإجراءات فإنه يعرض على وزير العدل الذي يوقع ذلك على شكل مرسوم الإذن بالتسليم إلا أن سريان صحة هذا المرسوم تنقضي بعد شهر من تاريخ تبليغه للدولة طالبة التسليم ولا يجوز المطالبة به لنفس السبب.

إن القضاء عند فحصه لطلب التسليم فهو يراقب مدى تطابق هوية الفاعل مع هوية الشخص المطلوب تسليمه وكذا مدى صحة المتابعة في الوقائع المطلوب التسليم لأجلها مع نصوص الدولة طالبة التسليم وأن مراقبة كفاية الأدلة من عدمه غير وارد كون المشرع لم يشترط أن تقدم أدلة الإثبات أو ما يفيد وجود أدلة من شأنها تؤدي إلى الإدانة بل اكتفى إلى تقديم إلى ما يفيد الإحالة بهذه الوقائع وبهذا يكون قد نهج المذهب الفرنسي[1].

[1]– **جمال ماهر**، مرجع سابق، ص22.

ب- مصادر نظام تسليم المجرمين:

فيما يتعلق بمصادر هذا النظام فهي ليست واحدة في كافة التشريعات وإنما تختلف باختلاف الظروف التشريعية لكل دولة، تنقسم مصادر نظام التسليم في الجزائر إلى :

- الدستور : ينص الدستور الجزائري على مبدأ جواز تسليم أي شخص بناءا على قانون تسليم المجرمين وتطبيقا له المادتان 82 و83 من القانون رقم 16-01 المتضمن التعديل الدستوري[1] عدم إمكانية التسليم أو طرد لاجئ سياسي يتمتع قانونا بحق اللجوء.

- الاتفاقيات الدولية وهي اتفاقيات دولية تتضمن أحكاما متصلة بتسليم المجرمين دون أن تكون بحد ذاتها اتفاقيات تسليم[2]،عقدت الجزائر منذ استقلالها اتفاقيات ثنائية[3] ودولية للتعاون القضائي وتسليم المجرمين[4].

تفضل الجزائر الاتفاقيات الثنائية غير أنّ ذلك لم يمنعها من الانضمام إلى الاتفاقيات الدولية الإقليمية المتعددة, وهذا لتكريس مبدأ التعاون الدولي وتنمية العلاقات الودية بين الدول على أساس المساواة والمصلحة المتبادلة وعدم التدخل في الشؤون الداخلية التي ينص عليه الدستور في مادته 31، وقد أعطت لنصوص الاتفاقيات الدولية مكانة تسمو على القانون الداخلي من حيث التطبيق وهذا ما تبينه المادة 694 من قانون الإجراءات الجزائية التي تنص على أنه يكون التسليم بناءا

---

[1]- الدستور الجزائري 2016، سالف الذكر.

[2] - من الأمثلة على هذا النوع من الاتفاقيات: اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، السالفة الذكر.

[3] - من الأمثلة على هذه الاتفاقيات، **اتفاقية التعاون القانوني والقضائي في المجال الجزائي** بين حكومة الجمهوريّة الجزائريّة الديمقراطية الشّعبية وحكومة دولة الكويت الموقّعة بالجزائر بتاريخ 12أكتوبر 2010، صادقت عليها الجزائر بموجب مرسوم رئاسيّ رقم 15-255 مؤرّخ في 21 ذي الحجة عام 1436الموافق 5 أكتوبر 2015، الجريدة الرسمية للجمهورية الجزائرية، عدد 53 بتاريخ 8 أكتوبر 2015.

اتفاقية التعاون القضائي بين الجمهورية الجزائرية الديمقراطية الشعبية وجمهورية تركيا الموقعة بالجزائر بتاريخ 14 مايو 1989، صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 2000-370 ممضي في 16 نوفمبر2000، يتضمن التصديق عليها، الجريدة الرسمية للجمهورية الجزائرية، عدد 69 بتاريخ 21 نوفمبر2000.

والاتفاقية المتعلقة بتسليم المجرمين والتعاون القضائي في المسائل الجنائية الموقعة في بروكسيل في 12 يونيو 1970 بين الجمهورية الجزائرية الديموقراطية الشعبية والمملكة البلجيكية، صادقت عليها الجزائر بموجب امر رقم 70-61 مؤرخ في 8 شعبان 1390الموافق ل 8 أكتوبر 1970، الجريدة الرسمية للجمهورية الجزائرية، عدد 92 بتاريخ 3 نوفمبر 1970.

[4] - Convention européenne d'extradition Paris, 13.XII.1957, in ; https://rm.coe.int/168006459c. consulté le: 03/04/2016.

على قانون الإجراءات الجزائية مالم تنص الاتفاقيات الدولية على خلاف ذلك.

والاتفاقيات الدولية التي عقدتها الجزائر تشبه إلى حد كبير الاتفاقيات الأوروبية وتأخذ بالمبادئ الأساسية الواردة في الاتفاقيات النموذجية لتسليم المجرمين التي أقرتها الجمعية العامة للأمم المتحدة[1].

– التشريع الداخلي :أما الأحكام المنظمة لتسليم المجرمين ,فإنها وردت في قانون الإجراءات الجزائية, حيث أفرد لها المشرع باب كامل يحتوي على 33 مادة، وهو الباب الأول للكتاب السابع ,الخاص بالعلاقات مع السلطات القضائية الأجنبية.

– العرف الدولي: الذي يطبق في حالة عدم وجود اتفاقيات أو قوانين داخلية[2].

ج– شروط وإجراءات تسليم المجرمين

هناك شروط لتسليم المجرمين لا بد من وجودها وإجراءات معينة لا يتم التسليم بدونها وذلك على النحو التالي:

1–شروط التسليم:

أهمية شروط التسليم تكمن 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 البت في قرار التسليم، وتكاد تتفق هذه الشروط في جميع حالات التسليم من حيث العناصر، أما من حيث الموضوع فهي محل خلاف بين الدول وذلك بحسب حاجتها للتسليم، واعتبارات المصالح الدولية التي تراعيها كل دولة[3]، وهي كالتالي:

– التجريم المزدوج: ويقصد به أن يكون الفعل المطلوب التسليم من أجله مجرّما في تشريع الدولة طالبة التسليم، وكذلك في تشريع الدولة المطلوب إليها التسليم. ان المشرع الجزائري قد أخذ

---

[1]–Traité type d'extradition, A/RES/45/116, 68ème séance plénière 14 décembre 1990 , in ; https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/567/63/IMG/NR056763.pdf?OpenElement. consulté le: 15/05/2016.

[2] – **أسامة بن نائل المحيسن، محمد بن درويش الشيدي،** القوانين المكملة، مجمع البحوث والدراسات بأكاديمية السلطان قابوس لعلوم الشرطة، مسقط، 2002، ص 41.

[3] – **عبد الفتاح محمد سراج،** النظرية العامة لتسليم المجرمين، دار النهضة العربية، القاهرة، 2003، ص 209.

بضرورة توفر شرط ازدواج التجريم إلا أنه لم يغالي في هذا الشرط، كأن يشترط تطابق الوصف والتسمية, بل اكتفى في بأن تكون الأفعال المطلوب بشأنها التسليم تشكل جناية أو جنحة في قانون الدولة طالبة التسليم وبالمقابل يعاقب عنها التشريع الجزائري[1] والمطلوب هنا أن يكون الفعل مجرّما أيا كانت الصورة التشريعية المعاقب عليها فلا عبرة للوصف أو التكيف القانوني الذي يطلق على الفعل عند تقرير توافر هذه الشروط والمعاقبة عليه، فقد تختلف تشريعات الدول في التكيف القانوني الذي توصف فيه الجريمة فمثلا لو كان الفعل معاقبا عليه في تشريع الدولة الطالبة التسليم تحت مسمى جريمة توظيف الأموال، بينما كان الفعل نفسه معاقبا عليه تحت مسمى جريمة النصب والاحتيال في الدولة المطلوب منها التسليم، فإن ذلك لا يمنع من توافر شرط ثنائية التجريم أو ازدواجيته[2].

ان شرط التجريم المزدوج يجد أساسه في أن الدولة طالبة التسليم تبتغي من وراء طلبها محاكمة من نسب إليه ارتكاب السلوك الإجرامي أو تنفيذ العقوبة المحكوم بها عليه، وهذا يفترض بداهة أن السلوك مجرّم في تشريعها، حيث أنه إذا لم يكن مجرّما فلا يتصور وجود دعوى عمومية أو ملاحقة جزائية ضد الشخص المتهم كما لا يتصور قيام حكم جزائي يقضي بعقوبة عليه هذا من ناحية، ومن ناحية أخرى لا يجوز مطالبة الدولة المطلوب إليها التسليم بإيقاع عقوبة على ارتكاب سلوك ما هو في الأساس غير مجّرم وفقا لقانونها[3].

أشهر الحالات التي وقعت في التسعينيات الهجوم الذي شنه شاب روسي على مصرف سيتي بنك، باستخدام حاسوبه الموجود في روسيا، نجح المتهم في أن يخترق دون إذن وحدات خدمة حواسيب المصرف في الولايات المتحدة، وقام بتجنيد عدد من المتواطئين لفتح حسابات مصرفية في شتى أنحاء العالم، ثم أصدر تعليمات إلى حاسوب سيتي بنك بتحويل أموالا إلى تلك الحسابات، وعند اكتشاف المخطط وتحديد هوية المتهم، صدر بحقه أمر اعتقال من محكمة

---

[1] – المادة 697 من القانون الإجراءات الجزائية الجزائري، سالف الذكر، التي تشترط في التسليم أن يكون:

– الشخص متابع بوقائع تحمل وصف جناية أو جنحة وعليه فإنه لا يجوز التسليم إذا كانت الجريمة ذات وصف مخالفة.

– أن تكون العقوبة المراد تنفيذها والمحكوم بها تساوي أو تجاوز شهرين حبس.

[2] – **سراج الدين محمد الروبي**، مرجع سابق، ص 53.

[3] – **أسامة بن نائل المحيسن، محمد بن درويش الشيدي**، مرجع سابق، ص 47.

اتحادية بالولايات المتحدة، ولم تكن هناك معاهدة لتسليم المجرمين في ذلك الوقت بين روسيا والولايات المتحدة، لكن المتهم ارتكب خطأً بزيارته إنجلترا لحضور معرض للحواسيب، وقد اضطرت السلطات البريطانية إلى التعاون في تسليمه لمواجهة التهم الموجهة ضده في الولايات المتحدة، فوفقاً لترتيبات تسليم المجرمين النافذة بين المملكة المتحدة والولايات المتحدة، يمكن لسلطات المملكة المتحدة تقديم المساعدة ما دامت الجريمة موضع الاتهام لها ما يقابلها في قانون المملكة المتحدة. طلب المتهم أن تنظر المحكمة في قانونية توقيفه للطعن في تسليمه، وساق حججاً منها أن أمر تحويل الأموال قد صدر في روسيا حيث توجد لوحة مفاتيح حاسوبه وليس في الولايات المتحدة، وارتأت المحكمة أن الوجود المادي للمتهم في سان بطرسبرغ هو أقل أهمية من كونه باشر عملياته على أقراص ممغنطة موجودة في الولايات المتحدة، وفضلاً عن ذلك فإن الأفعال الموجهة إلى المتهم لها مقابلها الواضح في قانون إساءة استعمال الحواسيب لعام 1990؛ ولو مارس عملياته من المملكة المتحدة بدلاً من روسيا لكان الاختصاص القضائي للمحاكم الإنكليزية، وأخيراً تم تسليم المتهم إلى الولايات المتحدة حيث أدين وسُجن[1].

– الشروط المتعلقة بالأشخاص المطلوب تسليمهم:

عدم جواز تسليم الرعايا: من المبادئ السائدة والمستقر عليها في المجتمع الدولي والتي نصت عليها معظم التشريعات الوطنية والاتفاقيات مبدأ عدم جواز تسليم الرعايا أيا كان نوع الجريمة المرتكبة من قبلهم في أي إقليم خارج دولتهم، إنه يكون في حكم رعايا الدولة الجزائرية كل من يحمل الجنسية الجزائرية أصلية كانت أو عن طريق التجنّس, ويكون هذا الأخير غير قابل للتسليم إذا كان تجنسّه قبل ارتكاب الجريمة ,وهذا ما نصت عليه المادة 698 فقرة أولى من قانون الإجراءات الجزائية الجزائري " لا يقبل التسليم في الحالات التالية: إذا كان الشخص المطلوب تسليمه جزائري الجنسية والعبرة في تقدير هذه الصفة بوقت وقوع الجريمة المطلوب التسليم من أجلها"، فطبقا لهذه المادة يحظر نهائيا تسليم المواطنين ذوي الجنسية الجزائرية إلى أي دولة أجنبية، فإذا ما قام أحد المواطنين بارتكاب جريمة في إحدى الدول ثم فر هاربا إلى وطنه، وقامت تلك الدولة بتقديم طلب لتسليمه لها، ففي هذه الحالة لا يجوز تسليم هذا الشخص كونه يتمتع

[1] –**حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص27.

بالجنسية الجزائرية، وان الجزائر هي الأحق بمحاكمته من الدولة الأخرى، عدم جواز تسليم ممن تمت محاكمتهم عن الجريمة ذاتها المطلوب تسليمهم لأجلها، متى ما كان الشخص المطلوب تسليمه قد سبقت محاكمته عن الجريمة المطلوب تسليمه لأجلها فبرَّأ أو عوقب عنها فإنه لا يجوز تسليمه، ليس هذا فحسب بل إنه أيضا لا يجوز التسليم متى ما كان قيد التحقيق والمحاكمة عن ارتكابه فعلا ما هو ذاته المطلوب تسليمه لأجله، ويعد هذا الشرط من الضمانات الأساسية عند محاكمة الشخص المطلوب تسليمه ويهدف إلى توفير أكبر قدر ممكن من الحماية القضائية للشخص المطلوب تسليمه في الدولة الطالبة، وذلك حتى لا يتعرض هذا الشخص لعقوبة مزدوجة.

ان المادة 698 من قانون الإجراءات الجزائية الجزائري تبين اهتمام المشرع بهذا الشرط والتأكيد عليه بعدم جواز التسليم متى ما كان الشخص المطلوب تسليمه قد سبقت محاكمته عن الجريمة المطلوب تسليمه لأجلها أو كان قيد التحقيق أو المحاكمة بالسلطنة عن هذه الجريمة. كما أن هناك العديد من الاتفاقيات والمعاهدات نصت وأكدت على هذا الشرط كمعاهدة الأمم المتحدة النموذجية لتسليم المجرمين في المادة الثالثة منها، واتفاقية جامعة الدول العربية لتسليم المجرمين في المادة الخامسة منها.

– الشروط المتعلقة بالجريمة المطلوب التسليم لأجلها:

الجرائم التي يجوز التسليم فيها وتلك التي لا يجوز التسليم فيها: تحديد طبيعة الجرائم التي تخضع لنطاق التسليم يعتبر في غاية الأهمية كونه يحدد عما إذا كان يجوز التسليم أو لا، فطبيعة تلك الجرائم هي الدعائم التي تقوم عليها شروط التسليم بصفة أساسية. وتتبع الدول في تحديد الجرائم التي يجوز التسليم فيها ثلاثة اتجاهات هي:

أسلوب الترقيم: يعتمد هذا الأسلوب على تعداد مجموعة من الجرائم وإدراجها في بنود الاتفاقية أو المعاهدة سوءا الثنائية منها أو الجماعية أو في نصوص القانون الداخلي المتعلق بالتسليم أو في قائمة ملحقة بها، لتكون هذه الجرائم دون غيرها من الجرائم الأخرى التي يتم التسليم لأجلها، يعتبر هذا الأسلوب من أقل الأساليب شيوعا وانتشارا بين الدول حيث يؤدي إلى إفلات بعض المجرمين من العقاب متى ما كانت الجريمة غير واردة في القائمة[1].

[1] – **عبد الفتاح محمد سراج**، مرجع سابق، ص 259.

أسلوب الاستبعاد: يعتمد على معيار العقوبة أساسا لها في تحديد الجرائم القابلة للتسليم، ويكفي للقانون الداخلي أو الاتفاقيات الدولية المتعلقة بالتسليم الإشارة إلى الحد الأدنى أو الأقصى للعقوبة المقررة قانونا للجريمة المطلوب بشأنها التسليم[1].

إن المشرع الجزائري اتبع في ما مضى طريقة الترقيم شأنه شأن باقي الدول أما حاليا فإنه انتهج طريقة الاستبعاد وهذا ما تشير إليه أحكام المادة 697 قانون الإجراءات الجزائية الجزائري التي تشترط في التسليم أن يكون :الشخص متابع بوقائع تحمل وصف جناية أو جنحة وعليه فإنه لا يجوز التسليم إذا كانت الجريمة ذات وصف مخالفة، أن تكون العقوبة المراد تنفيذها والمحكوم بها تساوي أو تجاوز شهرين حبس .

الأسلوب المختلط: وهو من الأساليب الشائعة أيضا في تحديد الجرائم التي يجوز التسليم فيها، وهو يحقق فائدتين، فمن جهة يضمن درجة معينة من جسامة الجريمة المعاقب عليها في البلدين ليتم التسليم ووفقا لها، ومن جهة أخرى يضمن خضوع جرائم محددة تمثل خطرا على الدول الأطراف للتسليم دون النظر لدرجة جسامتها أو العقوبة المقررة لها[2].

أخذت اتفاقية بودابست بهذا الأسلوب حيث نصت في المادة 24 منها على أنه « تطبق هذه المادة على عملية تسليم المجرمين فيما بين الدول الأطراف بالنسبة للجرائم المنصوص عليها وفقا للمواد من 2-11[3] بهذه الاتفاقية بشرط أن يعاقب عليها القانون بموجب القوانين بالدولتين المعنيتين طرفي الاتفاقية بالحرمان من الحرية لفترة لا تزيد عن سنة واحدة على الأقل أو بعقوبة أشد ».

- عدم انقضاء الدعوى العمومية أو العقوبة: يقصد بهذا الشرط أن تكون الدعوى العمومية للجريمة التي أتهم بارتكابها الشخص المطلوب تسليمه وكذا العقوبة الصادرة بحقه لا تزال قائمة

---

[1]- **جمال ماهر**، مرجع سابق، ص17.

[2] - Christopher BLAKESLEY , "The law of International extradition : A comparative study" RIDP , 1992 , p401.

[3] - هذه الجرائم هي:

الدخول غير المشروع المادة 2، الاعتراض غير المشروع المادة 3، التدخل في البيانات المادة4، التدخل غير المشروع في المنظومة المادة 5، إساءة استخدام الأجهزة المادة 6، جريمة التزوير المتعلقة بالكمبيوتر المادة 7، جريمة التدليس المتعلقة بالكمبيوتر المادة 8، الجرائم المتعلقة بالأعمال الإباحية وصور الأطفال الفاضحة المادة9، الجرائم الخاصة بالانتهاكات الخاصة بحقوق الطبع والنشر والحقوق المتعلقة بها المادة 10، الشروع والمساعدة والتحريض المادة11.

