جامعة دمشق
كلية الحقوق

# مشروعية الدليل الإلكتروني في الإثبات الجزائي

## دراســـة مقـارنـــة

# La légalité de la preuve éléctronique en preuve pénale

## *''Étude comparée''*

بحث علمي قانوني أُعدَّ لنيل درجة الدكتوراه في القانون الجزائي

إعداد

**عيسى غازي الذيب**

إشراف

**الدكتورة بارعة القدسي**

الأستاذة في قسم القانون الجزائي

١٤٤١هـ - ٢٠١٩م

**استناداً إلى قرار مجلس البحث العلمي والدراسات العليا رقم /٣١٩٣/ م.ب.د تاريخ ٢٠١٩/٦/١٠ القاضي بتشكيل لجنة الحكم لمناقشة رسالة الدكتوراه في القانون الجزائي للطالب:**

**عيسى غازي الذيب**

**بعنوان:**

**"مشروعية الدليل الإلكتروني في الإثبات الجزائي- دراسة مقارنة"**

**والمؤلفة من السادة الأساتذة:**

**- الدكتورة "بارعة القدسي" (عضواً مشرفاً)**

**الأستاذ في قسم القانون الجزائي بكلية الحقوق/جامعة دمشق.**

**- الدكتور "عبد القادر هباش" (عضواً)**

**الأستاذ في قسم القانون الجزائي بكلية الحقوق/ جامعة حلب.**

**- الدكتور "عبد الجبار الحنيص" (عضواً) الأستاذ في قسم القانون الجزائي بكلية الحقوق/ جامعة دمشق.**

**- الدكتور "عيسى المخول" (عضواً)**

**الأستاذ المساعد في قسم القانون الجزائي بكلية الحقوق/جامعة دمشق.**

**- الدكتور "تميم ميكائيل" (عضواً)**

**الأستاذ المساعد في قسم القانون الجزائي بكلية الحقوق/جامعة دمشق.**

**تمت المناقشة يوم الخميس الواقع في ٢٠١٩/٩/١٩م في تمام الساعة العاشرة صباحاً.**

# قائمة الاختصارات

## أولاً: باللغة العربية:

| | |
|---|---|
| ج: جزء. | د. ط: دون طبعة |
| ص: صفحة. | د. د. ن: دون دار نشر |

## ثانياً: باللغة الفرنسية:

| | |
|---|---|
| Art. Article | Vol. Volume |
| Éd. Edition | D. Dalloz |
| N. Numéro | S. Sirey |
| Op. cit. Ouvrage Précédent Cité. | P.U.F. Pressses Universaires de France |
| Cass. Crim. Cour de Cassation, Chambre Criminelle | PP. Pag |

## ثالثاً: باللغة الانكليزية:

| | |
|---|---|
| P. page. | Vol: Voulume |

﴿ يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَدۡخُلُواْ بُيُوتًا غَيۡرَ
بُيُوتِكُمۡ حَتَّىٰ تَسۡتَأۡنِسُواْ وَتُسَلِّمُواْ عَلَىٰٓ أَهۡلِهَاۚ
ذَٰلِكُمۡ خَيۡرٞ لَّكُمۡ لَعَلَّكُمۡ تَذَكَّرُونَ ﴾

(النور:٢٧)

# الإهداء

إلى منبع العطف والرحمة والتضحية والحب في أعلى الدرجات عرفاناً وتقديراً .....

**والدتي والدي**

إلى رياحين حياتي في الشدة والرخاء وأقرب الخلق لقلبي.....

**أخواتي وأخوتي**

إلى من سكن قلبي وملأ حياتي فرحة وسرور....

**ولاء**

إلى كل هؤلاء أهدي ثمرة جهدي

# الشكر والتقدير

لا يسعني بعد إتمام هذا البحث إلا أن أحمد الله تعالى وأشكره على فضله ومنته الواسعة والذي منحني القوة والصبر لإنجاز هذا البحث.

كما لا يسعني إلا أن أتقدم بخالص الشكر الجزيل والتقدير الكبير إلى الأستاذة الفاضلة **الدكتورة بارعة القدسي** للجهد الذي بذلته للإشراف على هذا البحث وتحملها عبء قراءته ومراجعته والتي أغنته بملاحظاتها القيمة، فلها مني كل الامتنان والعرفان.

كما أتقدم بجزيل الشكر والتقدير لكل من الأساتذة:

- **الدكتور عبد الجبار الحنيص** الأستاذ في قسم القانون الجزائي في كلية الحقوق- جامعة دمشق.

- **الدكتور عبد القادر هباش** الأستاذ في قسم القانون الجزائي في كلية الحقوق- جامعة حلب.

- **الدكتور عيسى المخول** الأستاذ المساعد في قسم القانون الجزائي في كلية الحقوق- جامعة دمشق.

- **الدكتور تميم ميكائيل** الأستاذ المساعد في قسم القانون الجزائي في كلية الحقوق- جامعة دمشق.

لتفضلهم بالمشاركة في لجنة الحكم لتحكيم هذه الرسالة ...

فلهم مني خالص الشكر والتقدير. . .

وأخيراً إلى عمادة كلية الحقوق وجميع أعضاء الهيئة التدريسية في كلية الحقوق في جامعة دمشق، فلهم جميعاً جزيل الشكر والعرفان وجزاهم الله عني كل الخير.

# المقدمة
# Introduction

مما لا شك فيه أن نظرية الإثبات هي الأساس الذي تقوم عليه قواعد الأصول الجزائية منذ لحظة وقوع الجريمة إلى حين صدور الحكم فيها من السلطة القضائية، بموجب السلطات الممنوحة لها.

وقد طرأ على الإثبات الجزائي تطورات كبيرة بفضل الطفرة العلمية الهائلة التي نتج عنها تطور وسائل ارتكاب الجرائم والتي لم تكن معروفة من قبل. فبعد أن كان السلوك الإجرامي في المجتمعات القديمة يتسم بالبساطة حيث يكفي لاكتشافه وإسناده إلى صاحبه استعمال أدلة الإثبات البسيطة كالشهادة والاعتراف(١)، وإن كان اللجوء إلى هذه الأدلة لا يطمئن إليها القاضي دائماً للنطق بالإدانة(٢)، أما في هذا العصر فقد وصلت الجريمة إلى أساليب متطورة، لاستثمار المجرمين معطيات العصر وتطوره العلمي والتقني مستفيدين من التسهيلات التي تقدمها هذه التقنية التي أعطت فرصاً كثيرة لا يستهان بها في استثمارها من قبل ضعاف النفوس ومريدي الإجرام، لما تهيئه من تسهيلات، يمكن لهم بواسطتها التخطيط والتنفيذ لعملهم الإجرامي(٣).

---

(١) د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، (أجهزة الرادار، الحاسبات الآلية، البصمة الوراثية)، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، ٢٠٠١م، ص٣.

(٢) لأن الشاهد قد يتعرض للنسيان أو يخطئ أو قد يشهد زوراً، وكذلك، الاعتراف لا يعبر دائماً عن الحقيقة إذ قد يعترف الشخص عن نفسه لإبعاد التهمة عن الفاعل الحقيقي (الابن مثلاً). راجع: بهلول مليكة، دور الشرطة العلمية والتقنية في الكشف عن الجريمة، رسالة دكتوراه، كلية الحقوق، جامعة الجزائر ١، ٢٠١٣م، ص٨٣ – ٨٤.

(٣) د. محمد أحمد المنشاوي، سلطة القاضي الجنائي في تقدير الدليل الإلكتروني، مجلة الحقوق، السنة السادسة والثلاثون، العدد الثاني، الكويت، ٢٠١٢م، ص٥١٧.

فتطور التقنيات مهدالسبيل إلى بروز أشكال جديدة من الجرائم، لا سيما بعد أن ربط الحاسوب الآلي بالشبكة المعلوماتية للإنترنت حيث وجد المجرم، تقنية عالية وأساليب حديثة تساعده في ارتكاب العديد من الجرائم دون أن يترك أثراً واضحاً لتلك الجريمة، والمجرم باستغلال هذه المخترعات العلمية والأجهزة الإلكترونية وما تقدمه من وسائل متقدمة في ارتكاب العديد من الجرائم من خلال الإمكانيات الهائلة لهذه التقنيات، ويصل إلى أي مكان يرغب فيه، وإلى أعداد بشرية هائلة في نفس الوقت، فلا مكان ولا زمان يستطيع وضع حدود لهذه الشبكة(١).

وأمام هذا التطور المذهل للجريمة والمجرم، وأمام تفاقم حجم الأضرار الناجمة عنهما فإن كافة وسائل البحث والتحقيق والإثبات التقليدية تقف عاجزة عن كشفهما وعليه ولتفادي تغلب وسائل ارتكاب الجريمة على وسائل الكشف عنها ومكافحتها، حتم ذلك ضرورة إثبات هذه الجرائم فبرز إلى الوجود الدليل الإلكتروني(٢) أو الرقمي(٣) أو ما يسمى بالبينة الإلكترونية(١) الذي يُعد من الأدلة

---

(١) ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية – دراسة تأصيلية تطبيقية – رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، ٢٠١٢م، ص١.

(٢) إن إطلاق صفة إلكتروني على دليل ما تعود إلى ضرورة وجود توافق بينه، وبين بيئته، فلا وجود لدليل إلكتروني خارج بيئته الإلكترونية. هلال آمنة، الإثبات الجنائي بالدليل الإلكتروني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، ٢٠١٤ – ٢٠١٥م، ص١٢.

(٣) ترجع تسمية الدليل الرقمي" كترجمة لمصطلح إلكتروني" إلى أن البيانات داخل الوسط الافتراضي سواء كان تصويراً أو تسجيلات أو نصوص تأخذ شكل أرقام على هيئة الرقمين (1 أو 0) ويتم تحويل هذه الأرقام عند عرضها لتكون في شكل صورة أو مستند أو تسجيل. د. هدى طلب علي، الإثبات الجنائي في جرائم الإنترنت والاختصاص القضائي بها (دراسة مقارنة)، رسالة ماجستير، كلية الحقوق، جامعة النهرين، بغداد، العراق، ٢٠١٢م، ص١١٤ – ١١٥. وانظر: أ. طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، مجلة الحقوق، المجلد الثاني عشر، العدد الأول، جامعة بنغازي، ليبيا، ص٤٤.

الجزائية المستحدثة في نطاق الإثبات الجزائي، والذي جاء بغرض التصدي لنوع مستحدث من الجرائم، ألا وهي الجرائم الإلكترونية[٢].

**وتاريخياً**، لحق ظهور الدليل الإلكتروني باعتباره نوع جديد على نظم العدالة الجزائية دليل الحمض النووي[٣]، وهناك من ربط ظهور الدليل الإلكتروني بظهور الجريمة الإلكترونية بغرض إثباتها[٤].وكانت الولايات المتحدة الأمريكية من السباقين الذين تطرقوا لموضوع الدليل الإلكتروني، فالولايات المتحدة الأمريكية تُعد

---

وقد يعتقد البعض أن مصطلح الجريمة الرقمية أو الدليل الرقمي يعني أن موضوعهما هو الأرقام، أو ينصب على الأرقام، وهو ما يجافي حقيقة هذا المصطلح فهذا المصطلح التقني يرجع أصله إلى استخدام النظام الرقمي الثنائي (٠،١) وهي الصيغة التي تسجل بها كل البيانات (أشكال وحروف ورموز وغيرها) داخل الحاسب الآلي، حيث يمثل (0) وضع الإغلاقOff ، والواحد (1) وضع التشغيلOn ، ويمثل الرقم صفر (0) أو الرقم واحد(1) ما يعرف بالبيتBit ، ويشكل عدد 8 Bits ما يعرف بالبايت Byte. انظر: عبد الناصر محمد محمود فرغلي، د. محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٧م، ص٥.

(١) بالنسبة لإطلاق تسمية البينة الإلكترونية فإنه مسمى غير دقيق لأن تعريف البينة هي ما يبين الشيء من الدلالة الواضحة عقلية كانت أو محسوسة، فالبينة ما يبين الدعوى ويظهر المقصود وهي حجة المدعي التي يثبت بها دعواه ولما كان الدليل الإلكتروني صادراً عن أجهزة، إن جاز التعبير، وليس حجة لفظية ينطق بها المدعي كانت تسمية بينة إلكترونية تسمية غير موفقة لذلك فمن الأفضل أن نطلق عليه الدليل الإلكتروني. انظر: معمر علي إبراهيم محمد، حجية الأدلة التقنية في الجرائم الإلكترونية، رسالة دكتوراه، جامعة الرباط الوطني، كلية الدراسات العليا والبحث العلمي، السودان، ٢٠١٤م، ص٣٥.

(٢) هلال آمنة، المرجع السابق، ص٤.

(٣) د. عمر محمد بن يونس، ورقة بحثية بعنوان" الدليل الرقمي"، ٢٠٠٦م، ص٢.

(٤) هلال آمنة، المرجع السابق، ص٥.

ثاني دولة بعد السويد في إصدار القوانين الخاصة بها التي تجرم عن طريقها نوعاً مستحدثاً من الجرائم وهي الجرائم الإلكترونية[١].

## أولاً: إشكالية البحث:

يثير الدليل الإلكتروني أحد أهم المشكلات التي تواجهها السياسية الجنائية المعاصرة، وهي كيفية تحقيق التوازن بين المصالح المتعارضة وهي مصلحة المجتمع وضمان تطبيق القانون من ناحية وضمان الحريات الفردية من ناحية أخرى، فكما أن لهذا الدليل ايجابيات كثيرة كتسهيل مهمة الكشف عن الحقيقة القضائية، فإنه قد يعصف بحريات الأفراد وحقوقهم إذا لم يحسن استخدامه، كانتهاك حرمة الحياة الخاصة للأفراد[٢]، ومعرفة أسرارهم التي يكرهون أن يطلع عليها أحد، فمن الممكن القول أن الإثبات بالدليل الإلكتروني قد يمس ضمانات قانونية هامة للأفراد مقررة في الدستور (مبدأ حق الخصوصية أو ما يطلق عليه حرمة الحياة الخاصة)، وأيضاً في القوانين الإجرائية (مبدأ حق الصمت – مبدأ النزاهة في البحث عن الدليل الجزائي) وهذه الضمانات جميعها تتعلق بمشروعية الحصول على الدليل، لا سيما أن المشرع السوري في قانون أصول المحاكمات

---

(١) ومن أهم القوانين التي أصدرتها الولايات المتحدة الأمريكية قانون تقرير الأشخاص الصادر في ١٩٧٠م، بالإضافة إلى قانون الخصوصية الصادر في ١٩٧٤/١٢/٣١م، وكذلك قانون حرية المعلومات عام ١٩٧٦م، وأيضاً قانون خصوصية الاتصالات عام ١٩٨٦م، وغيرها من القوانين، كما أن الولايات المتحدة الأمريكية قامت بإنشاء المنظمة الدولية لأدلة الحاسوب (ICOE)، ورافقتها بالفريق العامل على مستوى الأدلة الإلكترونية (SWGDE)، وهذا بغرض توحيد الجهود التي تقوم بها هذه المنظمة. هلال آمنة، المرجع السابق، ص١٧.

(٢) اعترف الإعلان العالمي لحقوق الإنسان لسنة ١٩٤٨م بالحق في الخصوصية، فتنص المادة (١٢) منه على أنه: "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات". كما أقرت الاتفاقية الأوربية لسنة ١٩٥٠ الحق في الخصوصية، فتنص المادة الثامنة على أنه: "لكل شخص الحق في أن تحترم حياته الخاصة وحياته العائلية ومسكنه ومراسلاته".

الجزائية نص على إجراءات الحصول على الأدلة التقليدية من تفتيش وخبرة وضبط ولم ينص على إجراءات الحصول على الأدلة الإلكترونية، وبالرغم من صدور قانون مكافحة الجريمة المعلوماتية السوري رقم (١٧) لعام ٢٠١٢م المسمى بـ **(قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية)**[١]، والذي نص في الفصل الرابع منه على الضابطة العدلية والدليل الرقمي إلا أنه لم يبين جميع طرق الحصول عليه ولم يحيطه بضمانات قانونية تكفل حقوق المدعى عليه، ولا سيما أنه لم يتعرض بشكل خاص للصعوبات التي تواجه الحصول عليه والتي قد تمس مبدأ المشروعية وبالتالي عدم الاعتداد به، وتفويت مصلحة المجتمع من الاستفادة منه[٢].

**من هنا تكمن إشكالية البحث الرئيسية في: مدى تحقيق نوع من التوازن بين حق الأفراد في الخصوصية والسرية في أن تبقى حقوقهم الأساسية مصانة ومحمية، وعدم المساس بها، وذلك في ضوء الضمانات الإجرائية المقررة لهم، والمبادئ المقررة في نظام الإثبات الجزائي من جهة، وحق المجتمع في مكافحة الجريمة بوسائل فعالة وذلك عن طريق الاستفادة من الدليل الإلكتروني في**

---

(١) صدر هذا القانون بتاريخ ٢٠١٢/٢/٨م، والذي أصبح نافذاً من تاريخ نشره في الجريدة الرسمية بالعدد ٧ تاريخ ٢٠١٢/٢/١٥م، وعالج هذا القانون الجرائم الإلكترونية بشقيها: الجرائم التقليدية التي تنفذ باستخدام منظومة معلوماتية، والجرائم المستحدثة التي تكون فيها المنظومة المعلوماتية أو الشبكة موضوعاً للجريمة (مثل: اختراق المنظومات المعلوماتية وتخريبها)، وقد تضمن القانون المذكور خمسة فصول وهي: الفصل الأول: تعاريف، الفصل الثاني: تنظيم التواصل على الشبكة، الفصل الثالث: مكافحة الجريمة المعلوماتية، الفصل الرابع:الضابطة العدلية والدليل الرقمي، الفصل الخامس: أحكام عامة وختامية.

(٢) وذلك بعكس قانون الشرطة والإثبات الجنائي الانكليزي لعام ١٩٨٤م الذي تم تعديله في ١٤ تشرين الأول عام ٢٠٠٢م، و الذي حدد الصلاحيات لشرطة "إنكلترا" و"ويلز"، وهو قانون يهدف إلى إقامة التوازن بين قوى الشرطة البريطانية وحقوق الأفراد، ويتناول آلية تفتيش الأماكن، وكيفية معاملة المشتبه بهم، والاعتقال وغير ذلك. د. محمد طارق الخن، الجريمة المعلوماتية، منشورات الجامعة الافتراضية، دمشق، سورية، ٢٠١٢م، ص١٢٠.