ولم تسقط أو تنقضي لأي سبب من أسباب الانقضاء القانونية, فعدم تحقق هذا الشرط يفقد التسليم أهميته ويصبح بدون جدوى ما دام الشخص مطلوب لوقائع لن يتابع لأجلها كسبب انقضاء الدعوى العمومية، أو يسلّم بشأن عقوبة سقطت سيفرج عنه حتما بعد التسلي،. وهذا ما أكد عليه المشرّع الجزائري في المادة 698 من قانون الإجراءات الجزائية الجزائري.

2-إجراءات التسليم:

يقصد بإجراءات 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 في مكافحة الجريمة بحيث لا يفلت أي مجرم من العقاب .

تعتبر إجراءات التسليم مجموعة الأعمال القانونية المنصوص عليها في القوانين الداخلية للتسليم وبنود الاتفاقيات والمعاهدات الدولية التي يشترطها التسليم حتى يرتب أثاره صحيحة.

هذه الإجراءات تتقاسمها الدولتان الطالبة والمطالبة، كما وأنها ليست مطلقة بل مقيدة ببعض الالتزامات الدولية أو التعاهدية.

- تقديم الطلب: يعتبر تقديم الطلب لسلطات الدولة المطلوب منها التسليم الخطوة الأولى لإجراءات التسليم

تعبر الدولة الطالبة صراحة عن رغبتها في استلام الشخص المطلوب، فبدونه لا يمكن أن ينشأ الحق في التسليم.

إنّ النصّ على شرط الكتابة في طلب التسليم قد يكون صراحة وقد يستفاد منه إذا تضمنت النصوص الداخلية أو بنود الاتفاقيات عبارة " يجب أن يرفق بطلب التسليم الوثائق"...التي يفهم منها أنه يستوجب في طلب التسليم الشكل الكتابي، غير أن بعض الاتفاقيات في حالات الاستعجال تسمح بأن يكون الطلب بواسطة الفاكس أو الهاتف على أن يعزز بطلب لاحق مكتوب[1].

- إرفاق الطلب بالوثائق : وهي مجموعة الوثائق التي تسهل على الدولة المطلوب منها

[1]- **جمال ماهر**، مرجع سابق، ص 15.

التسليم التعرف على هوية المطلوب تسليمه والقبض عليه بأسرع وقت وأقل جهد، إذ غالبا ما تكون الوثائق المطلوب إرفاقها بالطلب تبيّن الهوية الكاملة للشخص محل الطلب (أوصافه البدنية العلاقات المميزة للشخص، صورته الفوتوغرافية، عاداته الاجتماع)، كما أن هذه الوثائق تدفع الاطمئنان في الدولة المطلوب منها التسليم على جديّة متابعة الشخص المطلوب وسلامة هذه المتابعة من أي تجاوزات للقانون مما يدفع بها إلى الجدية في البحث على الشخص المطلوب تسليمه .بالرجوع إلى نص المادة 702 من قانون الإجراءات الجزائية الجزائري يتضح لنا أن الأوراق والمستندات والوثائق التي تطلب المشرع إرفاقها بالطلب هي:

بيان مفصل عن هوية الشخص المطلوب وأوصافه وإرفاق كل ما من شأنه الإعانة على تحديد شخصيته على وجه الدقة وصورته إن أمكن.

أمر القبض أو الإحضار صادر من سلطة مختصة إذا كان الشخص غير محكوم عليه وصورة من الحكم إذا كان محكوما عليه.

صورة من النصوص القانونية التي تعاقب على الفعل والأدلة التي تثبت مسؤولية الشخص المطلوب.

ان اتجاه المشرع الجزائري في تحديد الطريق الذي يسلكه طلب تسليم المجرمين بين الجزائر وغيرها من الدول واضحا وهو الطريق الديبلوماسي، وهذا ما أقرته المادة 702 ق إ ج ج، يوجه طلب التسليم إلى الحكومة الجزائرية بالطريق الديبلوماسي، وهو الطريق الأكثر شيوعا من حيث الاستعمال إذ تقوم الدولة الطالبة بتنظيم طلب التسليم وتسليمه إلى وزارة العدل الذي ترسله بدورها إلى وزارة الخارجية لتوصله إلى سفارتها أو قنصليتها المتواجدة بالدولة المطلوب منها التسليم كي تبلغه إلى وزارة خارجية تلك الدولة.

سابقا ولفترة طويلة لم تظهر أية أحكام أو معاهدات دولية بشأن تسليم المجرمين أو بشأن الإجراءات الواجب إتباعها من أجل تسليم فارّ من العدالة إلى دولة طالبة بغرض محاكمته أو تنفيذ حكم صادر عليه[1]، وكان تسليم المجرمين إلى حد كبير يعتبر من المسائل التي يحكمها مبدأ المعاملة بالمثل أو حسن المعاملة بين الدول، وكان الرأي السائد عموما هو أنه في ظل غياب

[1]- **CHERIF Bassiouni**, International extradition – us law and practice , New York , Oceana Publications ,I.N.C. Third edition, 1996 , p 32.

معاهدة دولية ملزمة فإنه لا وجود لالتزام دولي بتسليم المجرمين. ومع ذلك كان يوجد اتجاها ينادي بضرورة الاعتراف بوجوب تسليم المجرم أو محاكمته وخصوصا في جرائم دولية معينة[1].

بعد الحرب العالمية الثانية كانت الزيادة في عدد المعاهدات والاتفاقيات خاصة الثنائية منها لتنظيم إجراءات تسليم المجرمين خاصة عند دول القانون العام، حيث تم استخدامها على نطاق واسع.

ظهرت العديد من الاتفاقيات متعددة الأطراف بشأن تسليم المجرمين فهناك على سبيل المثال اتفاقية تبسيط إجراءات تسليم المجرمين بين الدول الأعضاء في الاتحاد الأوربي[2]، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000 والاتفاقية الأوربية لمكافحة الجرائم المعلوماتية 2001.

يوجد نوع أخر من مظاهر التعاون الدولي في مجال تسليم المجرمين يتمثل في الاعتراف المتبادل بأوامر القبض أو الحبس أو التوقيف وبمقتضاه تصدر السلطة المختصة بإحدى الدول أمرا بالقبض أو الحبس أو التوقيف، وتعترف بصلاحيته دولة أخرى أو أكثر ويتعين تنفيذه[3].

الفرع الثاني

التعاون الفني الدولي

أن المظهر الثاني من مظاهر التعاون الدولي في مجال مكافحة الجريمة المعلوماتية هو التعاون الفني الدولي إذ لا يقتصر هذا التعاون الفني الدولي على المساعدة القضائية المتبادلة

---

[1]– **CHERIF Bassiouni**, The need for International accountability, International criminal law,1999, p3.

[2] –Convention relative à la procédure simplifiée d'extradition entre les États membres de l'Union européenne - Rapport explicatif [Journal officiel n° C 375 du 12.12.1996, in ; http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM:l14015a. consulté le : 15/05/2016.

[3] – الأمر الأوربي الخاص بالتوقيف وإجراءات التسليم بين الدول الأعضاء، والذي يعد أول تدبير محدد في ميدان تنفيذ القانون الجنائي ينفذ مبدأ الاعتراف المتبادل في بالقرارات القضائية التي تصدرها أجهزة العدالة الجنائية لدى الدول الأعضاء في الاتحاد، ولقد أعتمد على أساس التوصيات الصادرة من المجلس الأوربي في اجتماعه المنعقد في تامبير فلندا يومي 15–1999/10/16. ووفقا لهذا القرار الأمر ينبغي أن يصبح مبدأ الاعتراف المتبادل هو حجر الأساس في التعاون القضائي في المسائل الجنائية داخل الاتحاد الأوربي.

Recommandations du conseil européen de Tampere,15 et 16 octobre1999, in ; http://www.europarl.europa.eu/summits/tam_fr.htm. consulté le: 15/05/2016.

فحسب، وإنما يشمل كذلك المساعدة التقنية وتبادل الخبرات بين الدول، ذلك أن العنصر البشري سواء على مستوى الأجهزة القضائية أو الأجهزة الأمنية ليس بذات الجاهزية والمستوى لمواجهة الجريمة المعلوماتية، وإنما يختلف من دولة إلى أخرى بحسب تقدم تلك الدولة ورقيها. حيث أن جميع الاتفاقيات الدولية أو الإقليمية ذات الصلة قد دعت صراحة إلى ضرورة وجود تعاون دولي في مجال التدريب ونقل الخبرات فيما بينها[1] ذلك أن التقدم المتواصل في تكنولوجيات المعلومات يفرض على الجهات القضائية والأمنية أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات والإلمام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا ومن ناحية أخرى فإن إعمال القانون في مواجهة الإجرام المعلوماتي يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة في المدونة العقابية التقليدية لما تتسم به هذه الجرائم من حداثة في الأسلوب وسرعة في التنفيذ وسهولة في إخفائها ومحو آثارها، وبالتالي إن ظهور هذه الأنماط الجديدة من الجرائم أصبح يشكل عبئا ثقيلا على عائق الأجهزة القضائية المختصة من قضاة تحقيق وقضاة حكم، وكذا رجال الضبطية القضائية، لأجل ذلك كان لا بد أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والمعرفة. من هذا المنطلق كانت الدعوى إلى ضرورة وجود تعاون امني دولي في مجالات متعددة منها مجال تدريب رجال القضاء والضبطية القضائية للاستفادة من مهارات وتجارب الآخرين من خلال أشخاص أكفاء ومؤهلين وقادرين على نقل هذه التجارب وتلك المهارات بوسائل سهلة ميسرة[2].

أولا: ضرورة التعاون الأمني الدولي

حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدرٍ من الأمن والنظام، تشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم، وتشغل اهتمام الحكومات والمختصين والأفراد على حد سواء. ولقد أثبت الواقع العملي أن الدولة – أي دولة – لا

[1] – المادة 29 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، سالفة الذكر.

[2] – يقصد بالتدريب ليس التدريب التقليدي فحسب، بل يكف أن تتوافر لدى رجال القضاء الخلفية القانونية، ولدى الضبطية القضائية خصائص عمل الشرطي وإنما لا بد من إكسابهم خبرة فنية في مجال الجريمة المعلوماتية، وهذه الأخيرة لا تأت دون تدريب تخصصي يراعي فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب. **سعيداني نعيم**، مرجع سابق ص 166.

تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة. نتيجة للتطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الأنترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بشبكة الأنترنت وهي نوعٌ من الجرائم المعلوماتية، التي باتت تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة[1].

ان تميزها بالعالمية وبكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجزائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالأنترنت وتعميمها[2].

مثلا في جرائم البث والنشر الفيروسي قد يكون مرتكب الهجوم يحمل جنسية دولة ما، ويشن الهجوم الفيروسي من حواسيب موجودة في دولة أخرى، وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة، فمن البديهي أن تقف مشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها، لذا فإن التحقيقات في الجرائم المتصلة بالحاسب الآلي وملاحقتها قضائيا تؤكد على أهمية المساعدة القانونية المتبادلة بين الدول، حيث يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود، لأن جهاز الشرطة في هذه الدولة أو تلك لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابع لها بمعنى آخر أنه متى ما فرّ المجرم خارج حدود الدولة يقف الجهاز الشرطي عاجزا[3].

تعد من أبرز الأمثلة لأهمية التعاون الدولي في مجال مكافحة الإجرام المعلوماتي هي عملية كاتريك Catterick Operation وتتعلق هذه العملية بالابتزاز الذي قامت به شركات القمار عبر الأنترنت في الفترة من مايو إلى أكتوبر 2004 وفي هذه العملية، كان المجرمون يرسلون إلى إحدى الشركات يطلبون منها أموالا، مهددين إياها بأن يشنوا على موقعها "هجمات حجب الخدمة

[1] – مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، سالف الذكر.

[2] – **جميل عبد الباقي الصغير**، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، مرجع سابق، ص 75.

[3] – **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص7.

الموزعة" في حالة امتناعها عن الدفع، وتحدث هذه الهجمات بأن تزور آلاف أو مئات الآلاف من أجهزة الكمبيوتر من جميع أنحاء العالم موقعا معينا في الوقت نفسه، ما يؤدي إلى تدمير الموقع وبعد تنفيذها للهجمات تعرض حوالي 57 شركة في أنحاء العالم، منها 10 شركات بالمملكة المتحدة، تجاوزت خسائرها 30 مليون جنيه إسترليني .وبالإضافة إلى الأثر الذي تتعرض له المواقع نفسها، فإن مقدار البيانات التي يتم توجيهها عبر قسم من الوصلات الرئيسة لشبكة الأنترنت يكاد يتسبب في تدمير هذه المواقع. ومع مباشرة التحقيقات لكل من المملكة المتحدة والولايات المتحدة باعتبارهما الأكثر تضرراً وقد قادتهم التحريات التي تمت بين أجهزة الشرطة في البلدين إلى لاتفيا، حيث قامت قوات الشرطة لديها بعملية مراقبة سرية أسفرت عن إلقاء القبض على 10 أشخاص يُشتَبه في تورطهم حيث تم تحديد موقع جهاز كمبيوتر تم اختراقه في مدينة بالاكوفو في روسيا، بدأت الشرطة الروسية على إثره بإجراء تحقيق بمفردها تحول بعد ذلك إلى تحقيق فعال مشترك؛ تم توقيف عدد من الأشخاص، وضبط عدد من أجهزة الكمبيوتر ووجهت إلى المتهمين تهم الابتزاز ونشر فيروسات علي أجهزة الكمبيوتر، وحُكم عليهم بالسجن ثماني سنوات[1].

أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من وجه العادلة.

يعد التعاون الشرطي الدولي من أهم صور التعاون الفني الدولي في مكافحة الإجرام لاسيما الإجرام المعلوماتي، ويتحقق هذا التعاون من خلال عدة أجهزة من أهمها:

- المنظمة الدولية للشرطة الجنائية" الإنتربول":

البدايات الأولية للتعاون الدولي الشرطي ترجع إلى عام 1904 عندما تم إبرام الاتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض بتاريخ 1904/5/18 والتي نصت في مادتها الأولى على "" تتعهد كل الحكومات المتعاقدة بإنشاء أو تعين سلطة لجمع المعلومات الخاصة باستخدام النساء

[1]– مثال مشار اليه عند: **مراد ماموش**، "الجهود الدولية لمكافحة الاجرام السبراني"، مجلة القانون والاعمال، تصدر عن كلية الحقوق، جامعة غرداية، ص 02، محمول من الموقع الإلكتروني التالي: http://www.droitetentreprise.com تم الاطلاع عليه يوم: 2018/02/01.

والفتيات لغرض الدعارة في الخارج، ولهذه السلطة الحق في أن تخاطب مباشرة الإدارة المماثلة لها في كل الدول الأطراف المتعاقدة.

لم تمر سنة على إبرام هذه الاتفاقية إلا وكانت سبع دول من الدول المتعاقدة تنشي مثل تلك الأجهزة وتتبادل من خلالها المعلومات والبيانات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج من أجل القضاء على هذه الجريمة في أقاليمها[1].

بعد ذلك أخذ التعاون الشرطي الدولي يأخذ صورة المؤتمرات الدولية[2]: أولها وأسبقها تاريخيا كان مؤتمر موناكو14-1914/4/18 والذي ضم رجال الشرطة والقضاء والقانون من 14 دولة، وذلك لمناقشة ووضع أسس التعاون الدولي في بعض المسائل الشرطية، خاصة ما يتعلق بمدي إمكانية إنشاء مكتب دولي للتسجيل الجنائي وتنسيق إجراءات تسليم المجرمين، إلا أنه ونتيجة لقيام الحرب العالمية الأولى لم يحقق المؤتمر أي نتائج عملية تذكر.

بعد انتهاء الحرب العالمية الأولي وتحديدا عام 1919 حاول الكولونيل "فان هوتين" أحد ضباط الشرطة الهولندية إحياء فكرة التعاون الدولي الشرطي وذلك بالدعوة لعقد مؤتمر دولي لمناقشة هذا الموضوع، غير أنه لم يوفق في مسعاه.

نجح الدكتور "جوهانو سويرا" في سنة1923 مدير شرطة فينا في عقد مؤتمر دولي يعد الثاني على المستوى الدولي للشرطة الجنائية وذلك في الفترة 3 – 1923/9/7، ضم مندوبي تسعة عشر دولة[3]، وتمخض عنه ولادة اللجنة الدولية للشرطة الجنائية(ICPO) يكون مقرها فينا، وتعمل على التنسيق بين أجهزة الشرطة من أجل التعاون في مكافحة الجريمة.

إلا أنه مع اندلاع الحرب العالمية الثانية توقفت اللجنة عن أعمالها، حتى وضعت الحرب أوزارها عام 1946، عقد في بروكسل ببلجيكا في الفترة6-1946/6/9 مؤتمر دولي بهدف إحياء مبادئ التعاون الأمني ووضعها موضع التنفيذ بدعوة من المفتش العام للشرطة

---

[1] – **H FERAUD , E SCHLANILZ**, "La coopération policière internationale", RIDP, 1974, p477-478.

[2] – راجع كل عن: **محمد منصور الصاوي**، أحكام القانون الدولي في مجال مكافحة الجرائم الدولية للمخدرات، دار المطبوعات الجامعية، الإسكندرية، 1980، ص648 . **علاء الدين شحاته**، التعاون الدولي لمكافحة الجريمة، إيتراك للنشر والتوزيع، القاهرة، 2000، ص 174-176.

[3] – **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص7.

البلجيكية(Louvage)، وانتهى الاجتماع إلى إحياء اللجنة الدولية للشرطة الجنائية(ICPO) ونقل مقرها إلى باريس بفرنسا، وغيّر اسمها ليصبح المنظمة الدولية للشرطة الجنائية(Interpol) وحتى كتابة هذه السطور تضم في عضويتها 182 عضوا[1].

تهدف هذه المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعّال في مكافحة الجريمة، من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة إليها[2]. وتتبادلها فيما بينها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف[3]، ومدها بالمعلومات المتوفرة لديها على إقليمها وخاصة بالنسبة للجرائم المتشعبة في عدة دول ومنها جرائم الأنترنت، ومن الأمثلة على دور الإنتربول في ما يتعلق بالجرائم المتعلقة بالأنترنت، ما حصل في الجمهورية اللبنانية عندما تم توقيف أحد الطلبة الجامعين من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصرة دون العشرة أعوام من موقعه على شبكة الأنترنت، وذلك أثر تلقي النيابة اللبنانية برقية من الإنتربول في ألمانيا بهذا الخصوص[4].

مرت جهود المنظمة في هذا المجال بمراحل عديدة، إلى أن تم إنشاء عدة مراكز اتصالات إقليمية في كل من طوكيو، نيوزيلندا، نيروبي، أذربيجان، بيونس أيرس لتسهيل مرور الرسائل، ويضاف إلى ذلك مكتب إقليمي فرعي في بانكوك. ونظرا لتنوع أنظمة الدول المختلفة، فقد كان هناك خيارين لأنظمة الاتصال[5]، داخل هذه الشبكة، أولهما هو نموذج يخصص للدول المركزية وتجرى الاتصالات العالمية للشرطة فيها من خلال الجمعية العامة واللجنة التنفيذية بواسطة السكرتارية العامة، والثاني للدول اللامركزية وتجري الاتصالات فيه مباشرة بين أجهزة الشرطة في الدول المختلفة.

يعد من أهم صور التعاون الأمني في مجال مكافحة جرائم المعلوماتية تبادل المعاونة

---

1 – http://www.interpol.com/public/Icpo/Members/default.asb.consulté le: 23/12/2012

2 – **Anderson MALCOM**, " Policing the world: Interpol the Politics of International Police Co-Operation" , Clarendon press.Oxford, 1989, p 168-185.

3 – هذا يؤكد أن هذه المنظمة ليست سلطة دولية عليا فوق الدول الأعضاء فالتعاون الشرطي في إطار هذه المنظمة يحكمه مبدأ احترام السيادة الوطنية للدول الأعضاء.

4 – **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص 9.

5 -**Anderson MALCOM**, op.cit , p 169.

لمواجهة الكوارث والأزمات والمواقف الحرجة[1]، لاسيما وأن أجهزة العدالة الجزائية ليست بنفس المستوي والجاهزية في جميع الدول وإنما هناك تفاوت فيما بينها فبعض الدول متقدمة تقنيا وتكنولوجيا ولها صيت كبير في مواجهة الجرائم المعلوماتية ومنها الجرائم المتعلقة الأنترنت تشريعيا وفنيا، والبعض الآخر تفتقد ذلك، من هنا كان لابد من التعاون بين الدول.

كما تقوم الشرطة الدولية ببعض العمليات الشرطية والأمنية المشتركة كتعقب مجرمي المعلوماتية والأدلة الإلكترونية، بوضع استراتيجيات جديدة بالتعاون مع هيئة الأمم المتحدة، كلها أمور تستدعي القيام ببعض العمليات الفنية والأمنية المشروعة[2].

- اليوروبول:

المجلس الأوربي النشاء شرطة أوربية وهي جهاز اليوربول، بوصفه مكتبا مركزيا للشرطة الجنائية في دول الاتحاد الأوربي لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة ولملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم المتعلقة بالأنترنت [3]. وفى قمة لكسمبورج عام 1991 بموجب اتفاقية ماسترتيخت تم تأسيس الجهاز المذكور، ووقعت اتفاقية اليوروبول في بروكسل بتاريخ 26 يونيو 1995 من قبل سفراء 15 دولة عضو في الاتحاد الأوروبي من اجل ضمان اقصى درجات التعاون والمشاركة وتبادل المعلومات في كافة المجالات، وتسهيل الاتصال فيما بين الدول الأعضاء، بوضع نقاط اتصال وتكليف منفد واحد لكل الخدمات المتعلقة بالكفاح ضد الجريمة المنظمة، يكون تحت تصرف تلك الدول متى تعلقت التحقيقات بهذه الجريمة [2].

فوض الاتحاد الأوروبي جهاز اليوروبول حق مشاركة السلطات الوطنية في سياستها المقررة، لمكافحة الجريمة المنظمة، وإعداد لإجراءات في مجال التحقيقات "الشرطية، الجمركية،

---

[1] – فقد تتعرض كافة دول العالم لاحتمالات وقوع كوارث ضخمة وأحداث جسام مفاجئة بشكل لا يمكن توقعه، أو يستحيل التنبؤ بتوقيت حدوثه، أو يصعب معه مواجهته بالإمكانيات القومية للدولة المنكوبة بمفردها ومع وقع مثل هذه الكوارث أو الأزمات أو المواقف الحرجة غالبا ما يكون عنصر الوقت من الأمور الحاسمة في المواجهة، الأمر الذي يحتاج إلى تكثيف خاص للجهود والخبرات والإمكانيات بشكل يصعب تحقيقه إلا بتضافر الجهود الدولية.

[2] – **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص10.

[3] – **جميل عبد الباقي الصغير**، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، مرجع سابق، ص 79.

القضائية، للعمل مع سلطات تلك الدول كوحدة متكاملة[1].

يوروبول هي وكالة تطبيق القانون الأوربية، وظيفتها حفظ الأمن في عن طريق تقديم الدعم للدول الأعضاء في الاتحاد الأوربي في مجالات مكافحة الجرائم الدولية الكبيرة خاصة الجرائم المعلوماتية، مقرها الرئيسي الكائن في لاهاي في هولندا، وهي تعمل بشكل وثيق مع أجهزة أمن دول الاتحاد الأوربي ودول من خارج الاتحاد كأستراليا وكندا والولايات المتحدة الأمريكية والنرويج. ستفيد أجهزة الأمن المستقلة لدول الاتحاد بدورها من خدمات الوكالة الاستخباراتية لتجنب وقوع الجرائم وللتحقيق فيها في حال وقوعها ولتعقب وإلقاء القبض على مرتكبيها.

- جهاز الاوروجست: تم إنشاءه في 2002/02/28 من قبل مجلس الاتحاد الأوربي، كجهاز يساعد على التعاون القضائي والشرطي في مواجهة الجرائم الخطيرة. ويتمثل أهم نشاطاته في تحسين التنسيق والتعاون بين السلطات القضائية المختصة للدول الأطراف، تبادل المعطيات بين دول الأعضاء الاتحاد الأوربي، كما يمكنه أن يطلب من الوكلاء ذوي الاختصاص الوطني إجراء تحقيقات أو ملاحقات أو التبليغ عن الجرائم إلى الجهات المختصة للدول الأطراف [2].

ولايزال الاتحاد الأوروبي يوصي بتوسيع نطاق اختصاص اليوروبول، وخلق نقاط اتصال بينه وبين دول العالم الثالث لضمان إقرار سياسة كفاحية موحدة ضد مختلف أشكال الجريمة المنظمة بما فيها الجريمة المعلوماتية، وبينه وبين المنظمات الدولية التي تمارس اختصاصات اليوربول نفسها، ولغرض تنسيق عمليات الأجهزة الشرطية وتوثيق تبادل المعلومات والاتصال المباشر والمستمر لتطوير التعاون القضائي أنشئ مركز الشرطة القضائية عام 1995 : le centre du renseignement et d’analyse du crime organisée لأجل إرسال واستقبال المعلومات المتعلقة بالجريمة محل الذكر والمعطيات الصادرة بالخصوص، بما يكفل سرعة ومرونة التعاون ويساعد الجهاز على وضع خريطة لمكافحة الإجرام[3].

---

[1] – **أبو المعالي محمد عيسى**، "الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية"، ورقة عمل المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، المنعقد في الفترة بين 28-29 أكتوبر 2009، ص 11.

[2] – http://www.finances-gouv.fr

[3] – **أبو المعالي محمد عيسى**، مرجع سابق، ص12.

- المجموعة الثمانية الاقتصادية G8: لا يقل دورها عن دور الأنتربول في مواجهة هذا النوع المستحدث من الإجرام على مستوى الدولي، حيث قامت بإعداد ملتقى دولي في نهاية نوفمبر 2000 في طوكيو لتكوين قوة دولية أطلق عليها «The Digital Opportunity Task Forced» تتمثل مهامها في تحقيق أمن تكنولوجيا المعلومات[1].
- منظمة التعاون الاقتصادي والتنمية (OECD)

تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي وتناغم التطور الاقتصادي مع التنمية الاجتماعية، بدأت هذه المنظمة الاهتمام بالجريمة المعلوماتية منذ عام 1978، حيث وضعت مجموعة من الأدلة وقواعد إرشادية تتصل بتقنية المعلومات، ويعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام بها. فأصدرت سنة 1983 تقريراً بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية، حيث استعرض التقرير السياسة الجنائية القائمة والمقترحات الخاصة في عدد من الدول الأعضاء، وتضمن التقرير الحد الأدنى من لأفعال سوء استخدام الحاسوب والتي على الدول تجريمها وتشمل هذه الأفعال:

- الاستخدام أو الدخول إلى نظام ومصادر الحاسب على نحو غير مصرح به
- الإفشاء غير مصرح به للمعلومات المعالجة آلياً والنسخ والإتلاف أو التخريب ما يحتويه من بيانات وبرامج والإعاقة غير المشروعة للوصول لمصادر الحاسب من منع أو تعطيل استخدام الحاسب أو برامجه أو البيانات المخزنة داخله.

وضعت المنظمة عام 1992 توصيات وإرشادات خاصة بأنظمة المعلومات وأوصت بضرورة أن تعطي التشريعات الجزائية للدول الأعضاء مبادئ عامة تتمثل في:

- حدود التجميع: يتعين فرض قيود على تجميع البيانات.
- نوعية البيانات: حيث تنص على أن تتعلق البيانات بالغاية والغرض الذي سوف تستخدم من أجله.

[1] – **عائشة بن قارة مصطفى**، مرجع سابق، ص167.

- تعيين الغرض: بحيث يكون الغرض الذي تستخدم فيه البيانات الشخصية محصورة ومحددة سلفا.
- حدود الاستخدام: يقتضي الالتزام بعدم إفشاء البيانات الشخصية ونشرها لغير المصرح لهم بذلك.
- الوقاية الأمنية: ضرورة اتخاذ تدابير وإجراءات أمنية ملائمة وحازمة في إحاطة البيانات.
- الانفتاح: أن تكون السياسة العامة للتطوير والخطط والتطبيقات معلنة فيما يتعلق بالبيانات ذات الطبيعة الشخصية.
- المشاركة الفردية: حق الأشخاص المعنية في الوصول والتعرف على البيانات التي تخصهم فضلاً عن رقابة مدى صحتها.
- المسائلة والمحاسبة : التي تقتضي محاسبة الأشخاص والجهات المرخص لهم الوصول والاطلاع على البيانات والتعامل معها في حالة تجاوز أي من الإجراءات التي تكفل حماية البيانات ذات الصفة الخاصة[1].

- أما على المستوى العربي، يعد المكتب العربي للشرطة الجنائية احد المكاتب الخمسة للأمانة العامة لمجلس الوزراء الداخلية العرب، وجد من اجل تأمين وتنمية التعاون بين أجهزة الشرطة للدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة[2]. بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء.

أصبح التعاون الأمني والقضائي المقنن اليوم إحدى أهم مقومات الاستراتيجيات القومية والإقليمية التي تأخذ جانباً كبيراً من اهتمام الأسرة الدولية، سعيا إلى خلق هيئة تعمل دون حدود وطنية، لمكافحة الجرائم الخطيرة، وتتمتع بالمرونة وتتجاوز البيروقراطية الإدارية، وتوحد الإجراءات العملية للأجهزة التنفيذية، وتعمل على تقارب أعضائه، الأمر الذي تفتقر إلى مثله المنتظمات الإقليمية لدول العالم الثالث.

---

[1] – **مراد ماموش**، مرجع سابق، ص 07.

[2] –**عمر محمد بن يونس**، الدليل الرقمي، مرجع سابق، ص2.

يتوجب على دول العالم الثالث خاصة العربية تفهم أن عملية التعاون لا تمس احترام سيادة الدولة التي ستجري على إقليمها عملية متابعة الأشخاص المشتبه فيهم أو الأموال المستهدفة على ضوء ذلك؛ بل يجب عليها اتخاذ تدابير عملية تكفل تعاون أجهزتها الأمنية لرصد وكشف عمليات النقل المادي للنقود، وإنشاء مراكز لجمع البيانات المشتركة، فقاعدة البيانات المدققة المتاحة للمختصين تسهل تعاون سلطات تنفيذ القانون في تبادل المعطيات لتيسير الكشف عن الأشخاص الفارين من العدالة، هذا بالإضافة إلي ضرورة كشف الأساليب والوسائل التي تلجا إليها المنظمات الإجرامية، ولتحقيق الأغراض المقررة، يجب:

– مراقبة التزام الدول الأطراف بالتنفيذ، والترتيبات والإجراءات المؤسسية المقررة بموجب الاتفاقية، وتطوير آلياتها بما يتوافق وتطور المعارف العلمية والتكنولوجية .

– تيسير تبادل المعلومات لمواجهة الجريمة المنظمة عبر الوطنية بصفة عامة، والاجرام المعلوماتي بصفة خاصة.

– تقييم مدى التقدم في تحقيق أهداف الاتفاقية وإصدار التوصيات بشأن مسائل ضرورية لتنفيذ الاتفاقية ولحشد الموارد المالية[1].

ثانيا: التعاون الدولي الأمني في مجال تدريب رجال العدالة الجزائية

التقدم المتواصل في تكنولوجيا الحاسب الآلي والأنترنت يفرض على جهات إنفاذ القانون أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات، والإلمام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا ومواجهتها هذا من ناحية، ومن ناحية أخرى فإن إعمال القانون في مواجهة الجرائم المعلوماتية يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة في المدونة العقابية التقليدية، لما تتسم به هذه الجرائم من حداثة في الأسلوب وسرعة في التنفيذ وسهولة في إخفائها والقدرة على محو آثارها. حيث أثبتت الوقائع العملية أن هناك جرائم متعلقة بالحاسب الآلي وشبكة الأنترنت قد ارتكبت على مرأى ومسمع من رجال الشرطة، بل قام بعض رجال الشرطة بتقديم يد المساعدة لمرتكبي هذه الجرائم دون قصد وعن جهل، أو على سبيل واجبات المهنة التي يلزمهم بها هذا القانون. مثلما حدث عندما طلبت

[1]– **أبو المعالي محمد عيسى**، مرجع سابق، ص16.

إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي لتتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة، ونتيجة لذلك أتلف ما كان قد سلم من الملفات والبرامج[1]. ان إتلاف الأدلة قد يقع كذلك عن خطأ مشترك بين الخبراء وبين الجهة المجني عليها، فمثلا في تحقيق إحدى الجرائم المعلوماتية والتي تدور وقائعها حول طلب أحد الأشخاص من إحدى الشركات زعم أنه وضع قنبلة منطقية بنظام حاسبها الآلي. تبين أن الشركة وقبل إبلاغ السلطات المختصة كانت قد استدعت خبيرا للتحقق من صحة ذلك وإبطال مفعول القنبلة إن وجدت، وبالفعل نجح الخبير في اكتشاف القنبلة وإزالتها من البرنامج الموضوعة فيه، وعندما تولت الشرطة التحقيق اتضح أنه بإزالة القنبلة أتلفت كل الأدلة على وجودها.

إن ظهور هذه الأنماط الجديدة من الجرائم أصبح يشكل عبئاً ثقيلا على عاتق جميع أجهزة العدالة الجنائية سواء رجال الضبط القضائي أو رجال التحقيق أو المحاكم على مختلف درجاتها، لاسيما وأن متطلبات العدالة وتقتضي أن تتحمل الأجهزة الأمنية الحكومية كامل المسؤولية تجاه اكتشاف كافة الجرائم المعلوماتية وضبط الجناة فيها وتحقيق العدالة في حقهم.

لأجل ذلك كان لابد أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والمعرفة والقدرة على كشف غموض تلك الجرائم والتعرف على مرتكبيها بسرعة ودقة متناهيين. وهذا لن يتحقق إلا بالتدريب[2]، فكفاءة رجال العدالة لمواجهة هذه الظواهر المستحدثة وقدرتهم في التصدي لها لابد أن ترتكز على كيفية تطوير العملية التدريبية والارتقاء بها والنهوض بأساليب تحقيقها لأهدافها، من هذا المنطلق كانت الدعوى إلى وجوب تأهيل القائمين على هذه الأجهزة[3].أنه ما من دولة يمكنها النجاح في مواجهة هذه الأنماط المستحدثة بمفردها دون تعاون وتنسيق مع غيرها من الدول، فكانت الدعوة إلى ضرورة وجود تعاون دولي في مجال تدريب رجال العدالة الجزائية.

---

[1] – **محمد أبو العلا عقيدة**، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، مرجع سابق، ص 24.

[2] – **هشام فريد محمد رستم**، الجرائم المعلوماتية، مرجع سابق، ص 439–440.

[3] – تعرف العملية التدريبية بأنها " مجموع الأنشطة أو العمليات الفرعية التي توجه لعدد من المتدربين لتحقيق أهداف معينة في برنامج تدريبي معين وتحدث الأثر أو الآثار المطلوبة فيه". **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص40.

أ- التدريب وأهميته في مجال مكافحة الجرائم المعلوماتية

التدريب يعد جزءا من عملية التنمية الإدارية وهو يهتم المتدرب وللمنظمة التي ينتسب إليها في آن واحد، سواء أكانت منظمة مدنية أو عسكرية، حكومية بالدرجة الأولي بالكفاءة والفعالية في إنجاز العمل، حرصت الكثير من المنظمات العامة والخاصة على العناية به، باعتباره أحد الأدوات الأساسية لرفع مستوى الأداء وزيادة الكفاية الإنتاجية وإعداد العاملين على اختلاف مستوياتهم للقيام بواجبات أعمالهم والمهام الموكلة إليهم على خير وجه. إضافة إلى تهيئتهم لتحمل المزيد من المسؤوليات من خلال زيادة قدراتهم على مواجهة المهام المعقدة في الحاضر والمستقبل.

لهذا أصبح ينظر إلى التدريب على أنه وسيلة للاستثمار الذي تلجأ إليه المنظمات الإدارية لتحقيق أهدافها باعتباره عنصرا حيويا لا بد منه لبناء الخبرات والمهارات المتجددة[1].

الواقع أن التدريب أصبح يلعب دورا هاما في حياة الإنسان في عصرنا الحاضر، فقد زاد الاهتمام بالتدريب بمختلف جوانبه الفنية والتكتيكية فقد أضح ضرورة للفرد أو خاصة، تعمل في قطاع العدالة أم في غيره، فهو أحد العناصر الأساسية لزيادة كفاءة العنصر البشري ويرفع إنتاجيته ويحقق التنمية بمفهومها الشامل. والهدف من عملية التدريب إدخال وإحداث تعديلات جوهرية على سلوك المتدربين، تبدو آثارها واضحة في سلوكهم لأداء الأعمال التي يكفلون بها كل في مجال تخصصه، بشكل أفضل بعد عملية التدريب لا قبلها.

تبدو أهمية التدريب وضرورته في أنه من ناحية يعد الوسيلة الفعلية والتطبيقية الناجحة والمؤثرة التي تكفل الاستفادة من مهارات وتجارب الآخرين من خلال أشخاص أكفاء مؤهلين وقادرين على نقل هذه التجارب وتلك المهارات بوسائل سهلة ميسرة، كما أنه يعد من ناحية أخرى الوسيلة الملائمة والفعالة لوضع المعارف العلمية موضع التطبيق الفعلي والتعرف على الأخطاء والسلبيات التي يمكن أن يكشف التطبيق العملي للقوانين والأنظمة واللوائح، ووضع الحلول الكفيلة بتجنبها. وتزداد أهمية التدريب في الوقت

[1] - Déclaration D-8 des Nations Unies, Commission pour la prévention du crime et la justice pénale Rapport sur la vingt-quatrième session (5 décembre 2014 et 18-22 mai 2015), in ; https://www.legal-tools.org/doc/609e53/pdf/, consulté le :30/07/2016.