**إثبات جميع الجرائم الجزائية (التقليدية – الإلكترونية) ليعيش آمناً ومطمئناً من جهة ثانية.**

**ولا نضحي بأي من الحقين في سبيل الآخر، بمعنى آخر، بيان الحدود المسموح بها من جهة، والمحظورة والتي لا يجوز بأي حال من الأحوال تجاوزها من جهة ثانية، في الإثبات بهذا الدليل المستحدث.**

ويتفرع عن هذه الإشكالية الرئيسية عدد من الإشكالات الفرعية والتي ينتظر أن تجيب عنها هذه الأطروحة:

١- ما مدى اعتراف أنظمة الإثبات الجزائية بهذا الدليل المستحدث؟

٢- ما مدى اعتراف الاتفاقيات والفقه والقضاء والقانون السوري والمقارن بالإثبات الجزائي بالدليل الإلكتروني؟

٣- ما هي الضمانات التي يجب مراعاتها في الحصول على الدليل الإلكتروني سواء في الإجراءات التقليدية أم في الإجراءات الحديثة ليكون مشروعاً ونستطيع الاعتداد به في الإثبات الجزائي؟ ولا سيما أنه لا يوجد موقف واضح للقانون وللقضاء السوري في مجال مشروعية استخدام الدليل الإلكتروني وعدم توضيحه ضمانات مشروعيته، فكان لا بد من استعراض موقف الفقه والقضاء والقانون للدول المتقدمة ولا سيما فرنسا والولايات المتحدة الأمريكية.

٤- ما هي مؤيدات عدم مشروعية الدليل الإلكتروني سواء بالنسبة لهذا الدليل أم بالنسبة للأشخاص الحاصلين عليه؟

٥- ما هو نطاق استخدام الدليل الإلكتروني في الإثبات الجزائي؟ هل يقتصر على إثبات الجرائم الإلكترونية أم أنه يمكن الاستعانة به في إثبات الجرائم التقليدية؟

٦- هل يملك القاضي الجزائي بالنظر إلى ثقافته وتكوينه القانوني السلطة في تقدير الدليل الإلكتروني الذي قد يصل إلى اليقين؟ وما هي حدود سلطته التقديرية؟

٧- كيف يتم تقدير الدليل الإلكتروني في أنظمة الإثبات المختلفة؟ وماهو موقف التشريعات اللاتينية والأنكلوسكسونية من تقدير هذا الدليل؟ وماهو النظام الأمثل لتقدير الدليل الإلكتروني؟

## ثانياً: أسباب اختيار الموضوع:

يرجع سبب اختيارنا لهذا الموضوع للأسباب التالية:

١ – لدوافع ذاتية متعلقة بالاختصاص والتعمق في هذا الجانب باعتباره فرض نفسه بقوة في العصر الراهن لمواكبته التطور التكنولوجي الذي أنتج الجرائم الإلكترونية، حيث يربط بين الأصول الجزائية والتكنولوجيا الحديثة في مجال الإثبات الجزائي، وما يرتبط بذلك من تقرير مصائر المتهمين بين الإدانة والبراءة.

٢ – ازدياد الاهتمام الكبير الذي يحظى به الدليل الإلكتروني قياساً بغيره من الأدلة الأخرى الذي كان مرده انتشار استخدام تقنية المعلومات الرقمية.

٣ – إن مشكلة النزاهة أو المشروعية في الأدلة الجزائية قد ازدادت بوضوح نتيجة لشيوع استخدام الدليل الإلكتروني في كشف الحقيقة، فبقدر ما أحدثه هذا التقدم من تطوير في أساليب الكشف عن الجرائم وتعقب مرتكبيها، على قدر ما آثار الجدل حول مشروعية هذا الدليل المستحدث، حيث قد يمس الحريات الشخصية وينتهك حرمة الحياة الخاصة.

## ثالثاً: أهمية البحث:

تكمن أهمية البحث في أن انتشار الحاسوب قاد إلى إساءة استخدامه وإلى وجود أنواع من السلوك غير المشروع وظهور الجرائم المتعلقة بالحاسوب والإنترنت، وقد أدى ظهور هذه الجرائم إلى الإضرار بجميع نواحي الحياة الاقتصادية والاجتماعية والأخلاقية والأمنية، مما دفع أجهزة العدالة الجزائية في كافة دول العالم إلى البحث عن دليل لإثبات هذه الجرائم المستحدثة مما استتبع ظهور الدليل الإلكتروني لإثبات هذه الجرائم لصلته الوثيقة بالجرائم الإلكترونية.

كما أن موضوع الدليل الإلكتروني في الإثبات الجزائي يعد من الموضوعات الجديدة والمهمة في إطار طرق الإثبات الجزائية على مستوى قانون أصول المحاكمات الجزائية، وبالتالي يضيف إسهاماً جديداً، يحتاج إليه الدارسون والمهتمون في الإثبات الجزائي بالدليل الإلكتروني من جوانبه كافة وذلك ببيان دوره في الإثبات الجزائي.

بالإضافة إلى ذلك تظهر أهمية دراسة هذا الموضوع في مدى الاعتراف بهذا الدليل المستحدث من قبل أنظمة الإثبات والقانون والقضاء الجزائي للاستفادة منه في مجال إثبات الجرائم بشكل عام والجرائم الإلكترونية بشكل خاص.

**رابعاً: هدف البحث:**

يتمثل الهدف من هذا البحث فيما يلي:

١ – بيان أهمية الدليل الإلكتروني، وبيان مشروعية استخدامه، وإظهار أهم العقبات المتعلقة بمشروعية الحصول عليه والتي تقف حجر عثرة في الأخذ بها، وبيان كيفية معالجة مشروعية الحصول عليه في الإجراءات التقليدية والمستحدثة (الفنية) وذلك بتكريس ضمانات لحماية حقوق وحريات الفرد والتي تضمن مشروعية الدليل الإلكتروني المتحصل عليه، وكذلك ببيان جزاء عدم مشروعية هذا الدليل ومسؤولية أجهزة العدالة الجزائية التي لم تلتزم بضمانات الحصول عليه، وأخيراً كيفية تقدير الدليل الإلكتروني وحجيته في الإثبات الجزائي وذلك بعرض مواقف التشريعات المقارنة والاستفادة منها في تشريعنا السوري.

٢ – تقديم بحث تستنير به أجهزة العدالة السورية سواء في التحقيق الأولي أو الابتدائي أو في مرحلة المحاكمة، للاستعانة به في سبيل مواجهة كافة الإشكالات القانونية التي يطرحها الإثبات بالدليل الإلكتروني ولا سيما كيفية تعامل السلطات القضائية مع الدليل الإلكتروني وكذلك تكريس ضمانات الحصول على هذا الدليل.

**خامساً: صعوبات البحث:**

ترجع صعوبات هذا البحث إلى الأسباب التالية:

١ – اتسام هذا الموضوع بالصبغة العلمية الغريبة على رجل القانون، فكان لابد من الفهم الدقيق والحقيقي للمشاكل التي يثيرها استخدام الدليل الإلكتروني في الكشف عن الجريمة ومرتكبها.

٢ – افتقار المكتبة السورية والعربية إلى المراجع والأبحاث التي تعالج المشاكل القانونية الناجمة عن استخدام الدليل الإلكتروني ولا سيما مشروعيته. فمعظم هذه المراجع والأبحاث اقتصرت على وضع الأطر العامة في مجال البحث والتحقيق، بحيث يمكن الأخذ بها عند وقوع إحدى الجرائم الإلكترونية، دون أي تحديد لضمانات مشروعية الحصول على الدليل الإلكتروني وكذلك الآثار المترتبة على عدم مشروعيته، وكيفية تقديره أمام القضاء.

**سادساً: منهج البحث:**

اعتمدنا في دراسة هذا البحث على المنهجين الآتيين:

أ– **المنهج التحليلي:** وذلك بتحليل بعض النصوص القانونية في التشريع السوري والتشريعات المقارنة ومختلف الآراء التي وردت في هذا الموضوع.

ب– **المنهج المقارن:** الذي يعتمد على المقارنة بين مختلف التشريعات لعدة دول غربية وعربية بما فيها سورية، وذلك في مختلف نواحي الموضوع ولا سيما من ناحية التكريس القانوني لهذا الدليل وضمانات الحصول عليه، ومن ناحية تقدير هذا الدليل في الإثبات الجزائي.

**ثامناً: خطة البحث:**

**الباب الأول: متطلبات مشروعية الدليل الإلكتروني في الإثبات الجزائي**

**الفصل الأول: مشروعية وجود الدليل الإلكتروني.**

المبحث الأول: ماهية الدليل الإلكتروني.

المبحث الثاني: الموقف من مشروعية وجود الدليل الإلكتروني.

**الفصل الثاني: مشروعية الحصول على الدليل الإلكتروني.**

المبحث الأول: الحصول على الدليل الإلكتروني في الإجراءات التقليدية.

المبحث الثاني: مشروعية الحصول على الدليل الإلكتروني في الإجراءات الحديثة.

**الباب الثاني: الأحكام المترتبة على مشروعية الدليل الإلكتروني في الإثبات الجزائي**

**الفصل الأول: آثار مشروعية الدليل الإلكتروني في الإثبات الجزائي.**

المبحث الأول: مؤيدات عدم مشروعية إجراءات الحصول على الدليل الإلكتروني.

المبحث الثاني: نطاق العمل بالدليل الإلكتروني.

**الفصل الثاني: تقدير الدليل الإلكتروني في الإثبات الجزائي.**

المبحث الأول: حرية القاضي الجزائي في تقدير الدليل الإلكتروني.

المبحث الثاني: تقدير القاضي الجزائي للدليل الإلكتروني في أنظمة الإثبات المختلفة.

# الباب الأول

## متطلبات مشروعية الدليل الإلكتروني في الإثبات الجزائي

# الباب الأول
# متطلبات مشروعية الدليل الإلكتروني في الإثبات الجزائي

يُعد مبدأ المشروعية الجزائية من أهم المبادئ الذي يسود التشريعات الجزائية المعاصرة[١]، حيث تُعد الشرعية الجزائية أساس القانون الجزائي بشقيه الموضوعي والإجرائي، فإذا كان أساس قانون العقوبات مبدأ الشرعية "لا جريمة ولا عقوبة ولا تدبير آمن بغير قانون"، فأساس قانون الأصول الجزائية "لا إجراء بغير قانون"[٢].

ويستمد مبدأ المشروعية الجزائية قوته من مصادر عدة تتمثل في الدساتير والوثائق الدولية ذات الصلة بحماية حقوق الإنسان وحرياته الأساسية[٣]، فضلاً عن التشريعات الجزائية المختلفة ذاتها في الكثير من الأحيان[٤].

وينتقد بعض رجال القانون عند التعبير عن مبدأ المشروعية الجزائية في صياغة "شرعية الجرائم والعقوبات" أو "لا جريمة ولا عقوبة إلا بنص"، بمعنى اقتصار مبدأ المشروعية الجزائية على القوانين العقابية دون الإجرائية، لأن ذلك يخالف الحقيقة القانونية، كما أن هذه الحلقة لا تكفي لوحدها لحماية حرية الإنسان إذا أمكن القبض عليه أو حبسه...الخ، لأن كل إجراء من هذه الإجراءات سوف يؤدي إلى تحمله عبء إثبات براءته بصدد الجريمة المنسوبة، مما يعني قصور

---

(١) د. حسن الجوخدار، شرح قانون أصول المحاكمات الجزائية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ١٩٩٧م، ص٢٠ – ٢٢.

(٢) بهلول مليكة، المرجع السابق، ص١٠.

(٣) د. عبد الحميد الشواربي، البطلان الجنائي، د.ط، منشأة المعارف بالإسكندرية، مصر، ١٩٩٧م، ص١١٤ – ١١٥.

(٤) كوثر أحمد خالند، الإثبات الجنائي بالوسائل العلمية، دراسة تحليلية مقارنة، الطبعة الأولى، مكتب التفسير للنشر والإعلان، أربيل، العراق، ٢٠٠٧م، ص٦٢.

المشروعية القانونية – وهي الحلقة الأولى من المشروعية الجزائية – من أن تسبغ الحماية الكافية بمفردها على حرية الإنسان، لذلك لا بد من استكمال هذه الحلقة من المشروعية الجزائية بحلقة ثانية تنظم الإجراءات التي تتخذ ضد المتهم بصورة تضمن احترام حريته الشخصية، وتسمى هذه الحلقة بالمشروعية الإجرائية[١].

**ونحن نؤيد النقد السابق حيث أن المشروعية الجزائية لا يجب قصرها على القوانين العقابية دون الإجرائية، بل لا بد من شمولها للقوانين الإجرائية وبالتالي يجب أن تشمل المشروعية الجزائية حلقتين المشروعية العقابية والمشروعية الإجرائية وبدون هاتين الحلقتين لا يستوي معنى المشروعية الجزائية في دورها بحماية حرية الإنسان وكرامته.**

وتختلف قاعدة مشروعية الدليل الجزائي (المشروعية الإجرائية) عن قاعدة شرعية الجرائم والعقوبات (المشروعية العقابية)، حيث تعني هذه الأخيرة مجرد التوافق مع أحكام القاعدة القانونية المكتوبة بخلاف القاعدة الأولى، فهي أعم، حيث تشمل فضلاً عن القواعد القانونية المبادئ التي نصت عليها المواثيق والمعاهدات الدولية، وقواعد النظام العام وحسن الآداب السائدة في المجتمع، بالإضافة إلى المبادئ التي استقرت عليها الأحكام القضائية[٢].

وتظهر أهمية مبدأ المشروعية الإجرائية في أنها هي الحلقة التي تكفل احترام الحرية الشخصية للمدعى عليه عن طريق اشتراط أن يكون القانون هو المصدر التنظيمي الإجرائي وأن تفترض براءة المدعى عليه في كل إجراء من الإجراءات التي تتخذ قبلهُ وأن يتوافر الضمان القضائي في الإجراءات، فالشرعية الإجرائية هي امتداد طبيعي لشرعية الجرائم والعقوبات بل هي في الواقع أكثر

---

(١) د. حسن الجوخدار، المرجع السابق، ص٢٠ – ٢٢. و د.فاضل زيدان محمد، سلطة القاضب الجنائي في تقدير الأدلة، دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠٠٦م، ص ٢٤١-٢٤٢.

(٢) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٥٣.

خطورة منها وأعظم شأناً، فهي بمثابة الإطار الخارجي الذي لا يمكن تطبيق القاعدة الموضوعية تطبيقاً صحيحاً إلا عن طريقه(١)، والشرعية الإجرائية تقوم على ثلاثة عناصر، يتمثل العنصر الأول في أن الأصل في المتهم البراءة بحيث لا يجوز تقييد حريته إلا في إطار من الضمانات الدستورية اللازمة لحمايتها، وبناء على نص في قانون أصول المحاكمات الجزائية، فكما هو ثابت في قانون العقوبات أنه لا جريمة ولا عقوبة إلا بنص فإن الثابت في قوانين الأصول الجزائية أنه لا إجراء إلا بنص وهذا هو العنصر الثاني من عناصر الشرعية الجزائية، أما العنصر الثالث فيتمثل في ضرورة إشراف القضاء على جميع الإجراءات باعتباره الحارس الطبيعي للحقوق والحريات(٢).

كما يُعد مبدأ المشروعية الإجرائية من بين ضمانات المحاكمة الذي يقتضي النص على أدلة الإثبات التي ينبني عليها الحكم الجزائي(٣). كما أنه يمنع من التطاول على حقوق الأفراد وحرياتهم الشخصية دون مقتضى قانوني، لذا يكفل هذا الشق من المشروعية الجزائية الحرية الشخصية للمتهم، وذلك عن طريق تنظيم الإجراءات القانونية التي تمس تلك الحريات مفترضاً في تنظيمها براءة المتهم في كل إجراء من الإجراءات التي تتخذ ضده(٤).

وإن أي دليل مستحدث تفرزه التكنولوجيا الحديثة، ويظهر في ساحة الإثبات الجزائي، يثير مشاكل عدة، تتجلى في ناحيتين: من ناحية أولى، تكون في مدى

---

(١) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، مصر، ٢٠٠٦م، ص١٦.

(٢) د. ميسون خلف حمد الحمداني، مشروعية الأدلة الالكترونية في الإثبات الجنائي، مجلة كلية الحقوق، جامعة النهرين، المجلد الثامن عشر، العدد الثاني، بغداد، العراق، ٢٠١٦م، ص٢٣٥.

(٣) فايزة جادي، البصمة الوراثية ومدى حجيتها في الإثبات الجنائي، رسالة ماجستير، كلية الحقوق، بن عنكون، الجزائر، ٢٠١١ – ٢٠١٢م، ص٢.

(٤) كوثر أحمد خالند، المرجع السابق، ص٥٧.

جواز الاعتماد عليه في إثبات الجرائم، أي بمعنى آخر، مدى اعتراف المشرع به كدليل يركن إليه في جواز اعتباره دليل إثبات أو نفي للجرائم التي يرتكبها الأشخاص، ومن ناحية ثانية، في ضرورة الحصول على هذا الدليل بطرق مشروعة، تراعى فيها ضمانات حقوق الإنسان في أن تبقى حياته الخاصة مصانة ودرء أي اعتداء عليها من قبل أعضاء الضابطة العدلية أو المحققين أو الخبراء الذين يستحصلوا على هذا الدليل[١].

وبما أن الدليل الإلكتروني يتمتع بصفة الحداثة، فهو من الأدلة الحديثة التي أفرزها التطور التقني، وهو أيضاً ذو طبيعة خاصة من حيث الوسط الذي ينشأ فيه والطبيعة التي يبدو عليها، وهذا يثير التساؤل حول مشروعية الأخذ به، إذ يشترط في الدليل الجزائي بوجه عام أن يكون مشروعاً من حيث وجوده والحصول عليه[٢]، ولذلك سوف نقوم بتقسيم هذا الباب إلى فصلين نتناول في:

**الفصل الأول: مشروعية وجود الدليل الإلكتروني.**

**الفصل الثاني: مشروعية الحصول على الدليل الإلكتروني.**

---

(١) هدى طلب علي، المرجع السابق، ص١٣١.

(٢) أ. طارق محمد الجملي، المرجع السابق، ص٤٢.