الحاضر نظرا للتطور التكنولوجي الكبير الذي يشهده العالم اليوم[1].

التدريب المقصود هنا ليس التدريب التقليدي فحسب فلا يكفي أن تتوافر لدي رجال العدالة الجزائية الخلفية القانونية أو أركان العمل الشرطي وإنما لا بد من إكسابهم خبرة فنية في مجال الجريمة المعلوماتية، وهذه الخبرة الفنية لا تتأتى دون تدريب تخصصي يراعي فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب[2]، ويلاحظ أنه من الأسهل تدريب متخصص في تكنولوجيا المعلومات وشبكات الاتصال بدلا من تدريب القائمين على تنفيذ القانون كرجال الشرطة أو ممثلي الادعاء العام . يذهب البعض إلى أنه يجب أن تتوافر لدى المتدرب خبرة لا تقل عن خمس سنوات في المجالات ذات العلاقة بتكنولوجيا المعلومات كالبرمجة وتصميم النظم وتحليلها وإدارة الشبكات وعمليات الحاسب الآلي[3]. وبالنسبة للمنهج التدريبي فيجب أن يشتمل على بيان بالمخاطر والتهديدات ونقاط الضعف وأماكن الاختراقات لشبكة المعلومات وأجهزة الحاسب الآلي مع ذكر لمفاهيم معالجة البيانات وتحديد نوعية وأنماط الجرائم المعلوماتية، وبيان لأهم الصفات التي يتميز بها المجرم المعلوماتي، والدوافع وراء ارتكاب الجرائم المعلوماتية[4].

ان منهج التحقيق لا بد أن يشتمل على[5]: إجراءات التحقيق، التخطيط للتحقيق، تجميع المعلومات وتحليلها، أساليب المواجهة والاستجواب، مراجعة النظم الفنية للبيانات، أساليب المعمل الجنائي، إضافة إلى ذلك لا بد إن يشتمل على ما يتعلق بالتفتيش والضبط وكيفية استخدام الحاسب الآلي كأداة للمراجعة والحصول على أدلة الاتهام وما يخص الملاحقة الدولية والتعاون المشترك.

ان التدريب فإنه لا بد وأن يراعى في البرنامج التدريبي نوعه وصفته وما إذا كان رسميا من خلال حلقات دراسية أو حلقات نقاش – ورش العمل– حول هذا النوع المستحدث من الجرائم، وحلقات النقاش التي يمكن أن تثمر أفضل تدريب رسمي هي تلك التي تكفل تفاعل المشاركين،

---

[1] – **محمد السيد عرفة**، تدريب رجال العدالة وأثره في تحقيق العدالة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2005، ص 2.

[2] – **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص42.

[3] – **هشام محمد فريد رستم**، "الجرائم المعلوماتية أصول التحقيق الجنائي الفني"، بحث مقدم لمؤتمر القانون والكمبيوتر والأنترنت، كلية الشريعة والقانون، جامعة العين، دولة الإمارات العربية المتحدة في الفترة 1–3–مايو 2000، ص 496.

[4] – **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص43

[5] – **هشام محمد فريد رستم**، الجرائم المعلوماتية أصول التحقيق الجنائي الفني، مرجع سابق، ص 497.

وتتضمن تحليلا لحالات دراسية وإكساب خبرة عملية في كيفية التعامل مع الحاسب الآلي وكيفية استخدام تقنيات الاتصال بين شبكات الحاسب الآلي، وما يرتبط بها من قواعد بيانات ومعلومات[1]، وقد يكون البرنامج التدريبي غير رسمي من خلال تكليف المتدرب بالعمل مع شخص لدية خبرة في تحقيق الجرائم المعلوماتية، أو التدريب باستخدام أسلوب الفريق والذي تقوم فلسفته على تدريب الفريق أو مجموعة متخصصة في جرائم الحاسب الآلي مرة واحدة بحيث يكون لكل فريق من الفرق مهمة محددة فضلا عن إلمامه بمهام زملائه الآخرين، فطبقا لهذا الأسلوب يتم التركيز على تدريب مجموعة من المتخصصين في مجالات معينة بحيث يلم كل منهم بتخصص الآخرين، ويزداد في نفس الوقت فهما لتخصصه الأصلي[2]، ويتعين هنا على الفريق أن يخوض تجارب عملية بحيث تعرض عليه عينة من الجرائم المعلوماتية التي تم التحقيق فيها، على أن يراعى في هذه العينة التنويع لكي تؤدي دورها في إكساب المشاركين في البرنامج التدريبي الخبرة المطلوبة، وهذا الأمر يتطلب أن يعهد بالتدريب إلى جهات متخصصة تعنى باختيار المدربين ممن تتوافر لديهم الصلاحية العلمية والفنية والصفات الشخصية ليتولوا التدريب في هذا المجال، والذي من شأنه تحقيق نتائج طيبة في عملية التدريب[3]،والعملية التدريبية لا بد وان تكون مستمرة ولا تتوقف عند حد معين، لاسيما وأن الجرائم المعلوماتية ومنها الجرائم المتعلقة بالأنترنت في

---

[1] – **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص42

[2] – يمكن تقسيم الفريق إلى ثلاث مجموعات رئيسية هي :

المجموعة الأولي: مهمتها تنفيذ القانون.

المجموعة الثانية: مهمتها التدقيق والمراجعة الحسابية.

المجموعة الثالثة: مهمتها معالجة البيانات إلكترونيا.

[3] – من الأمثلة على أنماط التدريب والاهتمام به على المستوى العالمي:

في الولايات المتحدة الأمريكية التدريب على تحقيق الجرائم المعلوماتية يتم من خلال دورات متخصصة مدة كل دورة أربعة أسابيع ويتم ذلك بمعرفة أكاديمية مكتب التحقيقات الفيدرالي الأمريكي في كوانتيكو Quantico وفيرجينيا Virginia

Parker DONN B, fighting computer crime, Published by Charles Scribner's, New York 1983,p231.

في كندا تنظم الشرطة الملكية الكندية دورات متخصصة مدة كل دورة 4 أسابيع يتم فيها التدرب على تقنيات وأساليب تحقيق الجريمة المعلوماتية وذلك بكلية الشرطة في مدينة أوتاوا. وتشتمل موضوعات من خمسة مواضيع هي: أساسيات الحاسبات والمعالجة الإلكترونية للبيانات، مقدمة في برمجة الحاسوب، أمن الحاسبات وشبكات المعلومات، القانون والإثبات، الجريمة المعلوماتية.

Parker DONNB, op.cit,p 239

تطور مستمر وبشكل سريع جدا.

ليس هذا فحسب بل لا بد وأن تسعى الأجهزة الأمنية المعنية بالتحقيق إلى استقطاب المتخصصين والكفاءات في المجال المعلوماتى وضمهم إليها ليكونوا ضمن كوادرها والاستفادة منهم، ومن أجل ذلك ينبغي على كليات الشرطة من جهة أن تعمل جاهدة لقبول دفعات من الجامعين من خريجي كليات الحاسبات الآلية لتخرجهم ضباطاً مؤهلين قانونيا وتقنيا، كذلك يتعين على الكليات المعينة بتدريس القانون أن تسعى جاهدة إلى تدريس الحاسبات الآلية وكل ما يتعلق به إلى الطلبة، وأن تكون مادة الحاسب الآلي وتقنية المعلومات إحدى المواد الأساسية، لأن من شأن ذلك أن تتكون لدي خريجي هذه الكليات ثقافة قانونية وثقافة حاسوبية[1].

أن غرس وتطوير الثقافة الحاسوبية وسط رجال القانون والشرطة، وربطها بالثقافة القانونية والشرطية التقليدية يكفل للأجهزة الأمنية ولسلطات التحقيق النجاح الباهر في مواجهة الجرائم المعلوماتية.

ب- مظاهر التعاون الدولي في مجال تدريب رجال العدالة الجزائية

أجهزة العدالة في الكثير من الدول لاسيما الدول النامية ليست لديها تلك الجاهزية لمواجهة الجرائم المعلوماتية ومثيلاتها من الجرائم المستحدثة ذات التطور المستمر لعدة أسباب منها الافتقار إلى الموارد الكافية مادية كانت أو بشرية، أو لأن سلطات التحقيق لديها محدودة أو لأنه لديها قوانين ونظم سبقها الزمن أو قد تفتقر لأي قوانين لتتصدى بها لهذه النوعية من الجرائم.

أنه ما من دولة يمكنها النجاح في مواجهة هذه الأنماط المستحدثة بمفردها دون تعاون وتنسيق مع غيرها من الدول كانت الدعوة إلى ضرورة وجود تعاون دولي ليس فقط في مجال المساعدات القضائية المتبادلة أو في مجال تسليم المجرمين فحسب، وإنما أيضا في مجال تدريب

[1] – **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص44.

رجال العدالة[1]، فتدريب الكوادر البشرية القائمة على إنفاذ القانون ليس بذات المستوى في جميع الدول وإنما يختلف من دولة لأخرى بحسب تقدم الدولة ورقيها، بعض الصكوك الدولية والإقليمية دعت وبصريح النص إلى ضرورة وجود تعاون بين الدول في مجال التدريب ونقل الخبرات فيما بينها. كما هو الحال في المادة 29 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000.

التعاون الدولي في مجال تدريب رجال العدالة على مواجهة الجرائم المعلوماتية قد يكون بين الدول وأجهزة العدالة الجزائية لديها، وقد يتم من خلال عقد ندوات ومؤتمرات أو ورش العمل الجماعي متخصصة في مواجهة تلك الجرائم تعقد على المستوى الدولي أو على المستوى الإقليمي، حيث تقدم هذه الفعاليات العلمية من أبحاثها ودراستها وموضوعات محاورها الضوء على المستجدات المتعلقة بالجرائم المستحدثة من خلال تحليل ومناقشة أبعادها بعقلية ناجحة مما يمكن المعنيين بالوقاية ومكافحة هذه الجرائم من التعرف على أساليب ارتكابها وأخطارها ووسائل الوقاية والمكافحة بأساليب تتناسب وتفوق أساليب ووسائل مرتكبيها. وعلى هامش هذه المؤتمرات أو الندوات أو ورش العمل الجماعي تعقد اللقاءات وتبادل الآراء والخبرات.

يتحقق من عقد اللقاءات وحلقات المناقشة المصغرة بين مسؤولي الاتصال بالسفارات أو المكاتب الجغرافية الإقليمية للمنظمات والأجهزة المعنية مع جهات أو أطراف يقعون في دائرة عملهم أو بالقرب منها بناء على رغبة الجهة التي يمثلونها، يتم خلالها تبادل الآراء والخبرات بين المشاركين. وتمثل كافة هذه اللقاءات وحلقات المناقشة وسيلة طيبة للحوار والمناقشة والتشاور للتعارف وتبادل الرأي والخبرة وطرح الأفكار والتصورات وتدارس سبل تنمية وتشجيع التعاون فيما

---

[1] – يقصد بتدريب رجال العدالة تلك العملية التي يخطط لها وتصمم لها البرامج، ويبذل الجهد والمال لتغير سلوك العاملين في أجهزة العدالة، سواء أكانوا من القضاء أو من رجال التحقيق والادعاء العام "النيابة العامة" أو من رجال الضبط الجزائي، أو من رجال السلطة العامة القائمين على تنفيذ القانون أو من الموظفين المعاونين لهذه الأجهزة كالخبراء وغيرهم، أو من المهنيين الذين يشاركون في تحقيق العدالة كالمحامين، حيث تهدف هذه العملية إلى تغير سلوكهم ورفع مستوى مهارتهم واتجاهاتهم، بما يكفل حسن إنجاز العمل القانوني والقضائي والتنفيذي، مما ينعكس إيجابا على الارتقاء بكيفية أداء العدالة وتقديمها للمتقاضين بشكل يكفل إقامة التوازن بين المصلحة العامة من جهة والمصلحة الخاصة للأفراد من ناحية أخرى، مما يجعل الناس يطمئنون إلى جدية وفاعلية سير العدالة، فيبعث ذلك على الثقة وتحقيق الأمن للجميع. **محمد سيد عرفة، ت**دريب رجال العدالة وأثره في تحقيق العدالة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2005، ص 9.

بين الأطراف[1].

قد يتحقق عن طريق تنظيم الدورات التدريبية للعاملين في أجهزة العدالة الجزائية والمعنيين بمكافحة الجريمة على المستوى الدولي، وتعد هذه الصورة أكثر تطورا للتعاون الدولي الذي يستهدف تقريب وجهات النظر وتوحيد المفاهيم بين المشاركين في مكافحة الجريمة في الدول المختلفة من خلال تبادل الخبرة، وطرح موضوعات ومشكلات للتدارس المشترك، والتعرف على أحدث التطورات في مجال الجريمة لاسيما المعلوماتية وأساليب مكافحتها، وغالبا ما يجري تنظيم مثل هذا التدريب من خلال المنظمات أو الدول أو الأجهزة الكبرى ذات مستوى أكثر تقدما يمكن أن يشجع الأطراف الأخرى على المشاركة في هذه البرامج التدريبية، كما يمكنها تحمل نفقات وأعباء مثل هذه الدورات.

تحقق مثل هذه الدورات والبرامج العديد من الفوائد للجهات المنظمة وللمشاركين فيها، فالجهة المنظمة يمكنها من خلال عقد مثل هذه البرامج أن تطرح ما تريد من موضوعات حيوية، كما أنها تعلن عن دورها الرائد لتزيد من ثقة الأطراف الأخرى في أدائها، بما يشجع على إجراء المزيد من التعاون معها، وبما يضعها في مكانه خاصة لدى المتدربون والجهات التي يتبعونها. وعلى الجانب الآخر فإن هذه البرامج يمكن أن تفيد متلقي التدريب عن طريق زيادة مهاراته وخبراته ومعلوماته وقدراته على التعامل مع الأجهزة الدولية الأخرى، الأمر الذي ينعكس على الجهة التي ينتمي إليها بالفائدة.

بادرت مختلف الدول الأجنبية بإنشاء وحدات متخصصة لمكافحة الجرائم المعلوماتية، وقد خولت وزارة العدل الأمريكية في عام 2000 خمس وجهات حكومية تعامل مع جرائم المعلوماتية منها مكتب التحقيقات الفيديرالي (FBI)، والذي يضم بداخله مجموعة أشخاص مدربين على كيفية متابعة تلك الجرائم والتحري عنها وضبطها والمحافظة على ما يتم تحصيله من أدلة.

- تجربة الولايات المتحدة الأمريكية في هذا المجال:

[1] – **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص47.

تعد الولايات المتحدة الأمريكية من الدول المتقدمة تكنولوجيا والمتطورة تقنيا في مجال مكافحة الجرائم المعلوماتية وجرائم الشبكات، وعلى الرغم من ذلك فهي تعي وتعلم أنه ما من دولة وإن كانت متقدمة يمكنها التصدي لأخطار هذه الأنماط المستحدثة من الجرائم.

من هذا المنطلق تحرص على توفير المساعدة التقنية والتدريب لرفع قدرات العدالة الجزائية لدى الحكومات الأخرى، ومساعدة ما لديها من أجهزة شرطة، ومسئولي الادعاء العام، والقضاة ليصبحوا أكثر فعالية في مكافحة الجريمة. فمثل هذه المساعدة لا تؤدي إلى تيسير بناء إطار للتعاون الدولي في مجال تطبيق القانون وحسب، ولكنها تعزز أيضاً قدرة الحكومات الأجنبية المعنية على ضبط مشاكل الجريمة المعلوماتية لديها قبل أن يمتد ليتجاوز حدود بلدانها.

مكتب المساعدة والتدريب على تطوير أجهزة الادعاء العام في الخارج، التابع لوزارة العدل الأميركية، مكلّف تحديداً بتوفير المساعدة اللازمة لتعزيز مؤسسات العدالة الجزائية في دول أخرى، وتعزيز إدارة القضاء في الخارج.

كما أن البرنامج الدولي للمساعدة والتدريب على التحقيق الجزائي(ICITAP) ، الذي كثيراً ما يعمل بالترادف مع وحدته الشقيقة – مكتب المساعدة والتدريب على تطوير أجهزة الادعاء العام في الخارج، العامل داخل وزارة العدل نفسها – على توفير مساعدات لأجهزة الشرطة في البلدان النامية في مختلف أنحاء العالم، وتهدف المساعدة التي يقدمها هذا البرنامج الأخير إلى تعزيز القدرات التحقيقية لدى أجهزة الشرطة في البلدان الناشئة[1].

تقدّم وزارة العدل الأميركية الوقت الحاضر، مساعدات لتطوير القطاع القضائي في عدد من البلدان في أفريقيا، وآسيا، وأوروبا الشرقية والوسطى وأميركا اللاتينية ومنطقة حوض الكاريبتي، والدول المستقلة حديثاً، بما ذلك روسيا والشرق الأوسط. مستعينة في ذلك بخبرة الوحدات المتخصصة التابعة لها. منها على سبيل المثال، وحدة مكافحة استغلال الأطفال وأعمال الفحش التابعة للقسم الجزائي بها، قامت بدور أساسي في صياغة قانون نموذجي يهدف إلى مكافحة استغلال الناس عن طريق الإتجار بالبشر والبغاء.

[1] – حسين بن سعيد بن سيف الغافري، "الجهود الدولية في مواجهة جرائم الأنترنت"، مرجع سابق، ص49.

هذا من جهة ومن جهة أخرى، أن أجهزة تطبيق القانون الأمريكية توفر أيضا تدريباً لنظيراتها من الأجهزة في البلدان الأخرى داخل الولايات المتحدة الأمريكية أو خارجها عن طريق إنشاء معاهد خاصة بتدريب العاملين في أجهزة تطبيق القانون كما هو الحال في كل من المجر، وبوتسوانا، وكوستاريكا، وتايلند. وفي هذه المعاهد، يقوم خبراء أميركيون في عمل أجهزة تطبيق القانون باطلاع المتدربين على أساليب وسبل مبتكرة للتحقيق، ويشجعون على تبادل الآراء مع نظرائهم في مختلف أنحاء العالم.

- بالنسبة لفرنسا وجدت وكالة الأمن القومي للنظام المعلوماتي (Anssi) في جويلية 2009، وضعت استراتيجية لتحقيق الدفاع والأمن ألمعلوماتي للوقاية من الهجمات الإلكترونية وضمان أمن الشركات الفرنسية والأمة في الفضاء الإلكتروني، وقد تم تقسيم هذه المهمة بين رجال الشرطة والدرك، حيث يختص هذا الأخير بالرقابة على المواقع التي تحتوى صورا إباحية، أما رجال الشرطة فيختص بمراقبة المواقع التي تبث فيها الجرائم التالية، القرصنة المعلوماتية، الإرهاب والأعمال العنصرية. ومن اجل تحقيق هذه الأهداف قامت فرنسا بتكوين شبكة خبراء من قوات الشرطة والدرك وتدريبهم تماشيا مع التطور التكنولوجي الذي يشهده العالم، وذلك من خلال زيادة الرقابة على المواقع الأنترنت وعقد مؤتمرات وندوات حول الجريمة المعلوماتية والتطورات المستجدة بها[1].

- أما بالنسبة للجزائر تم تنصيب إدارة متخصصة في مكافحة الجرائم المعلوماتية نظرا لازدياد معدلات الجريمة في الآونة الأخيرة مع ازدياد التقدم العلمي في المجال التكنولوجي واستخدام الجناة للوسائل العلمية الحديثة في ارتكاب جرائمهم، وجد المشرع نفسه مضطرا إلى التدخل من خلال تعديل قانون الإجراءات الجزائية بموجب قانون رقم 06-22، فاستحدث المشرع فصلين، الرابع والخامس من الباب الثاني من الكتاب الأول. كما جاء في نص المادة 3 من المرسوم المتعلق بتنظيم

[1] – L'Agence nationale de la sécurité des systèmes d'information (ANSSI) rend au publique la stratégie de la France en matière de défense et de sécurité des systèmes d'information, https://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite-2. consulté le: 01/02/2016.

المـركـزيــة لــوزارة الــبــريــد وتكنولوجيات الإعلام والاتصال[1]على إنشاء المديرية العامة لمجتمع المعلومات.

كما تم استحداث شبكة اتصالات وطنية موحدة لجمع البيانات تربط فيما بين مختلف مكاتب الدرك الوطني وتزودهم بقاعدة البيانات المتعلقة بشبكات الإجرام المعلوماتي.

أما من حيث التكوين والتأهيل في مجال مكافحة الجريمة المعلوماتية فالجزائر أبرمت العديد من الاتفاقيات الثنائية مع الدول الأوربية مثل فرنسا وكذلك الولايات المتحدة الأمريكية، من اجل بعث إطارات من الدرك الوطني للتكوين والتخصص في البحث والتنقيب وملاحقة مجرمين المعلوماتية.

إنّ الحاجة ملحة إلى وجود التعاون أجهزة الشرطة بين الدول المختلفة وذلك عن طريق إنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المعلوماتية، حيث أن الدولة لا تستطيع بمفردها القضاء على هذا النوع من الإجرام العابر للحدود الوطنية.

أنه ما من دولة يمكنها بنجاح مجابهة هذا التحدي في مواجهة هذه الأنماط المستحدثة من الجرائم، ولا مفر من مواصلة أجهزة تطبيق القانون في أنحاء العالم تطوير القدرة على التعاون الدولي في المجال التدريبي، ولا مفر للدول المتقدمة من مساعدة الدول النامية لتعزيز مؤسساتها المتخصصة بالتحري والتحقيق والمحاكمة، من خلال توفير التدريب وسائر أنواع المعونة التقنية.

[1]– مرسوم تنفيذي رقم 17–96 مؤرخ في 29 جمادى الأولى عام 1438 هـ الموافق 26 فبراير سنة 2017 يتضمن تـنـظـيم الإدارة المـركـزيــة لــوزارة الــبــريــد وتكنولوجيات الإعلام والاتصال، الجريدة الرسمية للجمهورية الجزائرية عدد 14 بتاريخ 1 مارس2017.

خاتمة

تناول موضوع البحث "الدليل الإلكتروني ودوره في الإثبات الجنائي" أهم مشكلة من المشكلات التي أفرزتها ثورة المعلومات والاتصالات عن بعد، التي جاءت بمفاهيم ومعاملات جديدة – العمليات المصرفية الإلكترونية والمستندات الإلكترونية والتوقيعات الإلكترونية وحتى عن حكومات الكرتونية– استوجب حمايتها جنائيا من جميع صور الاعتداء المتطور، فظهر هناك قصور كبير في النصوص الجنائية الموضوعية، ولم يكن في الواقع قانون الإجراءات الجزائية أحسن حال، حيث وجدت الكثير من المشاكل في التطبيق، خاصة جانب التحقيق والإثبات، فمنها مشاكل تتعلّق بجمع الأدلة، ومشاكل تتعلّق بالقانون.

تبين من البحث أن الخصوصية التي يتميز بها الدليل الإلكتروني، جعلت مختلف الدول والهيئات والمنظمات الدولية والإقليمية تتسارع لوضع أساليب وإجراءات حديثة تسهل عمليات البحث عنه واشتقاقه تتناسب مع طبيعته، كما تم عقد مؤتمرات واتفاقيات ومعاهدات بين الدول لتحقيق التعاون الدولي الفعال في هذا المجال.

ساير المشرع الجزائري التغيرات التشريعية التي فرضتها الثورة المعلوماتية، فسعى لسد الفراغ التشريعي الذي كان يعاني منه قانون العقوبات الجزائري، وذلك بتعديله بموجب قانون رقم 04-15، كذلك تعديل قانون الإجراءات الجزائية بموجب قانون رقم 06-22، وإصدار قانون خاص والمتمثل في قانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بالإضافة إلى تعديلات أخرى مست قوانين أخرى منها قانون حماية حق المؤلف والحقوق المجاورة، إلا أنه بالرغم من هذه المحاولات يبقى المشرع الجزائري بعيد عن التطور القانوني على المستوى العالمي، مما يستوجب إصدار المزيد من القوانين لتقوية الترسانة القانونية في هذا المجال.

بالتالي توصلنا من خلال البحث إلى النتائج التالية:

– وجود مواكبة حديثة لاقتناء التقنية المعلوماتية في الجزائر والاستفادة منها والتي صاحبتها جهود وقائية وردعية للجرائم المعلوماتية تتمثل في صدور الأنظمة والتشريعات.

– إن سهولة إتلاف الأدلة الإلكترونية تنطوي على مشكلات وتحديات إدارية وقانونية تتصل ابتداء بإجراءات التحري وبمقتضيات عمليات ملاحقة الجناة، فإن تحققت الملاحقة أصبحت الإدانة صعبة.

– نقص الخبرة لدى أجهزة الشرطة والقضاء في تمحيص عناصر الجريمة المعلوماتية وجمع الأدلة الإلكترونية للإدانة فيها.

– عدم كفاية معاهدات الثنائية أو الجماعية بين الدول التي تسمح بالتعاون الدولي لمواجهة المتطلبات الخاصة للجرائم المعلوماتية وديناميكية التحريات فيها وكفالة السرعة بها.

بالإضافة إلى ذلك:

– أظهر البحث أن الدليل الإلكتروني عبارة عن معلومات ذو طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان، من السهل إتلافه في أي لحظة.

– تبين أيضا من البحث أن الإجراءات التقليدية لجمع الدليل الإلكتروني غير كافية، بل لابد من أن تصاحبها الإجراءات الحديثة، كإجراء التسرب الذي استحدثه المشرع الجزائري، وكاعتراض الاتصالات الإلكترونية سواء بالنسبة للمعلومات المخزنة أو المتحركة.

– أصبح من المقرر في التشريعات المختلفة أنه يجوز إصدار إذن التفتيش لضبط المعلومات من الرغم من طبيعتها المعنوية، بالرجوع إلى مدلول كلمة شيء، فيعني كل ما يشغل حيزا في فراغ معين، ولما كانت الكيانات المنطقية والبرامج تشغل حيزا ماديا في ذاكرة الحاسوب، ويمكن قياسها بمقياس معين، فهي تأخذ شكل نبضات الكرتونية تمثل الرقمين صفر أو واحد، فهي تعد أشياء بالمعنى العلمي للكلمة ومن ثم تصلح لان تكون محلا للضبط.

– يجوز إصدار إذن التفتيش حتى وإن كان الشئ المراد تفتيشه خارج إقليم الدولة فان الإنابة القضائية الدولية هي السبيل لتحصيل هذا الدليل، بحيث تفوض الدولة الأخرى في جمع الدليل وإرساله لدولة التحقيق.

– لا يجوز الاطلاع أو الإعتراض على الحياة الخاصة للفرد كخصوصية بريده الإلكتروني بدون رضا صاحبه، إلا بالشروط التي يحددها القانون.

- أن مجرد الحصول على الدليل الإلكتروني وتقديمه إلى القضاء لا يكفي لاعتماده كدليل إدانة، إذ أن الطبيعة الفنية الخاصة للدليل تمكن من العبث بمضمونه على نحو يحرف الحقيقة دون أن يكون في قدرة الشخص غير المتخصص إدراك ذلك العبث.

- أن القاضي يملك سلطة واسعة في تقييم الدليل الإلكتروني من حيث قيمته الإثباتية، فللقاضي قبول الدليل أو رفضه، وهو يعتمد في ذلك على مدى اقتناعه الشخصي بذلك.

- ينشأ الدليل الإلكتروني في بيئة افتراضية بالتالي فعملية إستخراجه يكون في صورة نسخ مطابقة للأصل ولها نفس القيمة العلمية والحجية الثبوتية، الشيء الذي لا يتوافر في الدليل التقليدي، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقدان والتلف والتغيير عن طريق عمل نسخ طبق الأصل من الدليل.

- أن الشك في الدليل الإلكتروني قد لا يتعلق بمضمونه كدليل، وإنما بعوامل مستقلة عنه تؤثر في حجيته، إلا أنه هناك وسائل فنية تمكن من فحصه للتأكد من سلامته وصحة الإجراءات المتبعة في الحصول عليه.

- يجب عدم الخلط بين الشك الذي يشوب الدليل الإلكتروني بسبب إمكانية العبث به أو لوجود خطا في الحصول عليه، وبين القيمة الإقناعية لهذا الدليل، فالحالة الأولى لا يملك القاضي الفصل فيها لأنها مسالة فنية فالقول فيها لأهل الخبرة، فان سلم الدليل من العبث والخطأ، فانه لا يكون للقاضي سوى القبول به، ولا يمكنه التشكيك في حجيته الإثباتية لكونه يمثل اختبارا صادقا عن الواقع، ما لم يثبت عدم الدليل بالجريمة المراد إثباتها. أما فيما يخص تقدير الدليل، فان للقاضي أن يأخذ بتقرير الخبير كله أو بعضه، فعلى القاضي أن يحكم بما يطمئن إليه وجدانه.

- أن الدليل الإلكتروني لا يقتصر مجال العمل به كدليل إثبات الجرائم المعلوماتية فحسب، بل يصلح أحيانا لإثبات جرائم أخرى استعمل الحاسوب فيها كوسيلة لارتكابها.

على ضوء النتائج التي أظهرها البحث، خلص إلى جملة من التوصيات الآتية:

- ضرورة تعزيز الترسانة القانونية للجزائر لمكافحة الجريمة المعلوماتية لأنها غير كافية فيجب إثرائها للتمكن من وصف كل أنواع المخالفات الإلكترونية.

– إنه من الأجدر بالمشرع الجزائري أن ينص على الدليل الإلكتروني ضمن أدلة إثبات الزنا وذلك سدا للفراغ التشريعي الذي أصبح جليا في أغلب التشريعات خاصة العربية منها، خاصة وأنه سوى بين الكتابة والشكل الإلكتروني والكتابة في القانون المدني.

– على المشرع الجزائري مراجعة المادة 81 من قانون الإجراءات الجزائية، حيث يصبح التفتيش ليس مقتصرا فقط على الأشياء المادية، وذلك بإدراج في المادة صيغة " المعلومات".

– يجب تكوين القضاة وممثلي الهيئات النظامية في مجال الجرائم المعلوماتية، فعلى كل القضاة أن تكون لديهم فكرة "دقيقة" عن هذا النوع من الإجرام حتى يتمكنوا من وصف الجريمة المتعلقة بتكنولوجيات الإعلام والاتصال، تحقيقا لصالح المجتمع والأفراد، لكي يدان المتهم ويبرئ البريء.

– كما يجب التأكيد على أهمية تحسيس المؤسسات الاقتصادية ومؤسسات الدولة بضرورة حماية أنظمتهم الإعلامية ومواقع الواب الخاصة بهم من القراصنة من خلال وضع أنظمة لمكافحة هذا النوع من الجرائم يشرف عليها مهندسون يتصدون لكل خطر الإلكتروني.

– ضرورة تحسيس الموظفين بالمؤسسات بأهمية الأمن المعلوماتي وضرورة تكوين التقنيين في هذا المجال.

– ضرورة حماية برامج الحاسب الإلكتروني حماية قانونية بصفة عامة وحماية جنائية محليا ودوليا، والبحث عن الوسيلة المثلى لحماية هذه البرامج، ويرجع ذلك لحماية الاستثمارات المادية والبشرية، ولتشجيع الابتكار والخلق والاختراع.

– بالرغم من أن خطر الجريمة المعلوماتية في الجزائر يعد "ضعيفا" لأن الخدمات الإلكترونية على غرار الصحة والتجارة والإدارة الإلكترونية تكاد تكون منعدمة. ولأن مؤسساتنا ليست موجهة بعد نحو الصفقات وخدمات إلكترونية أخرى، إلا أن هذا لا ينبغي أن يمنعنا من التزود بأدوات لضمان حمايتنا من الجرائم المعلوماتية عند إدخال هذه التكنولوجيات لأن الأمر يتعلق بظاهرة لا مناص منها، إذ يجب أن نساير ركب التقدم العلمي في مختلف نواحي الحياة.

– أصبح التعاون الدولي أمر ضروري لمكافحة الجرائم المعلوماتية، وتطوير وسائل الإثبات، وتتبع المجرمين الذين أصبحوا مختفين وراء أجهزة الإعلام الآلي، متحكمين في آخر ما تنتجه التكنولوجيا، ولتفعيل التعاون الدولي لا بد من التركيز على العناصر الأساسية التالية وهي:

– الانضمام إلى المعاهدات الدولية التي تعمل على زيادة التعاون والتنسيق بين الجهود التي تبذلها الدول في مجال مكافحة جرائم المعلوماتية.

– إدخال تلك المعاهدات الدولية إلى حيز التنفيذ الفعلي، أي تنفيذ ما تنص عليه الاتفاقيات من إجراءات دون أي تأخير.

– العمل على وجود أكبر قدر من التناسق والتطابق فيما بين قوانين الدول المختلفة والمتعلقة بمكافحة الجرائم المعلوماتية، فلا يكون الفعل الذي ارتكب في بلد ما وغير معاقب عليه في قانون دولة أخرى، فمن هنا يجد المجرمون الملاذ الأمن الذي يلجؤون إليه دون أي اعتبار لما ارتكبوه من الجرائم

– تعاون جميع الدول في تسليم المطلوبين أمنيا إلى الدول التي تطالب بهم لارتكابهم جرائم الأنترنت.

– أخيرا على السلطات الجزائرية اتخاذ الإجراءات التالية لتخفيض نسبة الجرائم المعلوماتية، وذلك بـ:

– فرض رقابة على المقاهي التي تقدم الأنترنت كخدمة لمرتاديها مع التأكيد على منع ارتياد صغار السن لتلك المقاهي وفرض عقوبات وغرامات مالية على مقاهي التي تخالف ذلك، والعمل على تشجيع مرتدي هذه المقاهي في البحث عن المعلومات المفيدة واستخدام الأنترنت لمعرفة أسباب ظاهرة ارتيادها والانحراف إلى الجريمة بقين مرتاديها بجميع مناطق المملكة.

– حجب المواقع الإباحية والإرهابية التي تشجع الجريمة وتظهرها بوجه مشرق، فالدولة تتبع سياسة الحجب لكنها في الغالب تحجب شيئا قليلا جدا من المواد الإباحية بالإضافة إلى أن أجهزة الحجب لديها ضعيفة جدا ومقترنة بثغرات كبيرة، والحجب من الأساليب المجدية، حيث نجد الدول التي تفرض قوانين صارمة في منع المواد الإباحية تنخفض فيه نسبة هذه الجرائم.

– تفعيل دور وسائل الإعلام في نشر التوعية الوقائية من عواقب النظر في المواقع الإباحية وكذلك تحصين المواطنين فكريا ودينيا وإفهامهم أن مثل هذه المواقع تستهدف شبابنا وهي محاولة لتصدير الإباحة بدعوى الحرية وأن أهل الغرب يقيمهم الفاسدة وأمراضهم الخبيثة ومبادئهم الذميمة لمن يكتفوا بإفشاء الرذائل والمنكرات ودواعي غضب الجبار بينهم ولكن تمادى بهم الحال إلى محاولة تصدير هذه المصائب والفتن إلى بلاد المسلمين، كما أن يكون هناك تشهير وإعلان لكل من يقبض عليه في مثل هذه الجرائم لتحقيق الرادع النفسي وإتباع لأمر الله تعالى.

– استخدام المناهج التعليمية كأوعية ووسائل لمكافحة جرائم الكمبيوتر والأنترنت وربطها بالنواحي الدينية.

– إنشاء هيئة مشابهة لهيئة المواصفات والمقاييس يكون اختصاص هذه الهيئة تكوين مواقع علمية مفيدة ومتقدمة عالميا، فعلى سبيل المثال أن موقع (Google) بمجرد وضعك لأي كلمة بحث فستجد أن الصفحة قد امتلأت بالمواقع فمنها المفيد ومنها الضار، ولكن نريد من هذه الهيئة أن تنشأ مواقع مشابهة لهذا الموقع في الهيكل ومخالفة في المضمون بحيث يكون ما بداخله من أمنيا ودينيا ويقصد به البناء لا الهدم.

قائمة المراجع

أولا- باللغة العربية:

أ- الكتب:

1. **أحمد حسام طه تمام**، الحماية الجنائية لتكنولوجيا الاتصالات دراسة مقارنة، دار النهضة العربية، القاهرة، 2002.
2. أحمد خليفة **الملط**، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2005.
3. **أحمد شوقي الشلقاني**، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الجزائر،1999.
4. **أحمد فتحي سرور**، الوسيط في قانون الإجراءات الجنائية،، الطبعة الثانية، دار النهضة العربية، القاهرة، 1981.
5. ----------، القانون الجنائي الدستوري، دار أشرف، القاهرة، 2001.
6. **أسامة أحمد المنعاسة**، جلال محمد الزغبي، فاضل الهواوشة، جرائم الحاسب الآلي والأنترنت، دار وائل للنشر، عمان، 2001.
7. **أسامة بن نائل المحيسن ومحمد بن درويش الشيدي**، القوانين المكملة، مجمع البحوث والدراسات، أكاديمية السلطان قابوس لعلوم الشرطة، مسقط، 2002.
8. **أشرف توفيق شمس الدين**، الحماية الجنائية للمستند الإلكتروني دراسة مقارنة، دار النهضة العربية، القاهرة، 2006.
9. **أشرف عبد القادر قنديل**، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015.
10. **أمين مصطفى محمد**، حماية الشهود في قانون الإجراءات الجنائية دراسة مقارنة، دار النهضة العربية، القاهرة،2008.