# الفصل الأول
# مشروعية وجود الدليل الإلكتروني

يقصد بمشروعية وجود الدليل الإلكتروني هي: "أن يكون الدليل معترفاً به، بمعنى أن يكون القانون يجيز للقاضي الاستناد إليه لتكوين عقيدته للحكم بالإدانة"(١).

حيث إن مدى قبول الأدلة المستمدة من الكومبيوتر أي الأدلة الإلكترونية ليس ضرورياً فقط لاستخدام سجلات الكومبيوتر في عملية المحاكمة الجزائية، ولكن أيضاً أمر جوهري في تعريف مدى الصلاحيات المعطاة لرجال إنفاذ القانون، وكذلك في المسائل ذات التعاون الدولي، وفي معظم الدول تُعد الصلاحيات منطبقة فقط على المادة التي تكون مقبولة كدليل في المحكمة، ذلك إذا لم يكن في الإمكان استخدام بيانات كومبيوتر معين أو الأوراق المطبوعة كدليل، فلا يمكن البحث عنها ومصادرتها(٢).

ومن المعروف أن هنالك عدة أنظمة إثبات تأخذ بها الدول لذلك لا بد من معرفة موقف هذه الأنظمة من الأخذ بالدليل الإلكتروني، كما لابد من اعتراف الفقه والقضاء والقوانين المختلفة بالدليل الإلكتروني إلى جانب الأدلة الأخرى، بمعنى آخر الاعتراف بجواز الاستناد إليه من أجل تقرير الأحكام القضائية سواء بالإدانة أو البراءة.

---

(١) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠١١م، ص٢٣٥ – ٢٣٦.

(٢) د. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكومبيوتر والانترنت، دار الكتب القانونية، مصر، ٢٠٠٦م، ص١٢٧.

لكن قبل معرفة مدى الاعتراف بمشروعية الدليل الإلكتروني في الإثبات الجزائي، لابد من إلقاء الضوء على ماهية الدليل الإلكتروني والفهم الجيد لهذا الدليل المستحدث، وتقسيماته المختلفة.

لذلك لا بد من تقسيم هذا الفصل إلى المبحثين التاليين:

**المبحث الأول: ماهية الدليل الإلكتروني.**

**المبحث الثاني: الموقف من مشروعية وجود الدليل الإلكتروني.**

# المبحث الأول
# ماهية الدليل الإلكتروني

يُعَّرف الإثبات لغةً بأنه: "هو إثبات الشيء، أي عَرِفَه حق المعرفة وثبت ثباتاً وثبوتاً، فهو ثابت، والثبات والثبوت يعني الدوام والاستقرار، فالإثبات لدى علماء اللغة يعني تأكيد وجود الحق بالدليل"(١).

ويُعَّرف الإثبات اصطلاحاً في الدعوى الجزائية بأنه هو" الطريقة التي يتم بها إقامة الدليل على وقوع الجريمة وعلى نسبتها إلى المدعى عليه أو المتهم بصورة تحمل على الجزم واليقين بأن المدعى عليه أو المتهم هو الذي ارتكب الفعل الجرمي الذي أسند إليه"(٢).

فالإثبات إذن في المواد الجزائية، هو كل ما يؤدي إلى إظهار الحقيقة لأجل الحكم على المتهم، أي وقوع الجريمة بوجه عام ونسبتها إلى المتهم بوجه خاص، وبذلك يكون محل الإثبات الجزائي هو الواقعة المخالفة للقانون الجزائي، فالإثبات ينصب على الوقائع لا على القانون ذاته أو تفسيره(٣).

ويُعَّرف الدليل الجزائي **لغةً** بأنه: "المرشد، والدليل هو ما يستدل به، والدليل الدال أيضاً، ويقال دله على الطريق يدله بالضم، ودلالة بفتح الدال وكسرها، ودلولة بالضم والفتح أعلى، ويقال أدل فأمل والاسم الدالة بتشديد اللام وفلان يدل بفلان أي يثق به"(٤).

---

(١) الفيروز آبادي، القاموس المحيط، الطبعة الثانية، مؤسسة الرسالة، بيروت، لبنان، ١٤٠٧هـ، ص١٤٤.

(٢) د. بارعة القدسي، أصول المحاكمات الجزائية، سير الدعوى العامة، الجزء الثاني، الطبعة الأولى، منشورات جامعة دمشق، دمشق، سورية، ٢٠١٠ – ٢٠١١م، ص١٠٧.

(٣) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٦.

(٤) ابن منظور، لسان العرب، المجلد الحادي عشر، الطبعة الثالثة، دار صادر، بيروت، لبنان، ١٩٩٤م، ٢٤٨ – ٢٤٩.

ويُعَّرف **اصطلاحاً** بأنه: "الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها، أي كل ما يتعلق بالوقائع المطروحة عليه لإعمال حكم القانون عليها، فبدون هذا الدليل، لن تثبت الجريمة ولن تسند إلى متهم ولن يطبق قانون العقوبات"(١).

كما تُعَّرف وسيلة الإثبات بأنها هي: "كل ما يستخدم في إثبات الحقيقة – فهي نشاط يُبذَل في سبيل اكتشاف حالة أو مسألة أو شخص أو شيء ما أو ما يفيد في إظهار عناصر الإثبات المختلفة – أي: الأدلة – ونقلها إلى المجال الواقعي الملموس"(٢).

**ونرى أن الدليل بشكل عام هو وسيلة قانونية يستخدمها القاضي لإثبات أو نفي الجريمة عن الشخص.**

وللدليل في المواد الجزائية أهمية عظيمة لأنه هو الذي يناصر الحقيقة ويبين مرتكبها، وهو الذي يحول الشك إلى يقين، فالحقيقة في معناها العام تعني معرفة حقيقة الشيء بأن يكون أو لا يكون، وهذا لا يتحقق إلا بالدليل بحسبان أنه المعبر عن هذه الحقيقة(٣).

وبغرض دراسة ماهية الدليل الإلكتروني، لابد لنا من تقسيم هذا المبحث إلى مطلبين ندرس في:

**المطلب الأول: مفهوم الدليل الإلكتروني.**

**المطلب الثاني: أنواع الدليل الإلكتروني.**

---

(١) د. جميل عبد الباقي الصغير، المرجع السابق، ص١٢.

(٢) د. علي حسن الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي (دراسة مقارنة)، مركز الإعلام الأمني، جامعة العلوم التطبيقية، البحرين، ٢٠٠٩م، بحث منشور على الموقع الإلكتروني التالي:

www.policeem.gov.bh/reports ص٢١.

(٣) أ. م. جاسم خريبط خلف، بحث بعنوان: " صعوبات الدليل الجنائي في الجرائم المعلوماتية"، قسم القانون، كلية شط العرب الجامعة، بلا تاريخ، ص٧.

# المطلب الأول

# مفهوم الدليل الإلكتروني

لابد من تحديد مفهوم الدليل الإلكتروني من أجل تمييز هذا الدليل عن غيره من الأدلة الجزائية وذلك عن طريق تعريفه وتحديد خصائصه وطبيعته ومصادره، وأخيراً تحديد مكانة الدليل الإلكتروني من أدلة الإثبات الجزائي، وذلك في الفروع الخمسة التالية:

**الفرع الأول: تعريف الدليل الإلكتروني.**

**الفرع الثاني: خصائص الدليل الإلكتروني.**

**الفرع الثالث: طبيعة الدليل الإلكتروني.**

**الفرع الرابع: مصادر الدليل الإلكتروني في التحقيقات الجرمية.**

**الفرع الخامس: مكانة الدليل الإلكتروني من أدلة الإثبات الجزائي.**

## الفرع الأول

## تعريف الدليل الإلكتروني

إن محاولات تعريف الدليل الإلكتروني، كانت متباينة، فمنها ما جاء واسعاً، ومنها ما جاء ضيقاً، ومرد ذلك للعلم الذي ينتمي إليه هذا الدليل[١].

وسنذكر تعريف الدليل الإلكتروني فقهاً ثم قانوناً كالآتي:

### أولاً: تعريف الدليل الإلكتروني فقهاً:

عُـرَّف الـدليل الإلكترونـي بأنـه: "الـدليل الـذي يجـد أساسـاً لـه فـي العـالم الافتراضـي ويقود إلـى الجريمـة، فهو كل بيانـات يمكن إعدادها أو تخزينها بشكل إلكتروني بحيث تمكن الحاسوب من إنجاز مهمة ما"[٢].

---

(١) هلال آمنة، المرجع السابق، ص٨.

(٢) د. عمر أبو بكر يونس، الجرائم الناشئة عن الإنترنت، رسالة دكتوراه، جامعة عين شمس، مصر، ٢٠٠٠م، ص٩٦٩.

فهو ذلك الجزء المؤسس على الاستعانة بتقنية المعالجة التقنية للمعلومات، والذي يؤدي إلى إقناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة عبر الإنترنت(١).

فكلما كان هناك مزج في موضوع الدليل، الفكرة أو المعلومة او الصورة أو كبيانات **Data** ...إلخ، بالمعالجة الآلية للمعلومات فإنه يُعد هنا دليلاً إلكترونياً(٢).

كما يُعرَّف بأنه: "أي معلومات ذات قيمة في الكشف عن الحقيقة سواء أكانت مراسلة أو مخزنة في شكل رقمي"(٣).

كما يُعرَّف الدليل الإلكتروني بأنه: "الدليل المأخوذ من أجهزة الكومبيوتر، ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة، مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون"(٤).

وانتقد هذا التعريف لأنه يقصر مفهوم الدليل الإلكتروني على ذلك الذي يتم استخراجه من الحاسوب فقط، لأن فيه تضييق لدائرة الدليل الإلكتروني، فهو كما يمكن أن يستمد من الحاسوب يمكن أن يستمد من شبكة الإنترنت أو البريد الإلكتروني أو من الأجهزة الملحقة بالحاسوب أو أقراص التخزين، وأيضاً من الممكن أن يتحصل عليه من أية آلة رقمية أخرى، فالهاتف وآلات التصوير وغيرها

---

(١) د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩م، ١٧٧-١٧٨.

(٢) Anabda Giet , Analysis of the police and criminal evidence act sec. 69/ computer generated evidence, WEB jornal of Current Legal issues UK, 1996 Issue 1, p.1. Available on- line in june 2008 at: Http://webicli.nci.ac.uk/1996/issue1/hoev.html

(٣) سهى إبراهيم داود عريقات، ورقة بحثية بعنوان" الطبيعة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي"، كلية الحقوق، جامعة القدس، بلا تاريخ، ص١٠.

(٤) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٨٨.

من الأجهزة والتي تعتمد التقنية الرقمية في تشغيلها يمكن أن تكون مصدراً للدليل الإلكتروني[١]، فضلاً عن ذلك فإن هذا التعريف يخلط بين الدليل الإلكتروني ومسألة استخلاصه، حيث عرَّفه بأنه الدليل المأخوذ من الكومبيوتر..... إلخ، وهذا يعني أن الدليل الإلكتروني لا تثبت له هذه الصفة إلا إذا تم أخذه أو استخلاصه من مصدره، وهذا ليس صحيحاً، إذ من شأن التسليم بذلك القول أن تلك المجالات المغناطيسية أو الكهربائية قبل فصلها عن مصدرها بواسطة الوسائل الفنية لا تصلح لأن توصف بالدليل الإلكتروني، أي إن مخرجات الآلة الرقمية لا تكون لها قيمة إثباتية مادامت في الوسط الافتراضي الذي نشأت فيه أو بواسطته، وهذا غير دقيق، وهو ما يُوصم هذا التعريف بالقصور لكونه لا يعطي تعريفاً جامعاً للدليل الإلكتروني[٢].

وبناء على ذلك هناك من يُعرَّف الدليل الإلكتروني الجزائي بأنه: "الدليل الذي تم الحصول عليه بواسطة التقنية الفنية الإلكترونية من معطيات الحاسوب وشبكة الإنترنت والأجهزة الإلكترونية الملحقة والمتصلة به وشبكات الاتصالات من خلال إجراءات قانونية لتقديمها للقضاء كدليل إلكتروني جنائي يصلح لإثبات الجريمة"[٣].

ويُعرَّف كذلك بأنه: "معلومات يقبلها المنطق والعقل ويعتمدها العلم ويتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسوب وملحقاتها وشبكات الاتصال ويمكن استخدامها في أية مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شيء له علاقة بجريمة أو جاني أو مجني عليه"[٤].

---

(١) خالد عياد الحلبي، المرجع السابق، ص٢٣٠. كذلك هدى طلب علي، المرجع السابق، ١١٥.

(٢) أ. طارق محمد الجملي، المرجع السابق، ص٤٤.

(٣) خالد عياد الحلبي، المرجع السابق، ص٢٣٠ – ٢٣١.

(٤) هدى طلب علي، المرجع السابق، ١١٥.

بمعنى أن الدليل الإلكتروني يستخلص من البرامج المعلوماتية الموجودة في الحاسوب، وكذلك ما يمكن استخلاصه من معدات، وأدوات الحاسوب، وهذا مرتبط بأن يكون الدليل قد استُخرج بطريقة قانونية، بهدف تحليله، وتقديمه للقضاء في شكله النهائي(١).

كما عرَّفه آخرون بأنه: "الدليل الرقمي يمكن أن يكون معلومة محددة أو مخزنة في شكل معالج رموز وأرقام حيث يستخدمها الحاسوب في انجاز مهمة ما"(٢).

كما عُرَّف أيضاً بأنه: "الأدلة التي تشمل جميع البيانات الرقمية التي يمكن أن تثبت أن هناك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والجاني، أو بين الجريمة، والمتضرر منها "(٣).

وعرَّفه آخرون بأنه: "مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية"(٤).

كما يُعرَّف الدليل الإلكتروني بأنه: "هو ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي أو شبكات الاتصال من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علمياً أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور أو أشكال وأصوات لإثبات وقوع الجريمة أو لتقرير البراءة والإدانة فيها"(٥).

---

(١) هلال آمنة، المرجع السابق، ص٨.

(٢) د. ميسون خلف حمد الحمداني، المرجع السابق، ص١٩٧.

(3) "Digital evidence encompasses any and all digital data that can establish that crime has been committed or can provide link between a crime and it's victim or a crime and it's perpetrator " Eoghan Casey, Digital Evidence and computer crime, London, academic press, 2000, p.260.

(٤) أ. طارق محمد الجملي، المرجع السابق، ص٤٤.

(٥) هدى طلب علي، المرجع السابق، ص١١٦.

كـذلك عُـرَّف الـدليل الإلكترونــي بأنــه: "المعلومـات ذات القيمـة المحتملـة والمخزنة أو المنقولة في صورة رقمية"[١].

والملاحظ على هذه التعاريف الفقهية، أن هناك خلط بين الدليل الإلكتروني، وبرامج الحاسوب ، حيث تم اعتبار الدليل الإلكتروني كبيانات يتم إدخالها إلى جهاز الحاسوب، وهذا مفهوم يشبه تماماً مع ما يقصد به ببرامج هذا الجهاز، وبالنظر نجد أن كليهما له آثار معلوماتية، وباعتبار أن البيانات التي تخزن في جهاز الكومبيوتر مهما كانت صورتها نصوصاً، أو أرقاماً، أو صوراً، وغيرها، تتحول إلى طبيعة رقمية، وهذا مرده إلى أن التكنولوجيا الحديثة تعتمد على تقنية الترقيم، إلا أن هناك فرق بين الدليل الإلكتروني، وبرامج الحاسوب [٢].

ومن جهة أخرى فإن هذه التعريفات قد حصرت الأدلة الإلكترونية في الحاسوب، وملحقاته فقط، ولكن بالنظر لما تم التوصل إليه نجد أن هناك وسائل

---

(١) أ. طارق محمد الجملي، المرجع السابق، ص٥.

(٢) حيث يكمن هذا الفرق في الوظيفة التي يؤديها كل من الدليل الإلكتروني وبرامج الحاسوب ، حيث يتمحور دور برامج هذا الجهاز في تشغيله، وتوجيهه لحل المشاكل، بالإضافة إلى وضع الخطط المناسبة، وإلا كان مجرد آلة صماء، والملاحظ أن هناك برامج خاصة لها دور في استنباط الدليل الإلكتروني، كبرامج معالجة الملفات، مثل: (X tree pro Gold)، وبرنامج النسخ، مثل: (Lap Link). أما دور الدليل الإلكتروني، فيكمن دوره في التعرف على طريقة وقوع الجريمة الإلكترونية، وهذا بغرض إثباتها وكشف الحقيقة، ونسبتها لمرتكبيها، خاصة في هذه البيئة الافتراضية، بحيث يمكن تفتيش محتوى القرص الصلب بهدف تبيان المراحل التي مر بها المجرم، لكي يحقق الغرض من فعله الإجرامي.
ومالا ينبغي إغفاله فيما يخص الفرق بين الدليل الإلكتروني، وبرامج الحاسوب، أن الدليل الإلكتروني لا يقتصر دوره في إثبات الجرائم الإلكترونية فقط – كما سنرى في الفصل الأول من الباب الثاني–، كسرقة الملكية الفكرية، وإنما يمتد أيضاً إلى الجرائم التقليدية، كالقتل، والاختطاف، وأيضاً الاتجار بالمخدرات، وغيرها من الجرائم التي تستخدم فيها التقنية الإلكترونية للتسهيل فيها. هلال آمنة، المرجع السابق، ص٨ – ٩.

أخرى ترتبط بالحواسيب، كالهواتف النقالة، والبطاقات الذكية، وكذلك المساعد الرقمي الشخصي[١].

وتجدر الإشارة إلى أن الأدلة المتحصلة من الوسائل الالكترونية قد تنتمي إلى أدله الإثبات التقليدية وذلك إذا كانت نتاج شهادة أو اعتراف أو خبره، فقد يمكن إثبات جرائم الاحتيال والسرقة والاختلاس في الجرائم الالكترونية عن طريق الوثائق الأصلية المحفوظة في الميكروفيلم أو بالشريط الممغنط أو بحافظات الأكواد أو بمخرجات الحاسب وسجلات التشغيل[٢].

وعرَّفت المنظمة العالمية لدليل الكومبيوتر **(IOCE)**[٣] الدليل الإلكتروني لأول مرة في آذار سنة ٢٠٠٠م، بقولها بأنه: "المعلومات المخزنة، أو المنقولة، والتي يمكن الاعتماد عليها أمام المحكمة"[٤].