11. **أنس كيلاني**، موسوعة الإثبات في القضايا الجزائية، دار الأنوار للطباعة، دمشق، 1991.
12. **إيمان محمد علي الجابري**، يقين القاضي الجزائي، منشأة المعارف، الإسكندرية، 2005.
13. **جمال جرجيس**، الشرعية الدستورية لأعمال الضبطية القضائية، النسر الذهبي للطباعة، القاهرة، 2006.
14. **جميل عبد الباقي الصغير**، أدلة الإثبات الجنائي والتكنولوجيا الحديثة دراسة مقارنة، دار النهضة العربية، القاهرة، 1992.
15. ----------، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة 1998.
16. ----------، الأنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2002.
17. **جندي عبد المالك**، الموسوعة الجنائية، الجزء الأول، منشورات الحلبي الحقوقية، بيروت، 2010.
18. **حاتم عبد الرحمن منصور الشحات**، الإجرام المعلوماتي، دار النهضة العربية، القاهرة 2002.
19. **حسام الدين الأهواني**، الحق في احترام الحياة الخاصة دراسة مقارنة، دار النهضة العربية، القاهرة، 1978.
20. **حسام الدين الأهواني**، جميل عبد الباقي الصغير، مقدمة في الحاسب الآلي،دار النهضة العربية، القاهرة، 2000.
21. **حسن محمد ربيع**، دور القاضي الجنائي في الإثبات دراسة مقارنة، المؤسسة الفنية للطباعة والنشر، القاهرة، 1977.
22. **خالد عياد الحلبي**، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، عمان، 2011.
23. **خالد ممدوح إبراهيم**، أمن مراسلات البريد، الدار الجامعية، الإسكندرية، 2008.
24. ----------، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، القاهرة، 2010.

25. **رأفت عبد الفتاح حلاوة**، الإثبات الجنائي قواعده وأدلته، دار النهضة العربية، القاهرة، 2003.

26. **رمزي رياض عوض**، حماية المتهم في النظام الأنجلوأمريكي، دار النهضة العربية، القاهرة، 1998.

27. **رياض فتح الله بصلة**، حدود الإثبات العلمي في قضايا التزييف والتزوير دراسة في المفاهيم والأساليب والإجراءات، دار نوبار للطباعة، القاهرة، 2001.

28. **سراج الدين محمد الروبي**، آلية الأنتربول في التعاون الدولي الشرطي، الدار المصرية اللبنانية، القاهرة، 1998.

29. **سعيد عبد اللطيف حسن**، الحكم الجنائي الصادر بالإدانة، دار النهضة العربية، القاهرة، 1989.

30. ----------، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الأنترنت، دار النهضة العربية، القاهرة،1999 .

31. **سليمان عبد المنعم**، بطلان الإجراء الجنائي، دار الجامعة الجديدة، الإسكندرية، 1999.

32. **شريف محمد غنام**، حماية العلامات التجارية عبر الأنترنت في علاقتها بالعنوان الإلكتروني، دار النهضة العربية، القاهرة، 2003.

33. **شيماء عبد الغني محمد عطا الله**، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الاسكندرية، 2007.

34. **عبد الحافظ عبد الهادي عابد**، الإثبات الجنائي بالقرائن، دار النهضة العربية، القاهرة، 1998.

35. **عبد الحميد الشواربي**، جريمة الزنا في ضوء القضاء والفقه، دار المطبوعات الجديدة، الإسكندرية، 1985.

36. **عبد العظيم وزير**، شرح قانون العقوبات القسم الخاص جرائم الاعتداء على الأموال، دار النهضة العربية، القاهرة، 1993.

37. **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، القاهرة، 2005

38. ----------، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، القاهرة،2007.

39. ----------، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الاسكندرية، 2009.

40. ----------،الجريمة في عصر العولمة دراسة في الظاهرة الإجرامية المعلوماتي، دار الفكر الجامعي، الاسكندرية، 2010.

41. **عبد الفتاح عبد اللطيف حسين الجبارة**، الإجراءات الجنائية في التحقيق، الحامد للنشر والتوزيع، عمان، 2015.

42. **عبد الفتاح محمد سراج**، النظرية العامة لتسليم المجرمين، دار النهضة العربية، القاهرة، 1998.

43. **عبد اللطيف أبو السعود، الأنترنت**، الهيئة المصرية العامة للكتاب، القاهرة، 1987.

44. **عفيفي كامل عفيفي**، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، الطبعة الثانية، منشورات الحلبي الحقوقية، بيروت، 2007.

45. **عكاشة محمد عبد العال**، الإنابة القضائية في نطاق العلاقات الخاصة الدولية، الدار الجامعية، بيروت، 1992.

46. **علاء الدين شحاته**، التعاون الدولي لمكافحة الجريمة، إيتراك للنشر والتوزيع، القاهرة، 2000

47. **علي أحمد عبد الزعبي**، حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب، 2006.

48. **علي حسن محمد الطوالبة**، التفتيش الجنائي على نظم الحاسوب والأنترنت، عالم الكتب الحديثة، القاهرة، 2004.

49. **علي زكي العرابي**، المبادئ الأساسية للتحقيقات والإجراءات الجنائية، طبعة لجنة التأليف والترجمة، القاهرة، 1940.

50. **علي زكي محمود محمود مصطفى**، الإثبات في المواد الجنائية في القانون المقارن، الجزء الأول، مطبعة جامعة القاهرة، 1978 .

51. **علي محمد رحومة**، المجتمع الآلي، سلسلة عالم المعرفة، الكويت، 2008.

52. **عماد عوض عدس**، التحريات كإجراء من إجراءات البحث عن الحقيقة، دار النهضة العربية، القاهرة، 2007.

53. **عمر محمد بن يونس**، الإجراءات الجنائية عبر الأنترنت المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية، دار النهضة العربية، القاهرة، 2008.

54. **عوض محمد عوض**، قانون الإجراءات الجنائي، الجزء الأول، مؤسسة الثقافة الجامعية، الإسكندرية، 1989.

55. **فاروق علي الحفناوي**، موسوعة قانون الكمبيوتر ونظم المعلومات قانون البرنامجيات دراسة متعمقة في الأحكام القانونية ببرمجيات الكمبيوتر، الكتاب الأول، دار الكتاب الحديث، القاهرة، 2003.

56. **فتحي محمد أنور عزت**، الحماية الجنائية الموضوعية والإجرامية على المصنفات والحق في الخصوصية في الكمبيوتر والأنترنت في نطاق التشريعات الوطنية والتعاون الدولي، دار النهضة العربية، القاهرة، 2007.

57. ----------، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، دار النهضة العربية، القاهرة، 2010.

58. **فتوح عبد الله الشاذلي**، قواعد الأمم المتحدة لتنظيم قضاء الأحداث، دار المطبوعات الجامعية، الاسكندرية، 2014.

59. **فوزية عبد الستار**، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1986.

60. **قدري عبد الفتاح الشهاوي**، ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، 2005.

61. ----------، مناط مشروعية العمل الشرطي، دار النهضة العربية، القاهرة، 2007.

62. **محمد أحمد عياينة**، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، 2006.

63. **كامل السعيد**، شرح قانون العقوبات الجرائم الواقعة على الأخلاق والآداب العامة والأسرة، مكتبة الثقافة للنشر والتوزيع، عمان، 1994.

64. **كامل مصطفى**، مسائل عملية أمام المحاكم الجنائية، منشأة المعارف، الإسكندرية،1990.

65. **مأمون محمد سلامة**، الإجراءات الجزائية في التشريع المصري، دار النهضة العربية، القاهرة، 1992.

66. **محمد أبو العلا عقيدة**، شرح قانون الإجراءات الجزائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 2001.

67. **محمد الأمين البشيري**، التحقيق في الجرائم المستحدثة، مطبعة جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

68. **محمد السيد عرفة**، تدريب رجال العدالة وأثره في تحقيق العدالة، مطبعة جامعة نايف العربية للعلوم الأمنية، الرياض، 2005.

69. **محمد حسين منصور**، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2003.

70. **محمد حماد مرهج الهيتي**، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، عمان، 2004.

71. **محمد زكي أبو عامر**، الإثبات في المواد الجنائية، الفنية للطباعة والنشر، الإسكندرية، 1985.

72. -------، الإجراءات الجنائية، دار الجامعة الجديدة، الإسكندرية، 2008.

73. **محمد سامي الشوا**، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1998.

74. **محمد عيد الغريب**، حرية القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام، دار النهضة العربية، القاهرة، 2008.

75.**محمد فهمي طلبه**، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، مطابع المكتب المصري الحديث، القاهرة، 1991.

76. **محمد منصور الصاوي**، أحكام القانون الدولي في مجال مكافحة الجرائم الدولية للمخدرات، دار المطبوعات الجامعية، الإسكندرية،1980.

77. **محمود نجيب حسني**، شرح قانون الإجراءات الجزائية، الطبعة الثانية، دار النهضة العربية، القاهرة،1988.

78. ----------، شرح قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، 1978.

79.**ممدوح عبد الحميد عبد المطلب**، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، القاهرة، 2006.

80.**نائلة عادل محمد فريد قورة**، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، 2005.

81.**نبيلة هبة مولاي علي هروال**، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2005.

82. **نواف كنعان**، النماذج المعاصرة لحق المؤلف ووسائل حمايته، الطبعة الثالثة، كلية الحقوق، عمان، 2000.

83. **هشام محمد فريد رستم**، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992.

84. ----------، الجوانب الإجرائية للجرائم المعلوماتية، مكتب الآلات الحديثة، أسيوط، 1994 .

85. **هلالي عبد اللاه أحمد**، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، دار النهضة العربية، القاهرة،2006.

86. .....، حجية المخرجات الكمبيوترية في المواد الجنائية دراسة مقارنة، دار النهضة العربية، القاهرة، 1998

87. **موسى مسعود ارحومة**، قبول الدليل العلمي أمام القضاء الجنائي دراسة مقارنة، مطبعة جامعة قار يونس، طرابلس، 1999.

ب- الأطروحات والمذكرات:

1) -الأطروحات:

1. **إبراهيم الغمار**، الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1980

2. **أحمد ضياء الدين محمد خليل**، مشروعية الدليل في المواد الجنائية دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجزائية، رسالة دكتوراه، كلية الحقوق جامعة عين الشمس، القاهرة، 1982 .

3. **أحمد فتحي سرور**، نظرية البطلان في قانون الإجراءات الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1959.

4. **السيد محمد حسن شريف**، النظرية العامة للإثبات الجنائي، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2002.

5. **أمال عثمان**، الخبرة في المسألة الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1964.

6. **أيمن عبد الله فكري**، جرائم نظم المعلومات، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2006 .

7. **حسين بن سعيد بن سيف الغافري**، السياسة الجنائية في مواجهة جرائم الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2009.

8. **رشيدي محمد علين**، الحماية الجنائية للمعلومات على شبكة الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2009.

9.**سالم محمد سليمان** الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة،، 1997.

10.**فاضل زيدان محمد**، سلطة القاضي الجنائي في تقدير الأدلة دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة بغداد، 1992.

11.**فتحي محمد أنور عزت**، دور الخبرة في الإثبات الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، 2007.

12.**فرج إبراهيم العدوي عبده**، سلطة القاضي الجنائي في تقدير الأدلة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1995.

13.**محمد عبيد سعيد سيف**، مشروعية الدليل في المجالين الجنائي والتأديبي دراسة مقارنة، بالتطبيق على تشريعات دولة الإمارات العربية المتحدة، رسالة لنيل درجة الدكتوراه في علوم الشرطة، أكاديمية مبارك للأمن، القاهرة، 2007.

14.**مفيدة سويدان**، نظرية الاقتناع الذاتي للقاضي الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1975 .

15. **هلال عبد اللاه أحمد عبد العال**، النظرية العامة للإثبات الجنائي دراسة مقارنة بين النظم الإجرائية اللاتينية والشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1984.

2) –المذكرات:

1.**بلولهي مراد**، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، مذكرة ماجستير في العلوم القانونية، كلية الحقوق، جامعة باتنة، 2011.

2.**سعيداني نعيم**، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة باتنة، 2013 .

3. **عائشة بن قارة مصطفى**، حجية الدليل الإلكتروني في مجال الإثبات الجنائي دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2009.

4. **قارة آمال، الجريمة المعلوماتية**، مذكرة ماجستير، كلية الحقوق، جامعة الجزائر، 2002.

5. **محمد بن نصير محمد السرحاني**، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والأنترنت، رسالة ماجستير لقسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، 2004.

6. **ناير نبيل عمر**، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2012.

7. **نبيلة هبة مولاي علي هروال**، الجوانب الإجرائية لجرائم الأنترنت في مرحلة الاستدلالات دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2006.

ج- المقالات:

1. **أحمد أبو القاسم**، "المفهوم العلمي والتطبيقي للدليل الجنائي المادي"، مجلة مركز بحوث الشرطة، تصدر عن أكاديمية مبارك للأمن، القاهرة، العدد السابع والعشرين، يناير 2005، (ص ص151-164).

2. **أحمد بن بخيت الشنفري**، "التعاون الدولي في مجال تسليم المجرمين"، مجلة الأمانة الدورية، تصدر عن مجمع البحوث والدراسات بأكاديمية السلطان قابوس لعلوم الشرطة، مسقط، سلطنة عمان، العدد16، يناير 2005(ص ص155-170).

3. **علي احمد البسيوني**، "الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية"، مجلة الفكر الشرطي، تصدر عن مركز بحوث الشرطة بالقيادة العامة لشرطة الشارقة، دولة الإمارات العربية المتحدة، المجلد الحادي والعشرون، العدد 81، 2012، (ص ص51-73).

4. **جمال ماهر**، "اتفاقيات التعاون القانوني والقضائي في تسليم المجرمين"، (ص ص 01-30)، محمول من الموقع الإلكتروني التالي: http://montada.echoroukonline.com/showthread.php?t=84558.

5. **حسين بن سعيد بن سيف الغافري**، "الجهود الدولية في مواجهة جرائم الأنترنت "، (ص ص 01-62) محمول من الموقع الإلكتروني التالي: www.minshawi.com/vb/attachment.php?attachmentid=337&d.jl.

6. **خالد ممدوح ابراهيم**، "الدليل الإلكتروني في جرائم المعلوماتية"،(ص ص 01-02)،محمول من الموقع الإلكتروني التالي: http://kenanaonline.com/users/khaledMamdouh/posts/79345 /.

7. **رأفت رضوان**، "شرطة الأنترنت "، مجلة مركز بحوث الشرطة، تصدر عن أكاديمية مبارك للأمن، القاهرة، العدد 26، يوليو 2004، (ص ص98-116).

8. **رشيدة بوكر**، "الدليل الإلكتروني ومدى حجيته في الإثبات الجزائي في القانون الجزائري"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، تصدر عن كلية الحقوق جامعة دمشق، المجلد 27، العدد الثاني، 2011، (ص ص 297-331).

9. **عادل عبد الله خميس المعمري**، "التفتيش في الجرائم المعلوماتية"، مجلة الفكر الشرطي، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، دولة الإمارات العربية، المجلد الثاني والعشرون، العدد 86، 2013،(ص ص 50-57).

10. **عادل مستاري**، "دور القاضي الجنائي في ظل مبدأ الاقتناع القضائي"، مجلة المنتدى القانوني، تصدر عن كلية الحقوق الحقوق والعلوم السياسية بجامعة بسكرة، العدد الخامس، 2013، محمول من الموقع الإلكتروني التالي:

http://fdsp.univ-biskra.dz/images/revues/mntda/r5/mk5a13.pdf

11. **عبد الفتاح محمود كيلاني**، "مدى المسؤولية القانونية لمقدمي خدمة الأنترنت "، (ص ص 471-518) محمول من الموقع الإلكتروني التالي: http://www.flaw.bu.edu.eg/flaw/images/part2.pdf

12. **علاوة وهام**،" التسرب كآلية للكشف عن الجرائم في قانون الإجراءات الجزائية الجزائري"، مجلة الفقه والقانون، العدد الثاني، ديسمبر 2012، (ص ص 01-07). محمول من الموقع الإلكتروني التالي: http://taza2005.e-monsite.com/medias/files/tasarrob.pdf،

13. **علي احمد البسيوني**، "الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية"، مجلة الفكر الشرطي، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، دولة الإمارات العربية المتحدة، المجلد الحادي والعشرون، العدد 81، 2012،(ص ص 48-61).

14. **علي أحمد الفرجاني**، "جريمة القرصنة المعلوماتية دراسة مقارنة بين الجانبين الموضوعي والإجرائي"، مجلة التشريع والقضاء، تصدر عن مجلس القضاء الأعلى، بغداد، العدد السابع، أكتوبر 2005، (ص ص 12-21).

15. **علي حسن طوالبه**، "مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي دراسة مقارنة"، مقال مقدم إلى مركز الإعلام الأمني، البحرين، 2009، (ص ص 01-20)محمول من الموقع الإلكتروني التالي: http://www.policemc.gov.bh/mcms-store/pdf/K

16. ----------، "التعاون القضائي الدولي في مجال مكافحة الجرائم الإلكترونية"، (ص ص 01-37)، محمول من الموقع الإلكتروني التالي: https://www.policemc.gov.bh/mcms-store/pdf

17. **علي محمد رحومة**، "المجتمع الآلي"، سلسلة عالم المعرفة، تصدر عن المجلس الوطني للثقافة والفنون والآداب في الكويت، عدد يناير 2008،(ص ص 61-79).

18. **فاضل نصر الله عوض**، "الطبيعة القانونية للاستيلاء على الأموال من البنك الآلي"، مجلة كلية الحقوق الكويتية، تصدر عن كلية الحقوق، جامعة الكويت، العدد 122،، مارس 1988،(ص ص 283-291).

19. **محمد الأمين البشري**، "التحقيق في الجرائم الحاسب الآلي"، المجلة العربية للدراسات الأمنية والتدريب، تصدر عن جامعة نايف العربية للعلوم الأمنية، الرياض، العدد الثلاثون، نوفمبر 2000،(ص ص 350-365).

20. ----------، "الأدلة الجنائية الرقمية، مفهومها ودورها في الإثبات"، المجلة العربية للدراسات الأمنية والتدريب، تصدر عن جامعة نايف العربية للعلوم الأمنية، الرياض، المجلد 17، العدد 33، أبريل 2002، الرياض،(ص ص 122-134).

21. **محمد علي السالم عياد الحلبي**، "حرية القاضي الجنائي في الاقتناع في قوانين مصر، الأردن والكويت"، مجلة الحقوق الكويتية، تصدر عن كلية الحقوق، جامعة الكويت، العدد الثالث، السنة الحادية والثلاثون، سبتمبر 2007،(ص ص 369-381).

22. **محمد فؤاد الصاوي**، "جرائم الأنترنت"، (ص ص01 -10)، محمول من الموقع الإلكتروني التالي:http://www.startimes.com/?t=33677893

23. **محروس نصار غايب**، "الجريمة المعلوماتية"،(ص ص 01-25)، محمول من الموقع الإلكتروني التالي:
https://www.iasj.net/iasj?func=fulltext&aId=28397

24. **محمد ابراهيم زيد**، "الجوانب التاريخية والعلمية لاستخدام للوسائل الفنية الحديثة"، المجلة الجنائية القومية، تصدر عن المركز القومي للبحوث الاجتماعية والجنائية، القاهرة، المجلد العاشر، العدد الثالث، نوفمبر 1967،(ص ص 45-61).