ثم عرفته في تشرين الأول سنة ٢٠٠١م، بأنه: "المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية". كما عرفت الأدلة ذات الصلة على النحو التالي:

الدليل الإلكتروني الأصلي: "هو الأشياء المادية أو المعلوماتية المتصلة بهذه الأشياء المادية عند الضبط".

أما الدليل الإلكتروني المزدوج: "فهو كل الأشياء المتعلقة بالبيانات عند ضبط الشيء الملموس الأصلي"[٥].

وبالنسبة للتعريف الوارد سنة ٢٠٠١م، فله نفس معنى التعريف الوارد من الفريق العلمي العامل على مستوى الأدلة الإلكترونية **(SWGDE)** تقريباً، وهذا

---

(١) هلال آمنة، المرجع السابق، ص٩.

(٢) أ.م. جاسم خريبط خلف، المرجع السابق، ص٩.

(٣) اختصاراً لـ "Interruption organization on computer evidence".

(٤) هلال آمنة، المرجع السابق، ص٩.

(٥) د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، مصر، ٢٠٠٩م، ص٢١٣-٢١٤.

باعتباره قد أنشئ لتوحيد الجهود التي تقوم بها هذه المنظمة، هذا من جهة، ومن جهة أخرى العمل على تطوير مختلف التخصصات، والمبادئ التوجيهية للمحافظة على هذا النوع من الأدلة، ودراستها[١].

وتعريف المنظمة للدليل الإلكتروني يشمل عناصر كثيرة فيما يخص الدليل الإلكتروني، إلا أن تعريفها لم يكن جامعاً مانعاً كباقي التعريفات الفقهية، فلم يشتمل هذين التعريفين على طريقة الحصول على هذه الأدلة، والتي يجب أن تكون قانونية، وفنية، وكذلك الغرض من هذا الدليل وهو الأساسي أي أن يكون استعماله في إطار الإثبات[٢].

**ونرى أن جميع هذه التعريفات كانت قاصرة ولا تفي بالغرض في تعريف الدليل الإلكتروني وذلك باعتبارها أنها ضيقت من نطاق الدليل الإلكتروني حيث أنها حصرت استخراج هذا الدليل من جهاز الحاسوب فقط، في حين نرى أن الدليل الإلكتروني لا يقتصر على الدليل المستخرج من الحاسوب، بل يمتد إلى ما يستخرج من مختلف الآلات والأجهزة الرقمية كالهاتف النقال مثلاً.**

**ويمكن تعريف الدليل الإلكتروني بأنه مجموعة المعلومات التي يتم الحصول عليها من جهاز الحاسوب أو أي جهاز تقني حديث آخر، بهدف إثبات جريمة محددة، أو نسبتها إلى شخص معين.**

**ثانياً: تعريف الدليل الإلكتروني قانوناً:**

هنالك قلة من التشريعات المقارنة التي أعطت تعريف للدليل الإلكتروني وتحديد المقصود به. وقد عرَّف المشرع السوري **الدليل الإلكتروني** في المادة الأولى من قانون مكافحة الجريمة المعلوماتية بأنه: "البيانات الرقمية المخزّنة في الأجهزة الحاسوبية أو المنظومات المعلوماتية، أو المنقولة بواسطتها، والتي يمكن استخدامها في إثبات أو نفي جريمة معلوماتية".

---

(١) هلال آمنة، المرجع السابق، ص١٠.

(٢) هلال آمنة، المرجع السابق، ص١٠.

ومن خلال استقراء هذا التعريف، يمكن تحديد خاصتين للدليل الرقمي:

**الخاصة الأولى:** إن الدليل الرقمي عبارة عن معلومات أو بيانات رقمية مخزنة في الحاسوب أو منقولة بواسطته، أيّاً كان شكل هذا الحاسوب، بحيث يستوي أن يتخذ شكل الحاسوب الشخصي، أو مُخدّم الإنترنت، أو أن يكون ضمن الهاتف الجوال، أو ساعة اليد، أو الكاميرات الرقمية وغيرها.

**الخاصة الثانية:** القيمة الاستدلالية أو البرهانية لهذه المعلومات في إثبات أو نفي الجرائم[١].

**وقد أحسن المشرع السوري بإيراد تعريف للدليل الإلكتروني وتحديد المقصود به وعدم ترك هذه المسألة للفقه والاجتهاد القضائي، لأن ذلك يساعد على تمييز هذا الدليل عما سواه من الأدلة الأخرى.**

## الفرع الثاني

## خصائص الدليل الإلكتروني

للدليل الإلكتروني خصائص تميزه عن باقي الأدلة الجزائية التقليدية، وهذا يعود للبيئة التي يستخلص منها المتمثلة في البيئة الافتراضية، وهي بيئة متطورة بطبيعتها، حيث تتوافر أنواع متعددة من البيانات الرقمية التي قد تكون منفردة، أو مجتمعة، حتى تُكَّون دليلاً، ومنه فإن هذه البيئة انعكست على هذا الدليل، وأضفت عليه خصائص لا تتوافر في باقي الأدلة الجزائية[٢].

لذلك لا بد لنا من دراسة هذه الخصائص:

### أولاً: الطبيعة التقنية للدليل الجزائي الإلكتروني:

إن الدليل الإلكتروني ذو طبيعة تقنية وفنية وكيفية معنوية غير ملموسة لا تدرك بالحواس العادية ويتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبة

---

(١) د. محمد طارق الخن، المرجع السابق، ص١١٢.

(٢) هلال آمنة، المرجع السابق، ص١١.

الآلية (HARD WARE) واستخدام نظم برامجية حاسوبية (SOFT WARE)، فالدليل الإلكتروني – عبارة عن مجالات مغناطيسية كهربائية – ومن ثم فإن ترجمة الدليل الإلكتروني وإخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعد هو الدليل، بل إن هذه العملية لا تعدو كونها عملية نقل لتلك المجالات من طبيعتها الرقمية إلى الهيئة التي يمكن الاستدلال بها على معلومة معينة(١).

وترجع طبيعة الدليل الإلكتروني التقنية إلى أنه يتواجد في بيئة رقمية تقنية، ويتكون من عالم من الأرقام التي لا تنتهي، وما تنتجه التقنية ليس سوى نبضات رقمية تشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب(٢).

ومفاد هذه الخاصية أنه من الضروري أن يكون التعامل مع الدليل الإلكتروني من قبل تقنيين مختصين في العالم الافتراضي بصفة عامة، وفي الدليل الإلكتروني بصفة خاصة، وهذا راجع إلى أن الدليل الإلكتروني ليس كالدليل العادي، فما تتجه إليه التقنية هو نبضات إلكترونية، تتشكل قيمتها في إمكانية التعامل مع القطع الصلبة التي تشكل الحاسوب في أي شكل يكون عليه(٣).

وتظهر أهمية هذه الخاصية، في الدور الذي تقوم به هذه التقنية في كشف الدليل الإلكتروني وهذا ما يقتضي الاهتمام بهذا الأمر من ناحيتين، الأولى هي ضرورة الاهتمام بتقنية البرامج التي تتعامل مع الدليل الإلكتروني، وهذا من ناحية

---

(١) هدى طلب علي، المرجع السابق، ١١٩ – ١٢٠.

(٢) فرج بشير برنوص، ورقة عمل بعنوان" حجية الدليل الرقمي وموقف المشرع الليبي" مقدمة إلى ورشة العمل حول قوانين وتشريعات الأمن السيبراني والمنعقدة في جامعة طرابلس يوم ٢٣/٥/٢٠١٦م، منشور في ١/٧/٢٠١٦م على الموقع التالي:
https://www.slideshare.net/nissaly/ss - 6261086. تاريخ الدخول في ٢٢/٦/٢٠١٨م.

(٣) قام المشرع البلجيكي، على إثره بمقتضى القانون (٢٨) الصادر في تشرين الثاني سنة ٢٠٠٠، بتعديل قانون التحقيق الجنائي، أضاف المادة (٣٩)، التي سمحت بضبط الأدلة الإلكترونية، كنسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية. هلال آمنة، المرجع السابق، ص١٢.

الحصول أو التحفظ عليه، وتحليله، وتقديمه، والثانية هي أن هذه البرامج في حد ذاتها يجب أن تكون مقبولة من طرف المحكمة، وهذا ما يستدعي الإشارة في محضر التحقيق الأولي والابتدائي، إلى التقنية المستخدمة في الحصول على هذا الدليل[١].

**ثانياً: الدليل الإلكتروني دليل علمي:**

إن الدليل الإلكتروني هو دليل علمي يرجع إلى أنه يستمد مما يصنعه أهل العلوم التقنية من آراء واستنتاجات علمية على ضوء ما يتم الوصول إليه من برامج وأجهزة وبرامج تقنية[٢]، والدليل الإلكتروني يُعد من طائفة ما يُعرف بالأدلة المستمدة من الآلة[٣].

ولأجل ذلك فإن ما ينطبق على الدليل العلمي ينطبق على الدليل الإلكتروني، فلا يجب أن يخرج هذا النوع من الأدلة عما توصل إليه العلم الرقمي وإلا فقد معناه[٤].

وتفيد خاصية الدليل الإلكتروني بأنه هو دليل علمي أنه عند قيام رجال الضابطة العدلية، أو سلطات التحقيق، بالتعامل مع هذا الدليل سعياً لإظهار الحقيقة بطريقة علمية، يكون البحث بسبل علمية، وهذا مرده إلى أن الدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقاً لقاعدة في القانون المقارن مفادها "أن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة"، وعلى الرغم من الانتقادات التي وجهت لهذه القاعدة على أساس الإلزامية التي يوجبها القانون

---

(١) هلال آمنة، المرجع السابق، ص١٢.

(٢) هدى طلب علي، المرجع السابق، ١٢٠.

(٣) محمد نافع فالح رشدان العدواني، حجية الدليل الإلكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية (دراسة مقارنة بين القانونين الكويتي والأردني)، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، ٢٠١٥م، ص ٢٥.

(٤) سهى إبراهيم داود عريقات، المرجع السابق، ص١٨ .

المقارن على أعضائه بضرورة وجود معرفة علمية، إلا أنه لا يمكن التمييز بين ما هو قانوني، وما هو علمي.

وكذلك ما يمكن استنباطه من هذه الخاصية فيما يخص موضوع حفظه هو وجوب حفظ هذا الدليل على أسس علمية، ومنه ضرورة السعي وراء تحديث أسلوب تحرير المحاضر في هذا الشأن، فتحرير محضر يتناول دليلاً علمياً مختلفاً عن المحضر الذي يتناول اعتراف شخص بجريمة قتل أو سرقة عادية أو انتهاك حرمة مسكن... الخ[١].

وأخيراً يترتب على هذه الخاصية التي يتمتع بها الدليل الإلكتروني عدة نتائج أهمها تحديث الطرق، وكيفية التعامل مع هذا الدليل بما يتماشى مع هذه الخاصية، وكذا بما يتماشى مع التطور التكنولوجي الراهن، حتى تكون لهذا الدليل حجية أكبر[٢].

**ونرى أن الدليل الإلكتروني ما هو إلا نوع من أنواع الدليل العلمي الذي يتميز بالموضوعية والحياد في إقناع أجهزة العدالة الجزائية.**

**ثالثاً: الدليل الإلكتروني ذو طبيعة ديناميكية:**

الدليل الجزائي الإلكتروني ذو طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان[٣]، وتعتمد هذه الأدلة الجزائية على التطور التلقائي لبيئتها التقنية المتطورة بطبيعتها[٤]، وبالتالي يمكن

---

(١) فتحرير محضر يتناول دليلاً علمياً يعني في الحقيقة ضرورة توافر مسلك علمي في تحريره يتوافق مع ظاهرة الدليل العلمي تحديداً وبحيث يجب ألا يتخذ المحضر المظهر التقليدي فقط، فيجب مثلاً التذكير بضرورة الارتباط بالخبرة وتحديداً الخبرة في تحرير محضر ضبط الدليل العلمي. د. عمر محمد بن يونس، المرجع السابق، ص٧ – ٨.

(٢) هلال آمنة، المرجع السابق، ص١١.

(٣) محمد نافع فالح رشدان العدواني، المرجع السابق، ص٢٧.

(٤) هدى طلب علي، المرجع السابق، ١٢٠.

استغلال ذلك في تبادل المعرفة الرقمية بسرعة عالية، وبمناطق مختلفة من العالم، مما يساهم في الاستدلال على الجناة أو أفعالهم بسرعة أقل نسبياً[١].

**رابعاً: إسهام الدليل الإلكتروني في رصد تحركات الجاني:**

يمكن من خلال الدليل الإلكتروني رصد المعلومات عن الجاني، وتحليلها في ذات الوقت، فالدليل الإلكتروني يمكنه أن يسجل تحركات الفرد، كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه، لذا فإن البحث قد يجد غايته بسهولة أيسر من الدليل المادي[٢].

**خامساً: الدليل الإلكتروني قابل للنسخ:**

يمتاز الدليل الإلكتروني بإمكانية القيام بالنسخ الإلكتروني للدليل والتعامل مع النسخة كأنها أصل[٣]، وأن إمكانية نسخ الدليل الإلكتروني من أجهزة الكومبيوتر تقلل أو تعدم تقريباً مخاطر إتلاف الدليل الأصلي، حيث تتطابق طريقة النسخ مع طريقة الإنشاء[٤].

فمن الممكن استخراج نسخ من الدليل الإلكتروني مطابقة للأصل ولها نفس القيمة العلمية والحجية الثبوتية، الشيء الذي لا يتوافر في الدليل التقليدي[٥]، بحيث يمكن إجراء الفحص المعلوماتي على هذه النسخة لتفادي خطر إتلاف النسخة الأصلية أثناء عملية الفحص[٦].

وقابلية الدليل الإلكتروني للنسخ يشكل في الواقع ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد أو التلف أو التغيير وذلك عن طريق عمل نسخ

---

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٨٩.
(٢) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٨٩.
(٣) سهى إبراهيم داود عريقات، المرجع السابق، ص١٠.
(٤) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٨٩.
(٥) خالد عياد الحلبي، المرجع السابق، ص٢٣٢.
(٦) د. محمد طارق الخن، المرجع السابق، ص١١٢.

طبق الأصل من الدليل[١]. وهذا ما دفع المشرع البلجيكي، بمقتضى قانون ٢٨ /١١/٢٠٠٠م، تعدي قانون التحقيق الجنائي وإضافة المادة (٣٩مكرر) التي سمحت بضبط الأدلة الإلكترونية مثل: نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية[٢].

**سادساً: صعوبة التخلص من الدليل الإلكتروني:**

تعد هذه الخاصية من أهم خصائص الدليل الإلكتروني بالمقارنة مع الأدلة التقليدية[٣]، وهو بذلك يشبه الدليل العلمي المتعلق بالحمض النووي (DNA)، إذ إن كليهما يصعب التخلص منهما[٤].

فهناك صعوبة نسبية لتحطيم أو محو الدليل الإلكتروني، حتى في حالة إصدار أمر من قبل الجاني بإزالته من أجهزة الكومبيوتر[٥]، فالدليل الإلكتروني يمكن استرجاعه بعد محوه وإصلاحه بعد إتلافه وإظهاره بعد إخفائه، مما يؤدي إلى صعوبة التخلص منه، وهذا يعود إلى أن هناك العديد من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي تم حذفها أو إلغاؤها[٦]، سواء تم ذلك بالأمر (delete)، أو حتى لو تم عمل إعادة التهيئة أو التشكيل للقرص الصلب ( hard

---

(١) أ. طارق محمد الجملي، المرجع السابق، ص٦. وخالد عياد الحلبي، المرجع السابق، ص٢٣٢.

(٢) عبد الناصر محمد محمود فرغلي، د. محمد عبيد سيف سعيد المسماري، المرجع السابق، ص١٥.

(٣) ففيما يتعلق بالأدلة التقليدية يمكن التخلص بكل سهولة من الأوراق، والأشرطة المسجلة إذا كانت تحتوي على اعتراف شخص بارتكابه للجريمة، وذلك بحرقها أو تمزيقها مثلاً، كما أنه من المستطاع التخلص من بصمات الأصابع بمسحها من موضعها، كما أن هناك بعض الدول التي يتم فيها التخلص من الشهود عن طريق قتلهم، أو تهديدهم لعدم الإدلاء بشهادتهم. هلال آمنة، المرجع السابق، ص١٢.

(٤) د. محمد طارق الخن، المرجع السابق، ص١١٢ – ١١٣.

(٥) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٨٩.

(٦) مثل برنامج (Recover Lost Data).

disk) باستخدام الأمر (format) والبرامج التي تم إتلافها أو إخفاؤها سواء كانت صوراً أم رسوماً أم كتابات أم غيرها (فإن الملف الذي تم حذفه يمكن استرداده باستخدام أداة استردادية للملفات المحذوفة undeleted)[١]، مما يعني صعوبة إخفاء الجاني لجريمته أو التخفي منها عن أعين الأمن والعدالة طالما وصل لعلم رجال التحقيق الجنائي نبأ وقوع الجريمة[٢]، بل إن نشاط الجاني لمحو الدليل، يسجل كدليل أيضاً، حيث أن نسخة من هذا الفعل (فعل الجاني لمحو الدليل) يتم تسجيلها في الكومبيوتر ويمكن استخلاصها لاحقاً لاستخدامها كدليل إدانة ضده[٣].

وإن وجود هذه الخاصية في الحقيقة تعد حافزاً لمواصلة البحث في الجريمة الإلكترونية، وبالتالي تعد دافعاً لاتخاذ الحيطة والحذر تجاه القضايا التي لم يتم حسم الأمر فيها قضاءً بحكم الإدانة أو البراءة[٤].

ومن القضايا التي أبرزت هذه الخاصية، أنه أثناء التحقيق مع الكولونيل "أوليفر نورد" في قضية إيران عام ١٩٨٦م، تمّ استعادة جميع الرسائل الإلكترونية المتعلقة بالجريمة، بعد أن قام هذا الكولونيل بحذفها من حاسوبه، إذ لم يكن هذا الأخير يعلم بأن هذه الرسائل يمكن استعادتها عن طريق النسخ المحفوظة في النظام[٥].

ويترتب على هذه الخاصية مسائل مهمة في القانون أبرزها إن مسائل التخلص من الدليل معاقب عليه بمقتضى القانون[٦]، فمثلاً إن إعداد برمجيات يتم

---

(١) د. عمر محمد بن يونس، الدليل الرقمي، الطبعة الأولى، مصر، ٢٠٠٧م، ص٤٧.
كذلك د. ميسون خلف حمد الحمداني، المرجع السابق، ص٢٠١.

(٢) د. عبد الناصر حمد محمود فرغلي، د. محمد عبيد سيف المسماري، المرجع السابق، ص١٥.

(٣) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٨٩.

(٤) د. عمر محمد بن يونس، الدليل الرقمي، المرجع السابق، ص١٠.

(٥) د. محمد طارق الخن، المرجع السابق، ص١١٣.

(٦) هدى طلب علي، المرجع السابق، ص١٢١.

التعويل عليها من قبل مرتكبي جرائم الحاسوب عامة والإنترنت تخصيصاً، مهمتها التخلص من الأدلة بإزالة محتويات الحاسوب والبرمجيات التي يستخدمها هؤلاء في ارتكاب جرائمهم من الأمور غير المفيدة، حتى ولو تضمنت إمكانية التخلص من الأدلة فإنه يمكن إدانة مرتكب الجريمة بالنصوص التي تُجَّرم مثل هذه الأفعال، سيما وإن ما توصل إليه الخبير يثبت حدوث هذه الجريمة[١].

ومن القوانين التي عاقبت على العبث بالأدلة الإلكترونية أو تدميرها أو إتلافها أو تعديلها قانون الجرائم الإلكترونية الفلسطيني رقم (١٦) لسنة ٢٠١٧م، وذلك في المادة (٤٩) [٢].

كما عاقب قانون الأحوال المدنية السوري[٣] في المادة (٧٣) الفقرة (د) منه بالأشغال الشاقة من ثلاث إلى خمس سنوات كل من دخل وهو غير مخول بالدخول إلى معلومات السجل المدني المؤتمت بقصد تعديل بياناته (حذف، إضافة، تعديل) أو برامجه وتضاعف العقوبة إذا كان من قام بالفعل عاملاً بالوزارة سواء أكان مخولاً أم غير مخول بالدخول بقصد التزوير.

**ونرى أنه على التشريعات الجزائية أضحوا مطالبين بوضع نصوص قانونية تجرم التخلص من الأدلة الإلكترونية، وفي حال وجودها نطالب باعتبار أن التخلص من هذه الأدلة ظرف تشديد وذلك نظراً لإمكانية التخلص منها بشكل أكبر وأكثر شيوعاً من الأدلة التقليدية.**

---

(١) د. عمر محمد بن يونس، الدليل الرقمي، المرجع السابق، ص١٠.

(٢) نصت المادة (٤٩) على أنه: " كل من أقدم على العبث بأدلة قضائية معلوماتية، أو أقدم على إتلافها، أو إخفائها، أو التعديل فيها أو محوها، يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن ألف دينار ولا تزيد على خمسة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً".

(٣) صدر قانون الأحوال المدنية السوري بالمرسوم التشريعي رقم (٢٦) لعام ٢٠٠٧م.

نستنتج مما تقدم أن البيئة الإلكترونية التي نشأ فيها الدليل الإلكتروني هي التي أضفت على هذا الدليل عدد من الخصائص التي تميزه عن باقي الأدلة التقليدية.

## الفرع الثالث

## طبيعة الدليل الإلكتروني

**يدور التساؤل حول: ماهي طبيعة الدليل الإلكتروني؟ هل هي مادية أو معنوية؟** وفي الواقع انقسم الفقه إلى اتجاهين فهناك من يرى أنه ذو طبيعة مادية وهناك من يرى أنه ذو طبيعة معنوية، وسنبحث في هذين الاتجاهين كالتالي:

### أولاً: الدليل الإلكتروني ذو طبيعة مادية:

هنالك رأي يقول أن الدليل الإلكتروني بأنواعه ذو طبيعة مادية، مهما كان شكله، وسواء كان في شكل مخرجات ورقية، أو غير ورقية، وغيرها، باعتبار أنه حتى وأن كان غير ذلك فسيتم إخراجه في شكل دعامات، عبارة عن أشرطة ممغنطة، أو أقراص مغناطيسية، إلى غير ذلك، وبالتالي فهو سيصبح ذو طبيعة مادية، وما يؤكد الطبيعة المادية للأدلة الإلكترونية هو أن التطور التكنولوجي في الوقت الحالي يسمح باستخراج مختلف المعلومات من جهاز الحاسوب أو التقنيات المرتبطة به، في شكل أشياء مادية ملموسة لتصبح دليلاً يعتمد عليه في قضية ما، وتثبت به[١].

### ثانياً: الدليل الإلكتروني ذو طبيعة معنوية:

يذهب هذا الرأي إلى أن الدليل الإلكتروني مثل أي واقعة تحدث من خلال النظام الثنائي(Binary System) الرقمي (Digital) الذي يتم تفعيله ومباشرته عبر الحاسوب، لذلك يأخذ طابع القرص المرن تحديداً، فهو إذن عبارة عن برمجية (Software) أو برنامج (Program) أو حزم (packet switched)، ويختلف بذلك

---

(١) هلال آمنة، المرجع السابق، ص١٠.

عن حالة الدليل المادي المستمد من الحاسوب وهو الدليل الممثل في القطع الصلبة (Hardware) للحاسوب حتى مع الاعتراف المسبق بأن الدليل الإلكتروني يمكن أن يكون مقيداً بضرورة وجود القطع المادية للحاسوب باعتباره يمثل البيئة الاتصالية الكاملة للدليل الإلكتروني وفي أوسع مدى العالم الافتراضي ككل.

لذلك فإن التحفظ على قطع صلبة لحاسوب مسروق لا يعني على الإطلاق أننا بصدد دليل إلكتروني وإنما نكون في مواجهة دليل مادي عادي ناجم عن جريمة السرقة، كذلك الحال يسري حين التحفظ على مسروقات من بينها أقراص مرنة أو ليزرية مثلاً فهذه الأخيرة لا تعد من قبيل الأدلة الإلكترونية وإنما أدلة مادية بالطبيعة، والمثال التقليدي على ذلك هو القيام بالتحفظ على قطع صلبة غير مركبة لتتخذ شكل الحاسوب كما لو كانت قطع صلبة متعددة من موضوع واحد أو أن يكون التحفظ على حاسوب مسروق لا يعمل..... الخ، فالدليل المتحصل هنا من واقعة السرقة ليس بالدليل الإلكتروني وإنما مجرد أدلة مادية عادية(١).

والحال غير ذلك إذا كان التحفظ قد تم على أسطوانة تحتوي على ملفات تتضمن أرقام كروت ائتمان مصرفية أو أرقام دخول سرية لمواقع أو صفحات أو بريد إلكتروني أو كود دخول إلى برمجيات في التداول سواء مادياً أو عبر الإنترنت.. الخ، فكل من هذه وتلك أدلة إلكترونية حتى وإن كان الحال يستلزم ضرورة التحفظ على القرص المذكور لكونه حرز لازم هنا، حيث أنه يشكل البيئة التي يعيش فيها الدليل الإلكتروني(٢).

---

(١) د. عمر محمد بن يونس، ورقة بحثية بعنوان" الدليل الرقمي"، المرجع السابق، ص٦.

(٢) البيئة التي يعيش فيها الدليل الإلكتروني هي الحيز الافتراضي (cyberspatial) وهي بيئة المكان الافتراضي (cyberplace) والزمان الافتراضي(cybertime)، هذه البيئة ممثلة في الأقراص بأنواعها بالإضافة إلى معالجات حركة البرامج والذاكرة وكل قطعة يمكن أن تقوم بدور في هذا الشأن بما في ذلك القطع المرنة التي لا يعمل الحاسوب بدونها، مثل نظام التشغيل والبرمجية التي يعمل على تنفيذ أوامر تشغيل الملفات التي وضعها الإنسان، فهذه البيئة تشكل العالم الافتراضي الذي ننتقل إليه عبر الإنترنت، كذلك يضاف إليها نظام الحزم

ويخلص هذا الرأي إلى أن الدليل الإلكتروني هو دليل غير ملموس أي هو ليس دليلاً مادياً، فهو – أي الدليل الإلكتروني – تلك المجالات المغناطيسية أو الكهربائية، ومن ثم فإن ترجمة الدليل الإلكتروني وإخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعد هو الدليل، بل إن هذه العملية لا تعدو كونها عملية نقل لتلك المجالات من طبيعتها الرقمية إلى الهيئة التي يمكن الاستدلال بها على معلومة معينة(١).

**ويبدو أن الرأي الأخير في أن الدليل الإلكتروني ذو طبيعة معنوية وليست مادية هو الراجح والصائب لأنه دليل غير ملموس يتجسد بالمجالات المغناطيسية أو الكهربائية، ولا يغير من هذه الطبيعة المعنوية تحويله باستخراجه في شكل أشياء مادية ملموسة.**

**وإذا ما اعترفنا بالطبيعة المعنوية للدليل الإلكتروني فإنه برأينا يترتب على ذلك ضرورة اعتراف المشرع بالدليل الإلكتروني بطبيعته المعنوية أي بدون وضع هذا الدليل أو استخراجه بشكل مطبوع مادياً.**

## الفرع الرابع

## مصادر الدليل الإلكتروني في التحقيقات الجرمية

يمكن الوصول إلى الدليل الإلكتروني المتعلق بالجرائم الإلكترونية عن طريق البحث في المصدرين التاليين:

---

التراسلية (packets switched) التي يمكن من خلالها التوصل إلى الدليل الإلكتروني. انظر: د. عمر محمد بن يونس، ورقة بحثية بعنوان" الدليل الرقمي"، المرجع السابق، ص٦ – ٧.

(١) أ. طارق محمد الجملي، المرجع السابق، ص٤٤.

**أولاً: أنظمة الحاسوب وملحقاتها:**

تعدّ الحواسيب مصدراً غنياً بالأدلة الإلكترونية، وخاصة تلك الحواسيب الشخصية التي تعدّ بمثابة أرشفة سلوكية للأفراد. فهذه الحواسيب تحتوي على الكثير من المعلومات المتعلقة بنشاطات الأفراد ورغباتهم.

فالملفات الشخصية أو ملفات النظام وغيرها من أنواع الملفات، التي تكون مخزنة عادة في الأقراص الصلبة أو الأقراص الليزرية CD أو الذواكر المعروفة بـ Flash Memory[١] كثيراً ما تحتوي على معلومات تتعلق بالجريمة وتفيد في عملية التحقيق.

وعملية حجز الحاسوب أو ضبطه بقصد تفحصه، تعدّ نقطة البداية في الكشف عن خفايا جريمة إلكترونية، لأن الحاسوب هو وسيلة النفاذ إلى هذه الشبكة، أيّاً كان شكل هذا الحاسوب. ويجب أن تشمل عملية الفحص جميع البرمجيات المخزنة في المكونات الصلبة أو الذواكر الملحقة بالحاسوب، وجميع البرمجيات التي تمّ إلغاؤها من ذي قبل، كما يجب التأكد من أن المكونات الصلبة والبرمجيات تعمل بشكل سليم ومنتظم، وأن الحاسوب غير مصاب بفيروس[٢] يؤثر على نظامه أو على ملفات التشغيل أو التنفيذ، لأن ذلك يمكن أن ينال من صحة الدليل الإلكتروني المستخلص عند عرضه على القضاء[٣].

---

(١) ذاكرة سريعة بحجم القلم، ذات سعة كبيرة ومحمولة، يمكن ربطها بالحاسوب الشخصي وتسجيل ملفات ذات حجم كبير. د.محمد طارق الخن، المرجع السابق، ص١١٤.

(٢) يُعرف الفيروس بأنه: "برنامج صغير تم تجهيزه وإعداده من قبل أحد مستخدمي الحاسوب غير الأسوياء، وذلك لإرضاء نفسيته المريضة بنشر الفوضى والدمار في أجهزة الحاسوب الأخرى، وتختلف أنواع الفيروسات من ناحية الحجم والنوع وطريقة التشغيل ومستوى الدمار الذي تحدثه". خالد عياد الحلبي، المرجع السابق، ص٧٦.

(٣) د. محمد طارق الخن، المرجع السابق، ص١١٤.

**ثانياً: أنظمة الاتصال بالإنترنت:**

تشمل عملية فحص أنظمة الاتصال بالإنترنت، فحص حركة التنزيل والتحميل ودرجة الاستيعاب، والشبكات المحلية، والنظام الأمني المحاط بالإنترنت...الخ. فعملية الفحص هذه قد تؤدي إلى الحصول على دليل إلكتروني يفيد في كشف الحقيقة.

ولعلّ أهم المسائل المثارة في صدد فحص أنظمة الاتصال بالإنترنت هي مسألة تحديد مكان الجريمة، أو الحاسوب الذي ارتكب بواسطته النشاط الجرمي، حيث يمكن معرفة هذا الحاسوب عن طريق تتبع الحركة العكسية لمسار الإنترنت ويستخدم في عملية التتبع هذه نظام فحص إلكتروني يطلق عليه **علم البصمات المعاصر أو علم بصمات القرن الواحد والعشرين**، وهو منهج تم استخدامه في العديد من الجرائم، مثل تتبع مبتكر فيروس "ميليسا"، وكذلك في التوصل إلى الشخص الذي ابتكر موقع خدمات "بلومبرمج" لأخبار المال، وهو موقع احتيالي يرفع أسعار الأسهم بطريقة الخداع.

ومن الملاحظ أن ما يتم التوصل إليه بفضل تتبع الحركة العكسية لمسار الإنترنت هو عنوان رقمي فقط IP adress، وهذا الدليل الإلكتروني لا يكفي لنسبة الجريمة إلى مالك الحاسوب، إذ من الممكن ألاّ يكون هو مرتكب الجريمة، كما لو كان حاسوبه مسروقاً، أو مؤجراً في أحد مقاهي الإنترنت، أو أن يكون عنوانه الرقمي الخاص به مسروقاً، أو أن يكون هناك من يستخدم حاسوبه دون تصريح من مالكه، أو أن المشتبه به لا يعرف أي شيء عن الإنترنت... الخ. الأمر الذي يتطلب من جهات التحقيق توفير الدليل المادي كالاعتراف أو الشهادة أو الخبرة... الخ إلى جانب الدليل الإلكتروني، حتى يمكن أن تنسب الجريمة إلى مرتكبها.

أما مُخدّمات شبكة الإنترنت، فهي تحتوي على الكثير من المعلومات حول أنماط سلوك الأفراد في وقت محدد، فيمكن عن طريق فحص هذه المُخدّمات معرفة الرسائل الإلكترونية التي قام الجاني أو المجني عليه بإرسالها أو استقبالها،

والمواقع الإلكترونية التي سبقت زيارتها، وغرف الدردشة التي تمّ الدخول إليها، حيث يستطيع المحقق أو الخبير المعلوماتي بعد أن يصل إلى هذه المعلومات، أن يتصل بجميع الأفراد الذين كانوا على اتصال مع الجاني أو المجني عليه قبل ارتكاب الجريمة، وذلك عن طريق إرسال الرسائل الإلكترونية إليهم، وسؤالهم عن أي معلومات تتعلق بالجريمة(١).

## الفرع الخامس

## مكانة الدليل الإلكتروني من أدلة الإثبات الجزائي

إن تقسيم الأدلة الجنائية بحسب مصدرها، هو الذي يوضح الفرق بين الأدلة التقليدية والدليل الإلكتروني.

وتقسم الأدلة الجنائية بالنظر لمصدرها إلى:

الدليل القانوني: وهو مجموعة الأدلة التي حددها المشرع، وعين قوتها الثبوتية، وهي في المسائل الجزائية غير محدودة، وخاضعة للسلطة التقديرية للقاضي، ولكن في بعض الأحيان تكون هناك استثناءات على هذه السلطة.

الدليل الفني: وهو الدليل الذي يتولد بناءاً على رأي الخبير الفني، فهو إذا يتمثل عادة في الخبرة.

الدليل القولي: وهو الذي يكون مصدره من الأشخاص الذين أدركوا معلومات مفيدة للإثبات بأحد حواسهم كالشهادة.

الدليل المادي: وهو الدليل المنبعث من عناصر مادية ناطقة بنفسها، ولها تأثير على اقتناع القاضي بطريقة مباشرة(٢).

والتساؤل الذي يطرح نفسه على بساط البحث هو: إلى أي نوع من أنواع الأدلة تنتمي الأدلة الإلكترونية، أتنتمي إلى الأدلة المادية، لكونها ناتجة من

---

(١) د.محمد طارق الخن، المرجع السابق، ص١١٥.

(٢) هلال آمنة، المرجع السابق، ص١٥.

عناصر مادية ملموسة، وتستخدم العلم ونظرياته لاستخلاصها؟ أم أنها تعد من الأدلة الفنية لكونها تتولد من رأي الخبير الفني؟

ونلاحظ أن الاتجاهات الفقهية قد تباينت بصدد هذه المسألة، ويمكن ردها إلى اتجاهين:

**أولاً: الاتجاه الأول:**

ويرى أن الأدلة الإلكترونية ما هي إلا مرحلة متقدمة من الأدلة المادية والتي يمكن إدراكها بإحدى الحواس الطبيعية(١).

فهي إما أن تكون مخرجات ورقية يتم إنتاجها عن طريق الطابعات، أو الراسم، وإما أن تكون إلكترونية: كالأشرطة والأقراص الممغنطة وأسطوانات الفيديو وغيرها من الأشكال الإلكترونية غير التقليدية(٢)، وإما أن تتمثل في عرض مخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به، أو الإنترنت بواسطة الشاشات أو وحدة العرض المرئي(٣).

وهي بمفهوم هذا الاتجاه لا تختلف عن مفهوم الأدلة العلمية كآثار السلاح، على أساس أن هذا النوع من الأدلة له طبيعة مادية ملموسة تتمثل في المستخرجات الإلكترونية سواء كانت في شكل كتابة أو صور وغيرها(٤).

**ثانياً: الاتجاه الثاني:**

وهو مناقض للاتجاه الأول، حيث يرى أصحاب هذا الاتجاه أن الدليل الإلكتروني له طبيعته الخاصة التي تميزه عن غيره من أنواع الأدلة الجزائية

---

(١) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٢٨.

(2) Eoghan Casey, Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet, Second Edition, Academic Press An imprint of Elsevier, London, 2004, P 5.

(٣) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٢٩.

(٤) هلال آمنة، المرجع السابق، ص١٥.