25. **مراد ماموش،** "الجهود الدولية لمكافحة الإجرام السبراني"، مجلة القانون والأعمال، كلية الحقوق، جامعة غرداية، (ص ص 01-26)، محمول من الموقع الإلكتروني التالي: http://www.droitetentreprise.com

26. **مسعود كبها،** "اختراق "hacking team"،(ص ص 01) محمول من الموقع الإلكتروني التالي: http://www.arageek.com/tech/2015/07/11/hacking-team-hack.html

27. **معتصم خميس مشعشع،** "إثبات الجريمة بالأدلة العلمية"، مجلة الشريعة والقانون، تصدر عن مجلس النشر العلمي، كلية القانون، جامعة الإمارات العربية المتحدة، عدد56، أكتوبر 2013،(ص ص 01-22).

28. **منية غانمي،** "الجزائر.. هكذا يقود "الحوت الأزرق" الأطفال إلى الانتحار"، مجلة العربية.نت، 11ديسمبر2017، (ص ص 01) محمول من الموقع الإلكتروني التالي:https://www.alarabiya.net/ar/north-africa/2017/12/1/

29. **نبيل إسماعيل عمر،** "قاعدة عدم القضاء بعلم الشخص للقاضي في الشريعة الإسلامية والقانون الوضعي"، مجلة الدفاع الاجتماعي، تصدر عن المنظمة العربية للدفاع الاجتماعي ضد الجريمة الرباط، المغرب، العدد الأول، 1984،(ص ص41-57).

30. **هشام محمد فريد رستم،** "الجرائم المعلوماتية أصول التحقيق الجنائي الفني والية التدريب التخصصي للمحققين"، مجلة الأمن والقانون، تصدر عن أكاديمية شرطة دبي، دولة الإمارات العربية المتحدة، السنة الرابعة، العدد الثاني، يوليو 1999،(ص ص22-34).

31. مقال منشور في مجلة السلام، "المصلحة المركزية للجريمة الإلكترونية في مواجهة مجرمي العالم الافتراضي"،13/02/2016 ،(ص ص 01)محمول من الموقع

الإلكتروني التالي:
http://www.essalamonline.com/ara/permalink/52564.html
32. مقال منشور في مجلة الحرية، (ص ص01)محمول من الموقع الإلكتروني: http://horrya.net/2016/07/09 .

ج- المداخلات:

1. **أبو المعالي محمد عيسى،** "الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية"، ورقة عمل المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، الفترة بين 28-29 أكتوبر 2009.
2. **راشد بن حمد البلوشي،** "الدليل في الجريمة المعلوماتية"، ورقة عمل مقدمة إلى المؤتمر الدولي الأوّل حول حماية أمن المعلومات والخصوصية في قانون الأنترنت برعاية الجمعية الدولية لمكافحة الإجرام السيبري بفرنسا، القاهرة، المنعقد في الفترة 2-4 يونيو 2008.
3. **طارق محمد الجملي،** "الدليل الرقمي في الإثبات الجنائي"، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، المنعقد في الفترة 28-29أكتوبر 2009، محمول من الموقع الإلكتروني التالي:
محمول من الموقع الإلكتروني التالي: http://www.droit-dz.com/forum/threads/5952/
4. **عبد الناصر محمد محمود فرغلي وعبيد سيف سعيد المسماري،** "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة"، ورقة بحث مقدمة للمؤتمر العربي الأول لعلم الأدلة الجنائية والطب الشرعي، الرياض، المنعقد في الفترة 12 – 14 مايو 2003 .
5. **علي محمود علي حموده،** "الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي"، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية

والأمنية للعمليات الإلكترونية، مركز البحوث والدراسات، أكاديمية شرطة دبي، الإمارات العربية المتحدة، المنعقد في الفترة 26، 28 أفريل 2003.

6. **عمر محمد بن يونس،** "الدليل الرقمي"، ورقة عمل حول قانون الإجراءات عبر الأنترنت والإعلام، جامعة الدول العربية، مصر، الفترة بين 5و8 مارس2006، محمول من الموقع الإلكتروني التالي: http://unpan1.un.org/intradoc/groups/public/documents/arado/unpan026347.pdf

7. ----------، "مذكرات في الثبات الجنائي عبر الأنترنت "، ندوة الدليل الرقمي، جامعة الدول العربية، القاهرة، الفترة بين 5 – 8 مارس 2006

8. **محمد أبو العلا عقيدة،** "التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية"، ورقة عمل مقدمة في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث والدراسات، أكاديمية شرطة دبي، الإمارات العربية المتحدة، المنعقد في الفترة 26 – 28 أبريل 2003.

9. **ممدوح عبد الحميد عبد المطلب،**" استخدام بروتوكول tcp/ip في بحث وتحقيق الجرائم على الحاسوب"، ورقة عمل مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث والدراسات، أكاديمية شرطة دبي، الإمارات العربية المتحدة، المنعقد في الفترة 26-28 أبريل 2003 .

10. **هشام محمد فريد رستم،** "الجرائم المعلوماتية أصول التحقيق الجنائي الفني"، بحث مقدم لمؤتمر القانون والكمبيوتر والأنترنت، كلية الشريعة والقانون، جامعة العين، دولة الإمارات العربية المتحدة في الفترة 1-3-مايو 2000، 2004.

د-النصوص القانونية:

1)- النصوص القانونية الدولية:

1. الاتفاقية المتعلقة بتسليم المجرمين والتعاون القضائي في المسائل الجنائية، الموقعة في بروكسيل في 12 يونيو 1970 بين الجمهورية الجزائرية الديموقراطية الشعبية والمملكة البلجيكية، صادقت عليها الجزائر بموجب امر رقم 70-61 مؤرخ في 8 شعبان 1390الموافق ل 8 أكتوبر 1970، الجريدة الرسمية للجمهورية الجزائرية عدد 92، بتاريخ 3 نوفمبر 1970.
2. اتفاقية الأمم المتحدة لمكافحة الإتجار غير المشروع بالمخدرات والمؤثرات العقلية الموافق عليها في فيينا بتاريخ 20 ديسمبر 1988، صادقت عليها الجزائر بموجب مرسوم تشريعي رقم 94-02 ممضي في 05 مارس 1994،، يتضمن الموافقة عليها مع تحفظ، الجريدة الرسمية للجمهورية الجزائرية عدد 12 بتاريخ 06 مارس 1994 .
3. اتفاقية التعاون القضائي بين الجمهورية الجزائرية الديمقراطية الشعبية وجمهورية تركيا الموقعة بالجزائر في 14 مايو 1989، صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 2000-370 ممضي في 16 نوفمبر2000، يتضمن التصديق عليها، الجريدة الرسمية للجمهورية الجزائرية، عدد 69 بتاريخ 21 نوفمبر2000.
4. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من طرف الجمعية العامة لمنظمة الأمم المتحدة يوم 15 نوفمبر 2000، صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 02-55 ممضي في 05 فبراير 2002، يتضمن التصديق عليها بتحفظ، الجريدة الرسمية للجمهورية الجزائرية عدد 9 بتاريخ 10 فبراير 2002.

5. اتفاقية الأمم المتحدة لمكافحة الفساد، المعتمدة من قبل الجمعية العامة للأمم المتحدة بنيويورك يوم 31 اكتوبر 2003، صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 06-128 من عام 1425 الموافق ل 19 ابريل 2006، يتضمن التصديق عليها بتحفظ، الجريدة الرسمية للجمهورية الجزائرية، عدد 26، بتاريخ 25 ابريل 2006.

6. اتفاقية التعاون القانوني والقضائي في المجال الجزائي بين حكومة الجمهوريّة الجزائريّة الديمقراطيةDEL الشّعبية وحكومة دولة الكويت الموقّعة بالجزائر بتاريخ 12أكتوبر سنة 2010، المصادق عليها بموجب مرسوم رئاسيّ رقم 15-255 مؤرّخ في 21 ذي الحجة عام 1436الموافق 5 أكتوبر 2015، الجريدة الرسمية للجمهورية الجزائرية، عدد 53 بتاريخ 8 أكتوبر .2015.

2)- النصوص القانونية الوطنية:

1- الدساتير:

1. الدستور الجزائري لسنة 1996، صادر بموجب مرسوم رئاسي رقم 96-438 مؤرخ في 26 رجب 1417هـ الموافق ل 7 ديسمبر 1996 يتعلق بإصدار نص تعديل الدستور، المصادق عليه باستفتاء 28 نوفمبر 1996، الجريدة الرسمية للجمهورية الجزائرية عدد 76 بتاريخ 08 ديسمبر 1996.

2. الدستور الجزائري لسنة 2016، صادر بموجب قانون رقم 16 - 01 مؤرخ في 26 جمادى الأولى عام 1437 الموافق 6 مارس سنة 2016، يتضمن التعديل الدستوري، الجريدة الرسمية للجمهورية الجزائرية عدد 14 بتاريخ 7 مارس 2016.

2- النصوص التشريعية:

01. امر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق ل 8 جوان 1966، الذي يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية عدد 48 بتاريخ 11 جوان 1966 المعدل والمتمم.

02. امر رقم 66-156 المؤرخ في مؤرخ في 18 صفر عام 1386 الموافق ل 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية عدد 49 بتاريخ 11 جوان 1999 المعدل والمتمم.

03. امر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق ل 26 سبتمبر 1975، المتضمن قانون المدني، الجريدة الرسمية للجمهورية الجزائرية عدد 78 بتاريخ 30 سبتمبر 1975، المعدل والمتمم.

04. قانون رقم 2000-03 المؤرخ في 05 جمادي الأول عام 1421 الموافق ل 5 غشت سنة 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، الجريدة الرسمية للجمهورية الجزائرية عدد 48، بتاريخ 6 أوت 2000.

05. قانون رقم 04-15 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية عدد 71 بتاريخ 10 نوفمبر 2004.

06. قانون رقم 05-01 مؤرخ في 27 ذي الحجة 1425 الموافق 6 فبراير 2005 يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية للجمهورية الجزائرية، عدد 11 بتاريخ 9 فبراير 2005..

07. قانون رقم 05-10 المعدل ويتمم الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني الجزائري،

الجريدة الرسمية للجمهورية الجزائرية عدد 44 بتاريخ 20 يونيو 2005.

08. قانون رقم 06- 22 مؤرخ في 2 9 ذي القعدة عام 14 27 الموافق 20 ديسمبر سنة 20 06،يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية عدد 84 بتاريخ 24 ديسمبر 2006.

09. قانون رقم 06- 23 مؤرخ في 29 ذي القعدة عام27 14الموافق 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية عدد 84 بتاريخ 24 ديسمبر 2006.

10. قانون رقم 09- 04 مؤرّخ في 14 شعبان عام 1430 هـ الموافق 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية عدد 47 بتاريخ 16 غشت 2009.

11. قانون رقم 14-01 مؤرخ في 4 ربيع الثاني عام 1435 الموافق 4 فبراير 2014، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو 1966 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية عدد 07 بتاريخ 16 فبراير 2014.

12. أمر رقم 15-02 مؤرخ في 7 شوّال عام 1436 الموافق 23يوليو سنة r2015 يعدل ويتمم الأمر رقم 155-66المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية عدد 40 بتاريخ 23 يوليو 2015.

13. قانون رقم 16-02 مؤرخ في 14 رمضان عام 1437هـ الموافق ل19 سنة 2016 يتمم الأمر رقم 156-66المؤرخ في 18 صفر عام 1386هـ الموافق 8 يونيو سنة 1966 تضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية عدد 37 بتاريخ 22 يونيو 2016.

14. قانون رقم 17-07 مؤرخ في 28 جمادى الثاني لعام 1438 الموافق 27 مارس سنة 2017يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8يونيو سنة 1966 والمتضمن قانون لإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية عدد 20 بتاريخ 29 مارس 2017.

3- **النصوص التنظيمية:**

1.مرسوم رئاسي رقم 15-261 مؤرّخ في 24 ذي الحجة عام 1436الموافق 8 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، الجريدة الرسمية للجمهورية الجزائرية عدد 53 بتاريخ 08 أكتوبر 2015.

2.مرسوم تنفيذي رقم 06- 348 مؤرّخ في 12 رمضان عام 1427الموافق 5 أكتوبر سنة 2006 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهوريـ الجمهورية وقضاة التحقيق، الجريدة الرسمية للجمهورية الجزائرية عدد 63 بتاريخ 08 أكتوبر 2006.

3.مرسوم تنفيذي رقم 17-96 مؤرخ في 29 جمادى الأولى عام 1438 هـ الموافق 26 فبراير سنة 2017 يتضمن تنظيم الإدارة المركزية لوزارة البريد وتكنولوجيات الإعلام والاتصال، الجريدة الرسمية للجمهورية الجزائرية عدد 14 بتاريخ 1 مارس2017.

4-القرارات **المحكمة العليا:**

1. المحكمة العليا، غرفة الجنح والمخالفات، ملف رقم 059100، بتاريخ 1989/07/02، المجلة القضائية، العدد الثالث، 1991.

ثانيا: باللغات الأجنبية

I. Ouvrages :

a- Ouvrages en langue Française:

1. **André BERTRAND Thierry PIETTE-COUDOL** , Que sais-je ? Internet et le droit? P.U.F,Paris,2000
2. **David FOREST et Gautier KAUFMAN**, Droit de l'informatique, Galino Lextenso éditions, Paris, 2010.
3. **Dominique LALOUX**, Les virus informatiques, Morabout Alleur, Belgique, 1989.
4. **Georges BRIERE DE I'ISLE**, Procédure pénale tome 2, Adèle Colin, Paris, 1971.
5. **Jan Hruska J.C. Hoff M. Ginguay**, Virus informatiques et lutte anti-virus, Masson, Paris, 1992.
6. **Michel VIVANT et Christian LE STANC**, Informatique et droit pénal ; Les biens informatiques objets de fraude ,Lamy Informatique et Réseau ,Paris, 2002.
7. **Myriam QUEMENER,** Cybercriminalité défi mondial et réponses, Economica, Paris, 2007
8. **Pierre MATHELOT**, La télématique, que sais-je?, 3ème édition, PUF, Paris, 1995.
9. **Serge GUINCHARD, Jacques BUISSON**, Procédure pénale, Litec, 2ème édition, Paris, 2002.

b-Ouvrages en langue Anglaise :

1. **Adam C ENGST**, Internet starter Kit for Macintosh, 4th Edition, Hayden Books, U.S.A, 1996, in; http://vintageapple.org/macbooks/pdf/Internet_Starter_Kit_for_the_Macintosh_4th_Edition_1996.pdf. consulté le 22/10/2016.

2.**Marshall H JARRETT , Michael W BAILIE**, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Published by Office of Legal Education Executive Office for United States Attorneys, third edition, 2002, in ; https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.consulté le: 5/15/22017.

3.----------, prosecution of computer crimes, Published by office of legal education executive, office for United State Attorneys, 2013. in ; https://en.org/Computer_Fraud_and_Abuse_Act consulté le : 5/12/2017.

4.**Mohamed Cherif BASSIOUNI**, International extradition; us law and practice , Third edition , Oceana Publications ,New York,1996.

5.……, The need for International accountability, International criminal law, Ardsley, new York, 1999.

6. **Parker DONN B,** fighting computer crime, published by Charles Scribner Son, New York 1983.

7. **W KRUSE, J HEISER**, computer forensics, incident response essentiels, Eddison Wesley, Boston, 2002.

II. Thèses et Mémoires :

A. **Thèses** :

1. **Djavad FOUROUTANI,** Le fardeau de la preuve en matière pénal ; essai d'une théorie générale, thèse pour obtenir le grade de docteur, Paris2, 1977.
2. **Mickael BOUTROS**, Le droit du commerce électronique, thèse de doctorat, université de Grenoble, 2014.
3. **Pascal VERGUCHI**, La répression des délits informatique dans une perspective internationale, Thèse de doctorat , Montpellier, 1996.
4. **RACHED Aly A**, De l'intime conviction du juge; vers une théorie scientifique de la preuve en matière criminelle, thèse pour obtenir le grade de docteur, Paris, Pedone, 1942.
5. **Stéphane CLÉMENT**, les droits de la défense dans le procès pénal ; du principe du contradictoire à l'égalité des armes, thèse pour obtenir le grade de docteur, faculté de droit et de sciences politiques, université de Nantes, 2007.

B- **MEMOIRES :**

1. **Arnaud NIKIEMA Koulika**, La preuve dans le contentieux du cyberespace, mémoire de recherche droit du cyberespace africain, université Berger de saint Louis, Sénégal, 2010/2011.

2. **Emmanuelle MATIGNON**, la cybercriminalité ;Un focus dans le monde des télécoms, mémoire Master droit du numérique administrations, école de droit de la Sorbonne, université Paris 1 Panthéon ,Sorbonne, Paris , 2012.
3. **John Wilson RANDRIAMAHFLY**, De l'évolution de la cybercriminalité, mémoire de maîtrise, université de Toliara, Madagascar, 2010.

III. Articles :

a. Articles en langue Française :

1. **Alain STROWEL, Nicolas Ide**, « Responsabilité des intermédiaires actualités : législatives et jurisprudentielles », revue Droit et Nouvelles Technologies, 10/10/2000,pp 01-44, in ; https://www.droit-technologie.org/wp-content/uploads/2016/11/annexes/dossier/26-1.pdf.
2. **Bernard AMOURY et Yves POULLET**, « le droit de la preuve face à l'informatique et télématique », RIDP, Avril – juin 1985,pp331-352.
3. **LegiGlobe,** « Cybercriminalité (br, cn, es, us, nl, uk) », p p, 01-38, in ; http://legiglobe.rf2d.org/cybercriminalite-2/2013/09/05/.
4. **GARCIA Marylou et Max CHOUZIER**, « La preuve informatiques : Quelles nouveautés techniques pour quelles évolutions juridiques », Revue Lexbase, édition affaires N° 280 du 18 Janvier 2012, pp 1-6 ,in ; http://www.adij.fr/wp-content/uploads/2012/01/CompteRendu_PreuveInformatique.pdf.
5. **Henri LECLERC**, « L'intime conviction du juge, norme démocratique de la preuve », pp206-213, in ; https://www.u-

picardie.fr/curapp-revues/root/35/henri_leclerc.pdf_4a081ebec92b4/henri_leclerc.pdf

6. **Jacques BUISSON**, « Captation d'images, application du principe de la légalité dans l'administration de la preuve », R.S.C, 2008, pp 655-692.
7. **Jacques FRANCILLON**, « Les crimes informatiques et d'autre crimes dans le domaine de la technologie informatique en France », RIDP, v 64, 1er et 2ème trim., 1993, pp291-317.
8. **Jean Claude PATIN**, « la surveillance des courriers électroniques par l'employeur », revue du droit des technologie de l'information, 1999,pp01-4, in ; lthoumyre.chez.com/pro/1/priv19990810.htm.
9. **Jean François RENUCCI**, « la loyauté dans la reconnaissance de la preuve », RSC, 2007, pp 895-923.
10. **Jean LAMARQUE**, « la responsabilité pénale de l'expert », RSC, 1976,p p.7 -24.
11. **Jean Louis HALPERIN**, « La preuve judiciaire et la liberté du juge », revue communication, 2009,pp 21-32.
12. **Jean Yves CHEVALLIER**, « Rapport de Synthèse sur la preuve dans les pays de l'Europe continentale, La preuve en procédure pénale comparées, association internationale de droit Pénal », RIDP,1992,pp 41-52.
13. **John SPENCER**, « La preuve en procédure pénale, droit anglais », RIDP, vol 63, 1er et 2ème trim., 1992, p p83-103.
14. **L Nadine, C THWAITES** , « Eurojust, autre brique dans l'édifice de la coopération judiciaire en matière pénale », RSC, janvier, 2003, pp 38-51.