الأخرى، ومن ثم يُعد الدليل الإلكتروني إضافة جديدة لأنواع الأدلة الجزائية الأخرى[١].

وما يؤهله ليكون كنوع جديد يضاف إلى باقي الأدلة الجزائية، هو أن الأدلة الإلكترونية تتمتع بمجموعة من الخصائص جعلتها مختلفة عن باقي الأدلة التقليدية، والتي جعلت من غير الممكن اعتبار هذه الأدلة كطائفة من الأدلة التقليدية، خاصة ميزة العالم الافتراضي التي تعد من أهم ما يميز الدليل الإلكتروني عن باقي الأدلة الجزائية[٢].

**ونرى أن الاتجاه الثاني هو الأرجح وذلك يعود إلى خصائص الدليل الإلكتروني التي سبق أن أشرنا لها والتي تميز هذا الدليل عن باقي الأدلة التقليدية هذا من جهة، ومن جهة ثانية يعود إلى أن الاتجاه الأول يجانبه الصواب وذلك لأنه لا يمكن الأخذ به باعتبار أن الأدلة الإلكترونية ليست ذات طبيعة مادية بل معنوية.**

## المطلب الثاني

## أنواع الدليل الإلكتروني

على الرغم من أن الدليل الإلكتروني في أساسه يعد متحداً في تكوينه، أي في مجال الحوسبة الرقمية، إلا أنه يتخذ أنواعاً مختلفة، فمصطلح الدليل الإلكتروني يشمل كافة أنواع البيانات الإلكترونية الممكن تداولها رقمياً، ويكون بينها وبين الجريمة رابطة من نوع ما، بالإضافة إلى أنها تكون متصلة بالضحية مما يتحقق معه وجود رابطة بينها وبين الجاني، ففيما يخص التنوع المتعلق بالدليل الإلكتروني نجد أنه قد يظهر بطريقة علانية في هيئات مختلفة الأشكال، كأن

---

(١) محمد نافع فالح رشدان العدواني، المرجع السابق، ص٤٠. د. محمد أحمد المنشاوي، المرجع السابق، ص٥٢٩.

(٢) هلال آمنة، المرجع السابق، ص١٥.

يكون بينات غير مقروءة، كما هو الأمر في حالة المراقبة عبر الشبكات والملقمات أو الخوادم، وقد يكون الدليل الإلكتروني مفهوماً للأشخاص كما لو كان وثيقة معدة بنظام المعالجة الآلية للكلمات بأي نظام، كما يمكن أن يكون صورة ثابتة أو متحركة، أو معدة بنظام التسجيل السمعي المرئي، أو أن تكون مخزنة في نظام البريد الإلكتروني(١).

وبالتالي فالأدلة الإلكترونية ليست في صيغة واحدة، وإنما هي متنوعة(٢)، وحين تقسيم الدليل الإلكتروني لابد من الأخذ بعين الاعتبار التطور المستمر الذي يطرأ على هذا النوع من الأدلة من جهة، وعلى البيئة الافتراضية أو الإلكترونية من جهة أخرى(٣).

وسندرس أنواع الدليل الإلكتروني، وذلك بدراسة التقسيم الفقهي، ومن ثم التقسيم القضائي، وذلك في فرعين ندرس في:

**الفرع الأول: تقسيم الفقه لأنواع الدليل الإلكتروني.**

**الفرع الثاني: التقسيم القضائي لأنواع الدليل الإلكتروني.**

## الفرع الأول

## تقسيم الفقه لأنواع الدليل الإلكتروني

يوجد للفقه ثلاثة تقسيمات للدليل الإلكتروني، وسنعرض أولاً، التقسيم الفقهي الأول، وثانياً، التقسيم الفقهي الثاني، وثالثاً، التقسيم الفقهي الثالث، كالآتي:

**أولاً: التقسيم الفقهي الأول:**

قسم بعض الفقه الدليل الإلكتروني إلى عدة أقسام، وأوضحوا ذلك فيما يلي:

---

(١) هلال آمنة، المرجع السابق، ص١٢.

(٢) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٢٣.

(٣) هلال آمنة، المرجع السابق، ص٢١.

**أ- الأدلة الإلكترونية الخاصة بأجهزة الكومبيوتر وشبكاته:**

وهي تتماشى مع جرائم الكومبيوتر الواقعة على أجهزة الكومبيوتر بسلوك غير مشروع، سواء كان هذا الأمر على المكونات المادية له، أو المكونات المعنوية، أو قواعد البيانات الرئيسية، مثل تخريب مكونات الكومبيوتر كالشاشات.

**ب- الأدلة الإلكترونية الخاصة بالإنترنت:**

وهي تتطابق مع جرائم الإنترنت، وهي أيضاً سلوك غير مشروع يقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات، مثل الدخول غير المشروع لمواقع يمنع الدخول إليها، واستخدام عناوين (IP) غير حقيقية للدخول إلى الشبكة العالمية للمعلومات وغيرها.

**جـ- الأدلة الإلكترونية الخاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات:**

وهي متعلقة بالجرائم التي ترتكب باستخدام الكومبيوتر، حيث أنه لا يعد استعمال الكومبيوتر أو الشبكة العالمية للمعلومات أو الإنترنت، في هذه الجرائم من طبيعة الفعل الجرمي، وإنما تعتبر كوسيلة مساعدة لارتكاب الجريمة، مثل غسيل الأموال أو نقل المخدرات من مكان لآخر وغيره، وجهاز الكومبيوتر في هذه الحالة يحتفظ بآثار إلكترونية قد ترشد للفاعل.

**د- الأدلة الإلكترونية الخاصة بالشبكة العالمية للمعلومات:**

وهي متماشية مع الجرائم المتعلقة بهذه الشبكة، وهي فعل غير مشروع قانوناً يقع على أي وثيقة أو نص موجود بالشبكة، مثل قرصنة المعلومات، وسرقة بطاقات الائتمان، وانتهاك الملكية الفكرية للبرامج وغيرها، فهذا النوع من الجرائم يتطلب الاتصال بالإنترنت.

**هـ- مخرجات الحاسوب:**

قد يتخذ الدليل الإلكتروني المستمد من الحاسوب أو الإنترنت شكل المخرجات الورقية التي يتم الحصول عليها عن طريق الطابعات أو الراسمات، كما يمكن أن يتخذ الشكل الإلكتروني كالأقراص الليزرية وغيرها من الأشكال الإلكترونية. وإلى جانب ذلك يوجد مخْرَج ثالث وهو عرض المعلومات والبيانات المتعلقة بالدليل الرقمي عن طريق شاشة الحاسوب. ويطلق على جميع هذه الأشكال مصطلح **مخرجات الحاسوب**[١].

ويرى بعض الفقه [٢] أن هذا التقسيم مطابق لتقسيم الجريمة عبر الكومبيوتر.

ونستنتج مما سبق أن هذا التقسيم الفقهي للدليل الإلكتروني، مع أنه يتناسب مع تقسيم الجرائم عبر الكومبيوتر، لكنه غير متناسب مع مفهوم التقنية الحديثة، فكل هذه التقسيمات تدور حول موضوع واحد وهو الدليل الإلكتروني، رغم أن هذه التقسيمات ميزت بين شبكات الكومبيوتر والإنترنت وبروتوكول تبادل المعلومات والشبكة العالمية للمعلومات التي هي في الأصل واحد ولكنها تختلف في المصطلحات.

وكما انتقد هذا التقسيم فعلى الرغم من أنه جاء متماشياً مع الجرائم الواقعة عن طريق الكومبيوتر، وهذا جانب من الصحة فيه، إلا أنه لم يشمل كافة ما يتعلق بالدليل الإلكتروني، وخاصة أنه لم يأخذ بالحسبان وبصورة كبيرة التقنية الحديثة

---

(١) د. محمد طارق الخن، المرجع السابق، ص١١٦.

٢ د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٨٨.

التي تعد ركيزة مهمة لمعالجة موضوع الدليل الإلكتروني، باعتبار أن هذا الدليل ظهر بظهور التقنيات الحديثة[١].

**ثانياً: التقسيم الفقهي الثاني:**

القسم الثاني من الفقهاء قسم الدليل الإلكتروني لقسمين على النحو التالي:

**أ- أدلة أعدت لتكون وسيلة إثبات:**

وهذه الأدلة تشمل:

١- السجلات التي تم إنشاءها بواسطة الحاسوب تلقائياً، وتعد هذه السجلات من مخرجات الحاسوب التي لم يساهم الأفراد في إنشاءها مثل سجلات الهاتف وفواتير البطاقات البنكية.

٢- السجلات التي تم حفظ جزء منها بالإدخال وجزء تم إنشاءه بواسطة الحاسوب مثل رسائل غرف المحادثة المتبادلة على الإنترنت ورسائل البريد الإلكتروني[٢].

**ب- أدلة لم تُعَّد لتكون وسيلة إثبات:**

وهذا النوع من الدليل الإلكتروني نشأ من دون إرادة الفرد وله أثر يتركه الجاني دون أن يكون راغباً في وجوده ويسمى بالبصمة الرقمية[٣]، وهو ما يمكن تسميته أيضاً بالمعلومات الرقمية[٤]، وتتجسد في الآثار التي يتركها مستخدم شبكة الانترنت بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الحاسوب وشبكة الانترنت[٥].

---

(١) هلال آمنة، المرجع السابق، ص١٧.

(٢) د. خالد ممدوح إبراهيم، الدليل الإلكتروني في جرائم المعلوماتية، بحث منشور على الموقع الإلكتروني لكلية الحقوق في جامعة المنصورة www.f - law.com، ص٢. تاريخ الدخول في ٢٠١٧/١٢/١٢م.

(٣) خالد عياد الحلبي، المرجع السابق، ص٢٣٤ – ٢٣٥.

(٤) أ. طارق محمد الجملي، المرجع السابق، ص٤٦.

(٥) خالد عياد الحلبي، المرجع السابق، ص٢٣٤ – ٢٣٥.

حيث أن هذا النوع من الأدلة لم يُعد أساساً للحفظ من قبل من صدر عنه، غير أن الوسائل الفنية الخاصة تُمَّكن من ضبط هذه الأدلة ولو بعد فترة زمنية من نشوئها[١]، فالاتصالات التي تجري عبر الإنترنت والمراسلات الصادرة عن الشخص أو التي يتلقاها، كلها يمكن ضبطها بواسطة تقنية خاصة بذلك[٢].

في الواقع إن النوع الثاني من الأدلة الإلكترونية هو الأكثر أهمية من النوع الأول لأنه في العادة يتضمن معلومات تفيد في الكشف عن الجريمة ومرتكبيها، ولكن الحصول على هذا النوع من الأدلة الإلكترونية يتطلب تقنيات خاصة وفيه بعض الصعوبة والتعقيد، أما بالنسبة للنوع الأول فيتميز بسهولة الحصول عليه كونه قد أعد أصلاً لأن يكون دليلاً على الوقائع التي يتضمنها، ولكن النوع الثاني عرضه للفقدان لأنه لم يُعَّد أصلاً ليحفظ وليكون دليلاً أما النوع الأول عادة ما يُعمد إلى حفظه للاحتجاج به لاحقاً[٣].

**ثالثاً: التقسيم الفقهي الثالث:**

قسم الدليل الإلكتروني تبعاً لمكوناته وتبعاً لمكان وجوده إلى:

**أ-أقسام الدليل الإلكتروني تبعاً لمكوناته:**

١ - الأشرطة المغناطيسية: هذا الشريط هو عبارة عن شريط بلاستيكي مغطى بمادة قابلة للمغنطة، وقد يكون ملفوفاً على بكرة، كالتي تستخدم في أجهزة التسجيل الصوتي، وكما قد يكون داخل علبة على هيئة شريط الفيديو مثلاً.

---

(١) هدى طلب علي، المرجع السابق، ١١٨.

(٢) حيث يتم الاعتماد في ضبط هذا النوع من الأدلة على ما يعرف ببروتوكول IP والذي يتمكن من ضبط تحركات مستخدم الشبكة وتحديد الجهاز الذي يستعمله من خلال بيانات الجهاز عند مزود الخدمة، وهذا النظام لا يحدد شخص مرتكب الجريمة وإنما يحدد الجهاز الذي استعملت منه، وبالتالي يصلح ذلك قرينة لاعتبار صاحب الجهاز مرتكب الجريمة إلى أن يثبت العكس. أ. طارق محمد الجملي، المرجع السابق، ص٤٦.

(٣) د. عيسى مدالله المخول، الجريمة الإلكترونية، دمشق، سورية، ٢٠١٧م، ص١٤٨. سهى إبراهيم داود عريقات، المرجع السابق، ص٢١.

وكل الأشرطة الممغنطة بها رأس للقراءة والكتابة يسجل البيانات، على شكل نقطة مغناطيسية على الشريط بشفرة خاصة تدل على البيانات المستخرجة من داخل الحاسوب، كما يتمكن هذا الرأس من الإحساس بوجود هذا النقطة ويقوم بإرسال النبضات الكهربائية المقابلة لشفرة البيانات داخل الحاسوب.

والشريط المغناطيسي يستعمل في تخزين البرامج والملفات المتتالية، أي اللازمة لقراءة البيانات والمعلومات الموجودة فيه تنظم على شكل وحدات خاصة، بحيث تسمى كل وحدة بحزمة، وحجم هذه الحزمة يحدده المستعمل للجهاز، وبالنظر لهذا الأمر فإن الحزمة يتعامل معها كوحدة متكاملة، وذلك عند تخزينها، أو إخراجها.

٢ – الأقراص المغناطيسية: إن الأقراص المغناطيسية تعد من أفضل وسائط التخزين، التي يمكن استخدامها للتخزين المباشر، أو العشوائي، وهذا راجع لقدرتها الاستيعابية الكبيرة، ولها خاصية مهمة هي إمكانية القراءة أو التسجيل على أي قطاع من السطوح، وكذلك إمكانية تغيير أو تعديل أي ملف دون حاجة إلى إنشاء ملف جديد حيث يتم تعديل التسجيل، وهو في موضعه، وهناك عدة أنواع منها:

- **القرص المرن:** وهو من أشهر وسائط التخزين للبيانات، ينتشر استخدامه في الحاسبات الصغيرة والمتوسطة، وذلك لسهولة استخدامه وتداوله.
- **القرص الصلب:** وهو يتميز بالسعة التخزينية الكبيرة، وكذلك سرعة تسجيل واسترجاع البيانات وعدم إمكانية تحريكه من مكانه، لذا يطلق عليه اسم القرص الثابت، ويكون عادة داخل جهاز الحاسوب.
- **قرص الخرطوش أو قرص الكارتريدج:** وهو قرص هجيني يجمع بين خصائص القرص الصلب من حيث كبر حجم السعة التخزينية، والقرص المرن من حيث إمكانية تغيير مكانه بقرص آخر.

– **المصغرات الفيلمية:** تعد هذه الأدلة شكلاً مختلفاً من تكنولوجيا المخرجات، حيث تسجل فيها المعلومات والبيانات، بدلاً من تسجيلها على الورق، وهي عبارة عن أفلام فوتوغرافية يتم استخدامها في تصوير صفحات البيانات[١].

**ب–أقسام الدليل الإلكتروني تبعاً لمكان وجوده:**

تقسم الأدلة الإلكترونية بحسب مكان وجودها إلى:

١ – أدلة ورقية: مثل مخرجات الحاسوب والتقارير والرسوم البيانية.

٢ – أجهزة الحاسبات: وهي التي تحتوي على ملحقات الحاسوب من شاشات وغير ذلك.

٣ – الأقراص المرنة والصلبة: تعد من أهم الأدلة لاحتوائها على بيانات وكلمات مرور وصور وتقارير وخطط ارتكاب الجريمة وغيرها.

٤ – أشرطة تخزين المعلومات: تستخدم لحفظ النسخ الاحتياطية.

٥ – القطع الإلكترونية: مثالها أجهزة الإرسال التي يجب أن تفحص للتأكد من طبيعتها خاصة في قضايا التجسس.

٦ – أجهزة المودم: وهي التي تستخدم في نقل المعلومات، ويمتاز بعضها بإمكانية أن يعمل كجهاز الرد على رسائل الهاتف، ويجب تسجيل الكابلات المتصلة به عند ضبطه.

٧ – البرامج: وهي تمثل الأدوات الرئيسية التي يستغلها المجرم في ارتكابه جريمة نظم المعلومات.

٨ – الطابعات والأجهزة الخاصة بتصوير المستندات، وما قد تحتويه من أوراق مطبوعة ومصورة، أو ما هو مخزن في ذاكرتها من معلومات[٢].

---

(١) هلال آمنة، المرجع السابق، ص١٩ – ٢٠.

(٢) هلال آمنة، المرجع السابق، ص٢٠ – ٢١.

## الفرع الثاني

## التقسيم القضائي لأنواع الدليل الإلكتروني

كان للقضاء دور في معالجة موضوع الدليل الإلكتروني، وإعطاء تقسيمات له، ووفقاً لما قررته وزارة العدل الأمريكية سنة (٢٠٠٢) فإن الدليل الإلكتروني يمكن تقسيمه إلى ٣ مجموعات[١]:

### أولاً: السجلات المحفوظة في الحاسوب:

وهي عبارة عن وثائق مكتوبة ومحفوظة، والمقصود بالكتابة الإلكترونية أنها كل حروف أو أرقام أو رموز أو أي علامات أخرى، تثبت على دعامة إلكترونية أو رقمية أو ضوئية أو أية وسيلة مشابهة، وتعطي دلالة قابلة للإدراك[٢] .

ومن أمثلتها البريد الإلكتروني الذي عُرف بأنه: "طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات"[٣].

كما يُعرف بأنه: "عبارة عن رسالة عادية[٤] – لكن بطريقة إلكترونية – يكتبها شخص، بطريقة عادية جداً على جهاز الحاسوب الخاص به، وذلك بعد فتح

---

(١) د. ميسون خلف حمد الحمداني، المرجع السابق، ص١٩٨.

(٢) هلال آمنة، المرجع السابق، ص١٨.

(٣) فكرة البريد الإلكتروني تقوم على تبادل الرسائل الإلكترونية والملفات والرسوم والصور والبرامج وغيرها، عن طريق إرسالها من المرسل إلى شخص أو أكثر، وهذا باستعمال البريد الإلكتروني للمرسل إليه، فهو عبارة عن صندوق تتواجد به كل الرسائل المرسلة إلى صاحب البريد والتي سبق له إرسالها، والملغاة وغيرها من الأمور التي يحتوي عليها البريد الإلكتروني. هلال آمنة، المرجع السابق، ص١٨.

(٤) وهذه الرسالة يستوي أن ترسل إلى شخص مقيم في ذات المدينة أو الدولة أو دولة أخرى وفي لحظات معدودة، وتتوافر فيها عوامل الأمان والسرية ولا يمكن اختراق البريد الإلكتروني لشخص إلا بمعرفة كلمة السر الخاصة به، أو بناء على طرق فنية معقدة لا يجيدها سوى جهابذة المخترقين لشبكات الحاسب الآلي، ولذلك فهو وسيلة أمنة وسريعة ورخيصة التكلفة مقارنة بغيرها من وسائل التراسل. د. عبد الفتاح بيومي حجازي، الإثبات

الصفحة الخاصة ببريده الإلكتروني، والتي لها رقم سري، واسم المستخدم، ولا يمكن لغيره الدخول إليه، وبعد أن يتم الكتابة يقوم بالضغط على أمر معين في الصفحة وهو (send) أي أرسل وفي حالة نجاح وصول الرسالة للعنوان المطلوب على جهاز حاسوب آخر يظهر له علامة (ok) بما يفيد تمام إرسال الرسالة وإذا كان هناك خطأ ما في إرسالها يظهر للمرسل، رسالة موجزة، تشير إلى موضوع الخطأ ويتولى هو تصحيحه ثم يعيد إرسالها مرة أخرى"[١].

وهناك أيضاً ملفات برامج معالجة الكلمات، ورسائل غرف المحادثة على الانترنت[٢].

**ثانياً: السجلات المحفوظة جزئياً في الحاسوب:**

هذا النوع من السجلات يتم إنشاؤها بواسطة الحاسوب أي هي عبارة عن مخرجات برامج الحاسوب، وبالتالي لم يلمسها الإنسان مثل (Log Files) وسجلات الهاتف وفواتير أجهزة السحب الآلي (ATM).

**ثالثاً: السجلات المحفوظة للإدخال والمنشأة بواسطة الحاسوب:**

ومن الأمثلة عليها: أوراق العمل المالية التي تحتوي على مدخلات يتم تحويلها لبرامج أوراق عمل مثل (Excel)، ومن ثم تتم معالجتها بإجراء العمليات الحسابية[٣].

---

الجنائي في جرائم الكومبيوتر والإنترنت، د.ط، دار الكتب القانونية، المحلة الكبرى، مصر، ٢٠٠٧م، ص٣١ – ٣٢.

(١) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣١.

(٢) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٢٢.

(٣) هلال آمنة، المرجع السابق، ص١٨. و د. محمد أحمد المنشاوي، المرجع السابق، ص٥٢٢.

وقد أخذ القضاء الأمريكي بهذا التقسيم، فسجلات الحاسوب المقبولة أمام القضاء الأمريكي هي التي تكون في شكل نصوص، وهي أما تكون في هيئة سجلات الحاسوب المتوالدة، أو سجلات الحاسوب المخزنة، ويكمن الفرق بينهما فيما إذا كان الشخص هو المنشئ لمحتوى هذه السجلات أو الآلة، فسجلات الحاسوب المخزنة تحتوي على كتابات شخص أو بعض الأشخاص في شكل إلكتروني مثل البريد الإلكتروني، أما فيما يخص سجلات الحاسوب المتولدة فالكومبيوتر هو الذي يصدرها، فهي عبارة عن مخرجات برامج الحاسوب مثل سجلات الدخول على الانترنت التي يكون مصدرها مزود خدمة الإنترنت، كما أن هناك نوعاً ثالثاً من السجلات الذي يجمع بين التدخل الإنساني ومعالجة الحاسوب، مثلاً كأن يدخل متهم معين بيانات ويطلب من الكومبيوتر معالجتها للوصول إلى نتائج يسمح بها هذا البرنامج المستخدم، كالشخص الذي يتهرب من الضرائب فيسجل بيانات غير صحيحة تتعلق بدخله وربحه، ويطلب من الحاسوب حساب الضريبة المستحقة[١].

إلاَّ أنه ما يؤخذ على هذه التقسيمات أنها لا تشمل الدليل الإلكتروني، فهي حصرته في نوع واحد وهو سجلات الحاسوب المحتواة على نص، رغم أن الدليل الإلكتروني يتعلق بكافة البيانات الإلكترونية التي يمكن تداولها إلكترونياً، كالصور والأصوات والرسوم وغيرها، فحالياً يوجد بروتوكولات الاتصالات والتطبيقات المعلوماتية التي تستعمل في التحقيق فيما يخص الجرائم الإلكترونية، حيث يعد نظام (TCP/IP) من أكثر البروتوكولات المستعملة في شبكات الإنترنت، فهي تُعد جزءاً مهماً منه، وتدل بصفة يقينية على مصدر الجهاز الذي استخدم في الجريمة، كما تقوم بتحديد الأجهزة التي أصابها الضرر من هذا الفعل الإجرامي[٢].

---

(١) هلال آمنة، المرجع السابق، ص١٨ – ١٩.

(٢) هلال آمنة، المرجع السابق، ص١٩.

**وهكذا نرى أن التقسيم الذي تبناه القضاء الأمريكي فيه جانب من الصحة، على اعتبار أنه تحدث عن نوع مهم من الأدلة الإلكترونية وهي أدلة قوية، لكن مما نؤخذ عليه أنه حصر تقسيمه في الأدلة الإلكترونية على المكتوبة فقط أي كان محصوراً بالسجلات المتعلقة بالحاسوب فقط، لذلك يمكن القول إنه تقسيم ناقص ولا يستوعب كل الأدلة الإلكترونية.**

فتنوع الدليل الإلكتروني يفيد أنه لا يوجد وسيلة وحيدة للحصول عليه وإنما تتعدد وسائل التوصل إليه. وفي كل الأحوال يظل الدليل المستمد منه إلكترونياً حتى وإن اتخذ هيئة أخرى، ففي هذه الحالة فإن اعتراف القانون بهذه الهيئة الأخرى يكون مؤسساً على طابع افتراضي أساسه أهمية الدليل الإلكتروني ذاته وضرورته[١]، وهناك من يرى[٢] أنه لكي يكون هناك تناسق بين القانون والدليل الإلكتروني،، فإنه لابد من اتخاذ مسلك الافتراض باعتبار هذا الدليل دليلاً أصلياً، وهذا مرده إلى نقص توافر الإمكانات الإلكترونية في المحاكم الجزائية الناظرة في هذا النوع من الأدلة.

**وفي النهاية يمكن القول إن هذه التقسيمات المختلفة قد ألمت بجانب كبير جداً من أنواع الدليل الإلكتروني، لكنها لم تشملها جميعها وذلك مرده أن هذا الدليل متطور بطبيعته.**

**وفي هذا المبحث، قمنا بدراسة ماهية الدليل الإلكتروني، فبحثنا مفهومه وذلك بتعريفه وبيان أهم خصائصه وطبيعته ومصادره ومكانته من الأدلة الأخرى، وكذلك تحدثنا عن أنواعه المختلفة سواء ببيان التقسيم الفقهي لهذه الأنواع أو ببيان التقسيم القضائي لها.**

---

(١) د. عبد الناصر حمد محمود فرغلي، د. محمد عبيد سيف المسماري، المرجع السابق، ص٢٢.

(٢) هلال آمنة، المرجع السابق، ص١٨.

# المبحث الثاني
# الموقف من مشروعية وجود الدليل الإلكتروني

إن أي دليل مستحدث يظهر على ساحة الإثبات الجزائي يطرح تساؤلات عدة حول موقف أنظمة الإثبات الجزائية منه ومدى اعترافها بمشروعية الاعتماد عليه كدليل إثبات في إدانة المدعى عليه أو براءته.، كما يطرح تساؤلات حول موقف الاتفاقيات الدولية والفقه والقضاء والقانون من مشروعية استخدامه في الإثبات الجزائي، وبناء على ذلك سنقسم هذا المبحث إلى المطلبين التاليين:

**المطلب الأول: موقف أنظمة الإثبات من مشروعية وجود الدليل الإلكتروني.**

**المطلب الثاني: موقف الاتفاقيات الدولية والفقه والقضاء والقانون من مشروعية وجود الدليل الإلكتروني.**

## المطلب الأول
## موقف أنظمة الإثبات من مشروعية وجود الدليل الإلكتروني

وفقاً لما تكشف عنه الدراسات التاريخية المقارنة للأنظمة الإجرائية فإنه يوجد نظامان للأدلة المقبولة في الإثبات. نظام الإثبات المقيد، ونظام الإثبات الحر، حيث أن النظم القانونية تختلف في موقفها من الأدلة التي تقبل كأساس للحكم بالإدانة بحسب الاتجاه الذي تتبناه، فهناك اتجاهان رئيسان[١]: الأول: نظام الإثبات المقيد، والثاني: نظام الإثبات الحر[٢].

---

[١] بالإضافة إلى نظام ثالث مختلط يجمع بين خصائص النظامين، أي يجمع بين نظام الإثبات المقيد ونظام الإثبات الحر، ويسود هذا النظام في العديد من التشريعات التي تأخذ بمجملها بمبادئ ونظام الإثبات الحر، وعلى سبيل الاستثناء تأخذ بنظام الإثبات المقيد، وجاء نظام الإثبات المختلط نتيجة للتطور الذي وقع في مفهوم الإثبات الحر، ونظراً لطبيعة الاستثناءات التي وردت عليه. آمال عبد الرّحمن يوسف حسن، الأدلة العلمية ودورها في الإثبات الجنائي،

فكان لابد من بيان موقف أنظمة الإثبات الجزائية من الاعتراف بالدليل الإلكتروني كدليل إثبات من جملة أدلة الإثبات الجزائية المعترف عليها. وسنبحث في هذا المطلب الاعتراف بمشروعية الدليل الإلكتروني في نظام الإثبات المقيد، ومن ثم في نظام الإثبات الحر، في الفرعين التاليين:

**الفرع الأول: موقف نظام الإثبات المقيد من مشروعية وجود الدليل الإلكتروني.**

**الفرع الثاني: موقف نظام الإثبات الحر من مشروعية وجود الدليل الإلكتروني.**

## الفرع الأول

## موقف نظام الإثبات المقيد من مشروعية وجود الدليل الإلكتروني

إن دراسة موقف نظام الأدلة القانونية من مشروعية الدليل الإلكتروني في الإثبات الجزائي، تقتضي أولاً، التعريف بنظام الأدلة القانونية، كما تقتضي ثانياً، معرفة مدى اعتراف نظام الأدلة القانونية بالدليل الإلكتروني.

### أولاً: تعريف نظام الإثبات المقيد:

هذا النظام ينتمي للنظم الانجلوسكسونية، مثل المملكة المتحدة "بريطانيا" والولايات المتحدة الأمريكية[1]، ويعني نظام الأدلة القانونية أن المشرع هو الذي يحدد للقاضي الأدلة التي يجوز له أن يقبلها في حالة معينة، ويحظر عليه أن

---

رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، ٢٠١١-٢٠١٢م، ص ٢١.

(٢) د. ميسون خلف حمد الحمداني، المرجع السابق، ص ٢٢٨.

(١) خالد عياد الحلبي، المرجع لسابق، ص٢٣٦.

يقبل سواها[١]. فحسب هذا النظام فإن المشرع هو الذي يحدد حصراً الأدلة التي يجوز للقاضي اللجوء إليها في الإثبات [٢].

**ثانياً: مدى اعتراف نظام الإثبات المقيد بالدليل الإلكتروني:**

هناك من يرى[٣] أنه في نظام الإثبات المقيد، لا سبيل للاستناد إلى أي دليل إذا لم ينص القانون عليه صراحة ضمن أدلة الإثبات، إذ أن القانون قيد القاضي بقائمة من الأدلة التي حددت قيمتها الإثباتية.

ولذا فإن النظم التي تتبنى هذا النظام لا يمكن في ظلها الاعتراف للدليل الإلكتروني بأية قيمة إثباتية مالم ينص القانون عليه صراحة ضمن قائمة أدلة الإثبات، ومن ثم فإن خلو القانون من النص عليه سيهدر قيمته الاثباتية مهما توافرت فيه شروط اليقين فلا يجوز للقاضي أن يستند إليه لتكوين عقيدته، وتطبيقاً لهذا فقد نص قانون الإثبات في المواد الجنائية البريطاني على قبول الدليل الإلكتروني وحدد قيمته الاثباتية اتفاقاً[٤].

بينما هناك من يرى[٥] أن الدليل الإلكتروني في ظل نظام الإثبات المقيد مقبول ويؤخذ به، باعتباره دليل إثبات جزائي وله قوة ثبوتية أيضاً، على الرغم من أن الدليل الإلكتروني يتعارض بسبب طبيعته مع أهم قواعد الإثبات الجزائي المقيد، إلا أنه كان من الضروري الخروج عن الأصل العام في هذه القواعد وإيراد استثناءات عليه حتى يكون في الإمكان الأخذ بالدليل الإلكتروني، تماشياً مع التكنولوجيا الحديثة وإثبات الجريمة الإلكترونية.

---

(١) د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية، القاهرة، مصر، ١٩٩٨م، ص٧٧٠ – ٧٧١.

(٢) د. هلالي عبد االلاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص٤٩. و د. ميسون خلف حمد الحمداني، المرجع السابق، ص٢٢٨ .

(٣) هدى طلب علي، المرجع السابق، ص١٣١.

(٤) خالد عياد الحلبي، المرجع السابق، ص٢٣٦ – ٢٣٧.

(٥) هلال آمنة، المرجع السابق، ص٧٩ – ٨٠.

**ونؤيد هذا الرأي الأخير ونجد أنه لا مانع مع الاعتراف بالدليل الإلكتروني في ظل نظام الإثبات المقيد وذلك مواكبة للتطور العلمي في الإثبات الجزائي، وطالما أن القاضي الجزائي هو الذي يقدر في النهاية قيمة هذا الدليل المستحدث.**

## الفرع الثاني
## موقف نظام الإثبات الحر من مشروعية وجود الدليل الإلكتروني

إن دراسة موقف نظام الإثبات الحر من مشروعية الدليل الإلكتروني في الإثبات الجزائي تقتضي أولاً، التعريف بنظام الإثبات الحر، كما تقتضي ثانياً، معرفة مدى اعتراف نظام الإثبات الحر بالدليل الإلكتروني.

### أولاً: تعريف نظام الإثبات الحر:

يقصد بنظام الإثبات الحر[١] "أن تكون للقاضي الجزائي كامل الحرية في أن يستمد اقتناعه من أي دليل يطمئن إليه من الأدلة التي تقدم في الدعوى، ودون أن يتقيد في تكوين اقتناعه بدليل معين، إلا إذا نص القانون على غير ذلك"[٢].

ويسود هذا النظام في ظل الأنظمة اللاتينية، ويتمتع القاضي وفقاً له بحرية مطلقة في شأن إثبات الوقائع المعروضة عليه، فلا يلزمه القانون بأدلة للاستناد إليها في تكوين قناعته فله أن يبني هذه القناعة على أي دليل وإن لم يكن منصوصاً عليه، بل إن المشرع في مثل هذا النظام لا يهتم بالنص على أدلة الإثبات، فكل الأدلة تتساوى قيمتها الإثباتية في نظر المشرع، والقاضي هو الذي يختار من بين ما يُطرح عليه من الأدلة ما يراه صالحاً للوصول إلى الحقيقة، وهو

---

(١) يطلق على هذا النظام أيضاً حرية القاضي في تكوين اقتناعه ونظام الأدلة الأدبية أو حرية الأدلة.

(٢) د. جميل عبد الباقي الصغير، المرجع السابق، ص١٢.

في ذلك يتمتع بمطلق الحرية لقبول الدليل أو رفضه إذا لم يطمئن إليه، فالمشرع لا يتدخل في تحديد القيمة الإقناعية للدليل، فعلى الرغم من توافر شروط الصحة في الدليل إلا أن القاضي يملك أن يرده تحت مبرر عدم الاقتناع به، وعلى ذلك فالقاضي في مثل هذا النظام يتمتع بدور ايجابي في مجال الإثبات في مقابل انحسار دور المشرع(١).

وبالتالي يقوم نظام الإثبات الحر على مبدأ إطلاق الأدلة (٢)، ومن مبررات نظام الإثبات الحر أنه في المسائل الجزائية، قد ينصب الإثبات على وقائع مادية، وأخرى نفسية تحتاج نظراً لخصوصيتها إلى عدم التقيّد، بحيث يكون إثباتها متاحاً بكافة وسائل وطرق الإثبات. وبالتالي حتى لا يحكم على بريء، ولا يفلت مجرم من العقاب، ولو كانت الأدلة محددة، أو مقيدة لتقيدت صلاحيات النيابة والقاضي من ناحية الأخذ بالأدلة، أو عدمها مما يضطر القاضي في بعض الأحيان إلى الحكم بالبراءة على شخص متهم قد قام بارتكاب الجريمة، نظراً لتقييد القاضي بأدلة مقننة قانوناً(٣).

**ثانياً: مدى اعتراف نظام الإثبات الحر بالدليل الإلكتروني:**

في الواقع في نظام الإثبات الحر لا تثور مشكلة مشروعية الدليل الإلكتروني من حيث الوجود، إذاً ووفقاً لهذا النظام فإن الأصل في الأدلة مشروعية وجودها، فالدليل الإلكتروني سيكون مشروعاً من حيث الوجود استصحاباً للأصل(٤)، على اعتبار أن المشرع لا تُعهد عنه سياسة النص على قائمة أدلة الإثبات ولذلك

---

(١) د. علي حسن الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي (دراسة مقارنة)، المرجع السابق.

(٢) كوثر أحمد خالند، المرجع السابق، ص٣٢.

(٣) آمال عبد الرّحمن يوسف حسن، المرجع السابق، ص١٧.

(٤) خالد عياد الحلبي، المرجع السابق، ص٢٣٨.

فمسألة قبول الدليل الإلكتروني لا ينال منها سوى مدى اقتناع القاضي بها إذا كان هذا النوع من الأدلة يمكن إخضاعه للتقدير القضائي[١].

وبناء على ذلك، يصلح الأخذ بالدليل الإلكتروني في هذا النظام دون وجود أي عائق في الغالب[٢]،لأن كل دليل يمكن أن يتولد منه اقتناع القاضي الجزائي يكون – من حيث المبدأ – مقبولاً أمامه، وبالتالي فليس ثمة ما يمنع من قبول الأدلة الناشئة عن الحاسوب (الدليل الإلكتروني) باعتبارها من الأساليب العلمية الحديثة في الإثبات الجزائي[٣].