15. **Louis Edmond PETTITI**, « Les écoutes téléphoniques et la protection de la vie privée », RSC ,1998, pp82-839.
16. **Marie BAREL,** « Fraude informatique et preuve : la quadrature du cercle ? » ,p p 01-14, in ; http://sondage.sstic.org/SSTIC05/Delits_informatiques_et_preuve/SSTIC05-article-Barel-Delits_informatiques_et_preuve.pdf.
17. **PATIN Jean Claude**, « la surveillance des courriers électroniques par l'employeur » ,pp 1-1, in ; http://lthoumyre.chez.com/pro/1/priv19990810.htm.
18. **Peter HUNERFELD**, « Le Droit ALLEMAND La preuve en procédure pénale », RIDP, V 63, 1er et 2ème trim., 1992, pp57-81.
19. **Robert BADINTER**, « Le droit de l'écoute électronique en droit français », pp16-28, in ;https://www.u-picardie.fr/curapp-revues/root/1/badinter.pdf .
20. **Sahir ERMAN**, « Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Turquie », RIDP, v 64, 1er et 2ème trim., 1993, pp 617-625.
21. **Sassi BEN HALIMA**, « Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Tunisie », RIPD, v64, 1er et 2ème trim.,1993, pp609-615.
22. **Stephen J, Frunk SCHULHOFER, J BERNOCO, Berg GREEN**, Rapport de Synthèse pour les pays de « common Law », La preuve en procédure pénale comparée, association internationale de droit pénal, RIDP 1992, pp 39-52.

23. Yannick MENECEUR , « Justice et nouvelles technologies », revue les cahiers dynamiques 2010, pp102-109, in ; https://www.cairn.info/revue-les-cahiers-dynamiques-2010-2-page-102.htm

b**. articles en langue Anglaise** :

1. **Anderson MALCOM**, "Policing the world Interpol the Politics of International Police Co- Operation" , Clarendon press. Oxford, 1989, pp 168-185.
2. **Cathy T.H. CHEN, Kai-Yuan Cheng, Sih-Yan LiN**, « The Exploration of the Judge's Evaluation of Evidence through Inner Conviction on Whether Internet Messages Can be Evidence for Adultery in the Criminal Law---An Explication by Legal Positivism and Philosophical Theory », International Journal of Cyber Society and Education, June 2009 ,pp1-20,in ; http://www.academic-pub.org/ojs/index.php/IJCSE/article/view/498.
3. **Christopher BLAKESLEY**, "The law of International extradition, A comparative study",RIDP, pp 381-407.
4. **Patrick S CHEN**, "An automatic system for collection crime information on the Internet" , Journal of information law and technology, 31 October 2000, pp 06,in; https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/chen/.
5. **Susan BRENNER et Fred ERICKSON**, "computer searches and seizures, some unresolved, issues", pp01-01 in; http://www.mttlr.org/voleight/Brenner.pdf
6. **Susan BRENNER**, « Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law », Murdoch University

Electronic Journal of Law, June 2001, in ; http://www5.austlii.edu.au/au/journals/MurUEJL/2001/8.html .

7. **Tiffany CURTISS**, Computer fraud and abuse act enforcemen : cruel, unusual and due for reform, pp 01-30, in ; https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1643/91wlr1813.pdf?sequence=3&isAllowed=y.

IV. Colloques et congrès :

a. Colloques :

1. **Jean Pradel**, Les rôles respectifs du juge et du technicien dans l'administration de la preuve en matière pénale, 10ème Colloque des Instituts d'études judiciaires, Poitiers, Paris ,1975.
2. **Compagnie Nationale des experts de justice en Informatique et Techniques Associées CNEJITA**, La preuve numérique à l'épreuve du litige, colloque du 13 Avril 2010 à la première chambre de la cour d'appel de Paris, in ; http://www.lagbd.org/index.php/La_preuve_num%C3%A9rique_%C3%A0_l%27%C3%A9preuve_du_litige_(fr),
3. **George LEVASSEUR**, Le régime de la preuve en droit répressif français, in Troisième Colloque du Département des Droits de l'homme, La présentation de la preuve et la sauvegarde des libertés individuelles, Bruylant, Bruxelles, 1977.

b. Congrès :

1. Congres international de droit pénal, 6ème, Rome, 27 septembre- 3 octobre 1953, paragraphe 105.

2. Traité type d'entraide judiciaire en matière pénale, A/RES/45/117 68e séance plénière 14 décembre 1990, in ; https://www.unodc.org/documents/corruption/Publications/Model_Treaties_MLA_FR.pdf
3. congrès international de droit pénal, 15ème, Rio De Janeiro, Brésil , 4-10 septembre 1994, Association internationale de droit pénale, RIDP, 1er et 2ème trimestre , 1995, in ; http://www.penal.org/sites/default/files/files/RIDP_1995_1_2.pdf.
4. Traité type d'extradition, A/RES/45/116, 68ème séance plénière 14 décembre 1990, in ; https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/567/63/IMG/NR056763.pdf?OpenElement.
5. Congrès international de droit pénal, 3ème section de XVIIIème ,Istanbul du 20 au 27 Septembre 2009, in ; www.uterchtlawreview.org/article/abstract/10.18352/ulr.105/ .

V. Textes juridiques :

a. Textes juridiques internationaux :

1. -Convention relative à la procédure simplifiée d'extradition entre les États membres de l'Union européenne - Rapport explicatif, Journal officiel n° C 375 du 12.12.1996, in ; http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM:l14015a.
2. Convention inter américaine sur l'extradition. Conclue à Caracas le 25 février 1981, in ;

https://treaties.un.org/doc/Publication/UNTS/Volume%201752/volume-1752-I-30597-French.pdf..

3. Déclaration D8 des Nations Unies, Commission pour la prévention du crime et la justice pénale Rapport sur la vingt-quatrième session 5 décembre 2014 et 18-22 mai 2015, in ; https://www.legal-tools.org/doc/609e53/pdf/.

b. Textes juridiques européens :

1. Convention européenne d'extradition Paris, 13.XII.1957, in ; https://rm.coe.int/168006459c.
2. Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données , in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000697074.
3. Directive 2000/31/CE du parlement Européen et du conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») , in ; http://www.pedz.uni-mannheim.de/daten/edz-wf/gdm/00/R-2000-31-EG-FR.pdf.
4. Conseil de l'Europe ,recommandation n° R (95) 13 du comité des ministres aux états membre relative aux problèmes de procédure pénale liés à la technologie de l'information, adoptée le 11 septembre 1995 ,in ; https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1900873.

5. Conseil européen de Tampere, recommandations ,15 ET 16 OCTOBRE 1999, in ; http://www.europarl.europa.eu/summits/tam_fr.htm.

6. Convention sur la cybercriminalité, Conseil de l'Europe, signée à Budapest le 23 novembre 2001,in ; http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

c. Textes juridiques nationaux :

1) Législation allemande :

1. Strafgesetzbuch, StGB15/05/1871, in ; https://www.gesetze-im-internet.de/stgb/StGB.pdf.
2. Strafprozebordnung(stPO), in ; www.gesetze-im-internet.de/stpo/stPO.pdf.
3. Informations und Kommunikations dienste Gesetz, in ; http://www.bibliotheksverband.de/fileadmin/user_upload/Kommissionen/Kom_Recht/Publikationen_Allgemeines/1997_09_Informations-und_KommunikationsdiensteGesetz.pdf .

2) Législation Belge :

-Code d'instruction criminelle Belge ,in ; http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1808111730&table_name=loi.

3) Législation Canadienne :

-Loi concernant le droit criminel, L.R.C ,1985,ch.c-46, in ;law-loi.justice.g.c.ca/pdf/c-46.pdf.

4) Législation Anglaise :

1. Police and criminal evidence Act 1984, in ; http://www.legislation.gov.uk/ukpga/1984/60/pdfs/ukpga_19840060_en.pdf.

2. Computer Misuse Act 1990 , in ;
http://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf.
3. The Electronic Commerce Directive Regulations 2002,in ;
http://www.legislation.gov.uk/uksi/2002/2013/pdfs/uksi_20022013_en.pdf.
4. The penal code and Subsidiary Legislation in *England* , Revised Edition showing the law as at 1 January 2008,in ;
http://agc.gov.ms/wp-content/uploads/2010/02/penal_code.pdf.

5) Législation Française :

- **Lois :**

1. le Code pénal Français du 1810, in ;
http://www.koeblergerhard.de/Fontes/CodePenal1810.htm .
2. code pénal français, in ;
https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 .
3. Code de Procédure Pénale Français,
in ; http://codes.droit.org/CodV3/procedure_penale.pdf.
4. code civil Français, in ;
https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070721.
5. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, in ;
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460.

6. Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000875419.
7. Loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000533747.
8. Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000173519.
9. Loi n°92-1336 du 16 décembre 1992 - art. 11 JORF 23 décembre 1992 en vigueur le 1er mars 1994, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000177662.
10. Loi n° 92-1446 du 31 décembre 1992 relative à l'emploi, au développement du travail à temps partiel et à l'assurance chômage, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000542542.
11. Loi n° 93-1013 du 24 août 1993 en vigueur le 2 septembre 1993, modifiant la loi n° 93-2 du 4 janvier 1993 portant réforme de la procédure pénale (rectificatif), in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000732008&dateTexte=.
12. Loi n° 99-515 du 23 juin 1999 renforçant l'efficacité de la procédure pénale - art. 12 JORF 24 juin 1999, in ;

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005628093.

13. Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005629200.
14. Loi n° 2000-516 du 15 juin 2000 renforçant la protection de la présomption d'innocence et les droits des victimes, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000765204.
15. Loi n° 2000-719 du 1 août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication,in ;https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000402408
16. Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne,in ;https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052.
17. Loi n° 2003-329 du 18 mars 2003 pour la sécurité intérieure, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000412199.
18. Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000249995.
19. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, in ;

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164.

20. Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000454124

21. Loi n° 2007-291 du 5 mars 2007 tendant à renforcer l'équilibre de la procédure pénale, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000271253&dateTexte.

22. Loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000615568.

23. Loi du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet (HADOPI I), in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432&categorieLien=id.

24. Loi du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet, dite (HADOPI II),in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021208046&categorieLien=id.

25. Loi n° 2011-267, du 14 Mars 2011, dire d'orientation de programmation pour la performance de la sécurité intérieure L'OPSI 2, à légalité la hacking au détour des disposition de l'article 706-102-1 du code de procédure pénale, in ;

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&categorieLien=id

26. Loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032627231.

- **Décret :**

1. Décret n° 2007-29 du 5 janvier 2007 relatif au service universel postal et aux droits et obligations de La Poste et modifiant le code des postes et des communications électroniques, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000646118.
2. Décret n°92-1358 du 28 décembre 1992 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie, in ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000543201&categorieLien=id.
3. Circulaire française du 17 février 1988 prise en application de l'article 43 de loi 86-1067 du 30 septembre 1986 relative a la liberté de communication concernant le régime déclaratif applicable a certains services de communication audivisuelle jorf du 09 mars 1988 .

6) Législation Grecque:

- Code of penal procedure greece ,in ;
  https://www.unodc.org/res/cld/document/grc/penal_code_excerpts_html/Greece_Criminal_Code_Excerpts.pdf.

7) Législation Américaine:

a-Federal act:

1. The Constitution of the United States (1787–1992),
   in ;https://www.encyclopediavirginia.org/The_Constitution_of_the_United_States_1787-1992
2. United States Code,
   Title 18 , Crimes and criminal procedure, in ; https://www.unodc.org/res/cld/document/usa/1948/u_s__code_-_title_18_html/US_Code_Title_18.pdf.
3. Federal Rules of Evidence ,1975, in : www.uscourt-gov/sites/default/Rules%20of20%Evidence
4. Public law 98-473—OCT. 12, 1984 Chapiter XXI—Access devices and computers , in ; https://www.gpo.gov/fdsys/pkg/STATUTE-98/pdf/STATUTE-98-Pg1837.pdf.
5. Computer Fraud and Abuse Act section 1.short title. of 1986, in ; https://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1213.pdf.
6. Police and Criminal Evidence Act 1984 , in ;
   http://www.legislation.gov.uk/ukpga/1984/60/pdfs/ukpga_19840060_en.pdf.

7. Electronic Communications Privacy Act of 1986" ,in ;
https://www.loc.gov/law/opportunities/PDFs/ElectronicCommunicationsPrivacyAct-PL199-508.pdf .

8. Criminal Justice Act 1988, in ;
https://www.legislation.gov.uk/ukpga/1988/33/section/27.

9. Government paper work elimination act, octobre1998 , in ;
https://ocio.nih.gov/ITGovPolicy/Documents/Paperwork_Elimination_Act_Public_Law_105-277.pdf.

10. The Electronic Commerce Directive Regulations 2002,in ;
http://www.legislation.gov.uk/uksi/2002/2013/pdfs/uksi_20022013_en.pdf

11. The Canspam Act of 2003, Sec.4 §1037,in ;
https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf.

12. Online Copyright Infringement Liability Limitation Act, U.S. Code , Title 17 , Chapter 5 , § 51, in ;
https://www.law.cornell.edu/uscode/text/17/512.

b- States codes :

13. Code AMN. §5-41-108 (2000) ,in ;
https://law.justia.com/codes/arkansas/2010/title-5/subtitle-4/chapter-41/subchapter-1/5-41-108/

14. State of California evidence code, , in ;
http://www.clrc.ca.gov/pub/Printed-Reports/Pub064.pdf

15. Iowa Code ?https://www.law.cornell.edu/cfr/text/12/715.8

VI. Documents :

1. Agence Nationale de la sécurité des ssystèmes d'iinformation (ANSSI) , « la stratégie de la France en matière de défense et de sécurité des systèmes d'information », pp 01-02, in ; https://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite-2/. consulté le : 01/02/2016.
2. .Envoyé spécial 2014 , « le côté obscur du Net Darknet », Reportage complet ,in ; https://www.youtube.com/watch?v=AERRgC-GIuM.consulté le :17/11/2014.
3. UNODC/CCPCJ/EG, 25-28 février 2013 ,Vienne, pp 01-18, in ; https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_F.pdf. consulté le: 27/07/2015.

VII. LA JURISPRUDENCE :

a- La jurisprudence en langue Française :

- Cass crim. 31 Oct. 1957, D. 1958, Som. 27.Cass crim. 12 mars 1957, D. 1957, Som. 87, in; www.persee.fr/doc/afdi_00663085_1957_num_3_1_1354 .
- Cass. Crim. 28 nov. 2001,n° 01-86.467, in; www.legifrance.gouve.fr/affichJuriJudi.do?idtext=JURITEXT000007068863.

- La jurisprudence en langue anglaise:

- USA. V. Whitaker, 127F. 3d, 595 ,602 (7th, cir 1997), in ; https://www.leagle.com/decision/1997722127f3d5951655.consulté le: 23/04/2016.

- Vs. Rossi Town of Pelham 35f.supp.(D.N.H 1997)2d 58 65-66,in; https://www.gpo.gov/fdsys/pkg/uscourts-paed-2_06-cv-05315/pd//-consulté le:23/04/2016
- Vs. United States 206 f.3d 392 (4th cir 2000) Simon ,in; caselaw.findlaw.com/us-4th-circuit1452089.html.consulté le: 23/04/2016

VIII. Les sites d'internet :

http://www.usdoj.gov/criminal/cyberdrime/s&smanuel2002.htm consulté le: 30/06/2017

- http://www.juriscom.net/ variations/responsabilité des intermediaries techniques en USA.html . consulté le 23/06/2014
- http://e-lawresources.co.uk/Robbery.php.2016/02/07 تم الاطلاع عليه يوم:
- Sur la recevabilité des imprimés d'ordinateur dans les procédures pénales https://www.lccsa.org.uk/r-v-pettigrew-r-v-newark-1980/. Consulté le 29/01/2015 .
- https://www.policemc.gov.bh/mcms-store/pdf تم الاطلاع عليه يوم .2017/02/21:
- http://www.interpol.com/public/Icpo/Members/default.asb.consulté le: 23/12/2012
- https://Office_fédéral_de_police_criminelle. Consulté le 26/09/2016.

الفهرس

الفصل الثاني

إجراءات جمع الدليل الإلكتروني

الباب الثاني:

حجية الدليل الإلكتروني في الإثبات الجنائي

الفصل الأول

قبول الدليل الإلكتروني

الفصل الثاني

يقينية الدليل الإلكتروني

ملخص:

إن الغاية من دراسة الدليل الإلكتروني ودوره في الإثبات الجنائي، دراسة مقارنة بين عدة تشريعات وأنظمة قانونية كالنظام اللاتيني وعلى قمته القانون الفرنسي، مع النظام الأنجلوسكسوني من خلال دراسة القانونين الأمريكي والإنجليزي اللذان يعدان من أوائل القوانين التي أيقنت بسلامة منطق الأدلة الإلكترونية في الإثبات الجنائي.

بدأت الدراسة بالبحث في ذاتية الدليل الإلكتروني والوقوف عند محله وعرض أهم إجراءات وأساليب التحقيق التقليدية والمستحدثة لجمعه، ثم التطرق إلى حجية الدليل الإلكتروني في الإثبات الجنائي للإظهار قوته الاستدلالية على صدق نسبة الفعل إلى شخص معين، حيث تم تسليط الضوء على أهمية دور القاضي الجزائي في قبول هذا الدليل والاقتناع به، مع إظهار فعالية ونجاحة التعاون الدولي في هذا المجال.

Résumé:

La preuve revêt une importance particulière en matière pénale en ce qu'elle permet de démontrer l'existence d'une infraction et d'établir qui en est l'auteur.

Le juge rassemble toutes sorte de preuve nécessaire à la manifestation de la vérité, il se base aussi sur des preuves apportées par les parties qui peuvent faire appel à n'importe quel moyen de preuve sans qu'il ait de hiérarchie dans leurs valeurs probantes : c'est le principe de la liberté des preuves.

La généralisation des outils informatiques et numériques a conduit à l'apparition de nouvelles infractions (cybercriminalité), afin d'être en adéquation avec ce nouvel environnement, le droit pénal a du s'adapter au monde numérique, ainsi le principe de la liberté de preuve.

Cependant la question de la force probante des preuves informatiques est actuellement un sujet extrêmement préoccupant.