## المطلب الثاني
## موقف الاتفاقيات الدولية والفقه والقضاء والقانون من مشروعية وجود الدليل الإلكتروني

تقتضي مشروعية الدليل الإلكتروني الاعتراف بجواز استخدامه كدليل إثبات في المواد الجزائية من قبل الاتفاقيات الدولية، كما لابد من اعتراف الفقه والقضاء والقانون بجواز استخدامه كدليل إثبات، وبناء على ذلك سنقسم هذا المطلب إلى الفرعين التاليين:

**الفرع الأول: موقف الاتفاقيات الدولية من مشروعية وجود الدليل الإلكتروني.**

**الفرع الثاني: موقف الفقه والقضاء والقانون من مشروعية وجود الدليل الإلكتروني.**

---

(١) وهذه المسألة سنتناولها بالتفصيل عند بحث حجية هذا الدليل وذلك في الفصل الثاني من الباب الثاني من هذا البحث.

(٢) هلال آمنة، المرجع السابق، ص٨٤.

(٣) د. جميل عبد الباقي الصغير، المرجع السابق، ص٢١.

## الفرع الأول
## موقف الاتفاقيات الدولية من مشروعية وجود الدليل الإلكتروني

من المنطقي أن تكون مسألة قبول الأدلة الناتجة عن الحاسبات الآلية إحدى المسائل المهمة التي تعرضت لها وناقشتها المؤتمرات الدولية المختلفة، لذا فإن المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد في ريو دي جانيرو بالبرازيل في الفترة من ٤ – ٦ أيلول ١٩٩٤م[١]، والذي أكد ووقع جملة من الأسس الواجب احترامها ومراعاتها في مكافحة الجرائم المتعلقة بالكمبيوتر أهمها السماح للسلطات باستخدام الأدلة الإلكترونية المتحصل عليها أمام المحاكم[٢].

كما أن هذه المسألة أيضاً كانت محل بحث على المستوى الدولي في فريبورج (Warzbourg) بألمانيا لبحث جرائم الكومبيوتر والتي عقدت في الفترة من ٥ – ٨ تشرين الأول ١٩٩٤م، كما أصدرت الأمم المتحدة مرشداً عاماً حول مكافحة والحد من جرائم الكومبيوتر في يناير ٢٠٠٠م[٣].

وعلى الصعيد الأوربي أصدر المجلس الأوربي التوصية رقم (ر (٩٥) ١٣) في ٩/١١/ ١٩٩٥م، في شأن مشاكل الأصول الجزائية المتعلقة بتكنولوجيا المعلومات لحث الدول الأعضاء لمراجعة قوانين الأصول الجزائية الوطنية لتلائم التطور في هذا المجال وأهم ما ورد بتوصية المجلس الأوربي هو:

---

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١٢.

(٢) د. جميل عبد الباقي الصغير، المرجع السابق، ص٨. ولموسخ محمد، تنازع الاختصاص في الجرائم الالكترونية، جامعة قاصدي مرباح ورقلة، الجزائر، منشور على الموقع الإلكتروني التالي:
https://revues.univ - ouargla.dz/index.php/numero - 02 - 2009 - dafatir/559 - 2013 - 05 - 02 - 11 - 40 - 10.

(3) International Review of Criminal Policy - United Nations " Manual on the Prevention and Control of Computer Related Crime 2000": http://www.ifs.univie.ac.at/ - przg91/ser4344.html.

"تفرض المصالح المشتركة في جمع الأدلة والمحافظة عليها وتقديم أدلة إلكترونية الاعتراف بقيمة هذه الأدلة القانونية وتكاملها على المستوى الوطني أو في مجال التعاون الدولي"[١].

أما على الصعيد العربي فقد أوصى المؤتمر العربي الثاني لوزراء الداخلية العرب[٢] على ضرورة الاهتمام بالأساليب العلمية والطرق الفنية، من أجل الأخذ بها لمواجهة المشاكل المتعلقة بالأمن ومكافحة الجريمة، وهذا عن طريق الدعم والتشجيع للدراسات والبحث العلمي والسعي للارتباط بالتقدم التكنولوجي على المستوى العالمي.

كما جاء في القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة لعام ٢٠٠٨م[٣]، في الفصل الثالث (حجّية الكتابة والمحرّرات والتواقيع الإلكترونية)، ثم ذكر لهذه الحُجِّيَّة شروطًا، وهي:

أ – ارتباط التوقيع الإلكتروني بالموقِّع وحده دون غيره.

ب – سيطرة الموقِّع وحده دون غيره على أداة إنشاء التوقيع الإلكتروني.

ج – إمكانية كشف أي تغيير في بيانات المحرَّر الإلكتروني أو التوقيع الإلكتروني بعد وضعه على أي محرَّر.

وجاء في المادة العاشرة من هذا الفصل:

(للمحرّر الإلكتروني صفة النسخة الأصلية، إذا توافرت فيه الشروط الآتية:

أ – أنْ تكون المعلومات الواردة به قابلة للحفظ والتخزين بحيث يمكن في أي وقت الرجوع إليها.

---

(١) د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، ٢٠٠٠م، ص٨٢.

(٢) عقدته المنظمة العربية للدفاع الاجتماعي ضد الجريمة في الفترة الممتدة (٢٠ – ٢٦) من شهر نيسان سنة ١٩٧٨م.

(٣) اعتمده مجلس وزراء العدل العرب بقرار رقم (٧٧١/د٢٤ – ٢٠٠٨/١١/٢٧).

ب – أن يكون محفوظًا بالشكل الذي تمّ إنشاؤه أو إرساله أو تسلّمه أو بأي شكل يُسهِّل دقّة المعلومات التي وردت به عند إنشائه أو تسلّمه.

ج – أن تدلّ المعلومات الواردة به على من أنشأه أو تسلَّمه وتاريخ ووقت إرساله وتسلّمه.

د – إمكانية الاعتداد بمصدر المعلومات إذا كان معروفًا).

وهكذا يكون القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة آنف الذِّكر قد اخذ صراحةً بحُجيَّة الكتابة والمحرّرات والتواقيع الإلكترونية، واعتبار المحرَّرات الإلكترونية أدلة إثبات يمكن الاحتجاج بها عند التنازع[١]

## الفرع الثاني
## موقف الفقه والقضاء والقانون من مشروعية وجود الدليل الإلكتروني

من أجل التأكيد على مشروعية الدليل الإلكتروني، لابد من بحث أولاً، موقف الفقه من مشروعية وجود الدليل الإلكتروني كأحد أدلة الإثبات الجزائي، وثانياً، موقف القضاء من مشروعية وجود الدليل الإلكتروني كأحد أدلة الإثبات الجزائي، وثالثاً، موقف القانون من مشروعية وجود الدليل الإلكتروني كأحد أدلة الإثبات الجزائي.

### أولاً: موقف الفقه من مشروعية وجود الدليل الإلكتروني:

إن قدرة الجناة على تطوير طرق الإجرام على هذا النحو من التقنية العالية في بيئة تكنولوجيا المعلومات، كان لا بد من الناحية المقابلة من تطوير طرق الإثبات بما يواكب هذه الطفرة التي حدثت في الجرائم الإلكترونية، وما يستلزمه ذلك من ضرورة

---

(١) ورقة بعنوان: «دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول»، ضمن فعاليات المؤتمر الثالث لرؤساء المحاكم العليا (النقض، التمييز، التعقيب) في الدول العربية المنعقد في جمهورية السودان الشقيقة خلال الفترة ٢٣-٢٥ /٢٠١٢/٩م الموافق ٧- ١٤٣٣/١١/٩هـ، ص٢٤.

قبول الأدلة الناتجة عن هذا التطوير، ومن أهمها المخرجات الكومبيوترية بأنواعها المختلفة[١].

ويذهب البعض[٢] إلى القول بأنه في عصر التكنولوجيا الحديثة أصبحت وسائل الإثبات التي كانت محلاً للاختبار من عشرات السنين أمراً واقعاً وعادياً، فالأدلة المستمدة من أجهزة التصوير وأجهزة قياس السرعة والبصمة الوراثية والحاسبات الإلكترونية أي الدليل الإلكتروني – وغيرها من وسائل العلم الحديثة – أصبحت مقبولة اليوم أمام المحاكم، نظراً للثقة الكبيرة وإمكانية الاعتماد عليها دون غيرها، حيث لا تحتاج – عند كل استخدام لها– أن يتولى الخبراء شرح المبادئ العلمية التي تقوم عليها تلك الوسائل أو النظريات العلمية التي تعتمد عليها.

كما ذهب البعض الآخر[٣] إلى القول بأن: "الأدلة ذات الطبيعة الالكترونية يتعين مساواتها بالأدلة ذات الطبيعة المادية – الأدلة القائمة على الكتابة والورق – من حيث المقبوليَّة والحُجِيَّة .. وكلما كان التصرف المادي في البيئة الواقعية محل اعتبار يتعين الاعتراف بما يقابله من تصرف معنوي في البيئة الرقمية"[٤].

---

(١) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، بحوث مؤتمر القانون والكومبيوتر والإنترنت، من ١ – ٣ مايو ٢٠٠٠م، المجلد الثاني، الطبعة الثالثة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٤م، ص٧١٥.

(٢) د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، المرجع السابق، ص٤. ود. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٤٤.

(٣) د. يونس عرب، التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية، ورقة عمل مقدمة أمام الندوة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي، النادي العربي للمعلومات، دمشق، سورية.

(٤) د. يونس عرب، التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية، ورقة عمل مقدمة أمام الندوة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي، النادي العربي للمعلومات، دمشق، سورية.

وعلى هذا الأساس، ينبغي أنْ يَقْبَلَ بالأدلَّة المستمدَّة من الكمبيوتر لإثبات وقائع الدعوى التي تتناول الجرائم الإلكترونية، ويساعده في هذا الأمر طرق وقواعد ومبادئ الإثبات العامَّة، والقناعة الشخصيَّة للقاضي في المجال الجزائي [١].

وهناك من يرى[٢] أنه يمكن أن تستخدم المعلوماتية للبحث عن أدلة الجرائم التي ترتكب بواسطة الحاسب الآلي، وفي هذه الأحوال سيكون الدليل الإلكتروني – في أغلب الأحيان – الأثر الوحيد الموجود الذي يمكن أن يساعد على اكتشاف الحقيقة، ومن ثم يكون طريقة إثبات ضرورية وكافية.

فظهور التقنيات العلمية الحديثة مثل الإنترنت، والتي تتيح للفرد سيل هائل من المعلومات والأفكار، فإنه لا يوجد ما يمنع من استخدامها في المجال الجنائي، وذلك إذا ما تم تتبع الجريمة محل البحث والكشف عنها من قبل الضابطة العدلية عبر شبكة الإنترنت، ونشر الإعلانات التي تتضمن دعوة صريحة إلى الفسق والفجور، ومعرفة المواقع الموجودة على شبكة الإنترنت، وتحديدها ومعرفة مستخدمي تلك المواقع والتوصل إليهم وضبط تلك الأنشطة المنافية للآداب العامة. فليس هناك ما يمنع من استثمار التطورات العلمية في خدمة العدالة الجنائية، بل إن هذه التطورات تساعد العدالة على مكافحة الجريمة، وبالتالي يكون الدليل المستمد منها دليل مشروع طالما أنه يهدف إلى تحقيق العدالة، ولا ينال من مشروعية الدليل المستمد من الإنترنت القول بأن تدخل القانون الجنائي في هذا الصدد يعتبر تدخلاً في حرية الأفراد، حيث يمكن الرد على ذلك بأن استخدام الوسائل العلمية الحديثة مثل الإنترنت، واستخدامه كدليل على وقوع جريمة الإعلان عن البغاء ونشر المطبوعات الفاضحة يستهدف

---

(١) ورقة بعنوان: «دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول»، المرجع السابق، ص٢٥.

(٢) د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، المرجع السابق، ص١٠٠.

المصلحة العامة، وحتى تتمكن الدولة من حماية النظام الاجتماعي حتى لا ينهار هذا النظام بسبب احترام مبالغ فيه للحقوق والحريات، ولا يمكن الاعتراض عليه بحجة عدم مشروعية الدليل المستمد من الإنترنت ونسبته للمتهم. فكل ما يسفر عنه العلم الحديث يجب أن يستخدم في تحقيق أمن المجتمع ولا شك في مشروعيته. وإذا تم التسليم بالقول بان هناك تعدي على حريات الأفراد، فإنه تعد ضئيل للغاية، ومما يتعين الاعتداد به هو مدة خطورة العدوان أو المساس بالنظام الاجتماعي، فلا يمكن استبعاد كل وسيلة لمجرد منافتها للقواعد العامة دون دراسة أو تعمق(١).

وبالتالي فإن الدليل الإلكتروني متى وجد بالصورة التي يقبلها القانون فإنه يصلح للإثبات متى اقتنع به القاضي وإن لم يعززه دليل آخر تطبيقاً لمبدأ حرية الاقتناع(٢).

ويتجه الفقه في فرنسا إلى قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية، مثل الرادارات، وأجهزة التصوير، وأشرطة التسجيل، وأجهزة التصنت(٣).

وأخيراً هناك من يرى(٤) أنه نظراً للطبيعة الخاصة للجرائم الإلكترونية فإن دليل إثباتها يختلف ويتميز عن الدليل الجزائي التقليدي، فالدليل الإلكتروني يعثر عليه في بيئة متطورة بطبيعتها وتشمل على أنواع متعددة من البيانات الرقمية تصلح مجتمعة أو منفردة لكي تكون دليلاً للإدانة أو البراءة.

---

(١) د. محمد الألفي، مدى مشروعية الدليل المستمد من الإنترنت، القاهرة، مصر، بلا تاريخ، ص٣.

(٢) أ. طارق محمد الجملي، المرجع السابق، ص٥٧.

(٣) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٣٨. ود. محمد طارق الخن، المرجع السابق، ص١٢١.

(٤) سهى إبراهيم داود عريقات، المرجع السابق، ص١١.

ويخلص الفقه إلى أنه يمكن استخدام الأدلة الإلكترونية في أي مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شيء له علاقة بجريمة أو جان أو مجني عليه[١].

## ثانياً: موقف القضاء من مشروعية وجود الدليل الإلكتروني:

سبق للاجتهاد القضائي الاعتداد بالدليل الإلكتروني في غير المسائل الجزائية، حينما أكد الاجتهاد القضائي في مجال الإثبات التجاري على قبول الدليل الإلكتروني حيث جاء في أحد الاجتهادات أن: "المعلومات المشتقة من الحاسب الآلي أو غيره من أجهزة التقنية الحديثة بمثابة المشتقات من دفاتر تجارية"[٢].

كما اعتدت المحاكم بالدليل الإلكتروني سواء بناء على نص تشريعي تارة، وعلى الاجتهاد القضائي تارة أخرى[٣].

وجاء في اجتهاد لمحكمة النقض المصرية أنه: "للمحقق أن يستعين بأية وسيلة علمية مشروعة مفيدة في الإثبات طالما توافرت دلائل جدية على ارتكاب المتهم لجريمة معينة، وبشرط ألا تنال من حرية الأفراد، ولو لم يرد لها ذكر في القانون"[٤].

---

(١) د. محمد أحمد المنشاوي، المرجع السابق، ص٥١٨. و د. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، منشورات أكاديمية نايف للعلوم الأمنية، الرياض، السعودية، ٢٠٠٤م، ص٢٣٤.

(٢) محكمة تمييز دبي، قرار رقم ١٨١/ ١٩٩٩ تاريخ ١٩ حزيران ١٩٩٩م. مشار إليه لدى: المحامي نزيه نعيم شلالا، الإثبات بواسطة الفاكس، البرقيات، الشريط المغناطيسي، الإثبات على أقراص مدمجة، الإثبات الإلكتروني، دراسة مقارنة (من خلال الفقه والاجتهاد والنصوص القانونية)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٨م، ص٤٣.

(٣) د. محمد طارق الخن، المرجع السابق، ص١١١.

(٤) نقض مصري ٢٠ آذار سنة ١٩٥٦، مجموعة أحكام محكمة النقض المصرية، س٧، رقم ١١٦، ص٣٦٤.

د. جميل عبد الباقي الصغير، المرجع السابق، ص٨٠.

كما أن القضاء الفرنسي قد قَبِل الدليل الإلكتروني إذا توافرت فيه مجموعة من الشروط، من أهمها أن يتم الحصول عليه بطريقة مشروعة ونزيهة، وأن يتم مناقشته حضورياً من قبل الأطراف. وقد قضت محكمة النقض الفرنسية بأن أشرطة التسجيل الممغنطة، التي يكون لها قيمة دلائل الإثبات، يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي(١).

وقد جاء في اجتهاد لمحكمة النقض الفرنسية بأن: "أشرطة التسجيل الممغنطة التي تكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي"(٢).

وأيضاً قبل القضاء الإثبات بالأدلة المتحصلة عنها عن طريق الرادار، والتصوير، والسينموتر، وكاميرات الفيديو، ومسجلات الصوت، والوسائل الإلكترونية في التصنت(٣).

كما أن الغالب الأعم في القضاء الأمريكي أنه يعول على قبول دليل السجلات المحتفظ بها على الحاسوب(٤).

ومن أشهر التطبيقات القضائية لاستخدام الدليل الإلكتروني في كشف الجرائم هي القبض على القرصان الشهير (Kevin Mitnick) بمعرفة المخابرات الأمريكية التي أظهرت الطريقة التي يتم فيها استخدام المعلوماتية للكشف عن الدلائل، ففي كانون الثاني سنة ١٩٩٤ اكتشف أحد الباحثين (Chimomura) في مركز الحاسبات الآلية الموجود في (San Diego) – بجنوب كاليفورنيا – أنه تم اختراق الحاسوب الشخصي الخاص به من جهاز يقع بمدينة شيكاغو، والتحكم فيه عن بُعد، وبعد شهر عثر على المعلومات المسروقة على موقع (Well) على

---

(1) Cass. Crim. 28 avr. 1987, Bull. Crim.no.173

مشار إليه لدى: د. محمد طارق الخن، المرجع السابق، ص١٢١.

(٢) مشار إليه لدى: د. محمد أحمد المنشاوي، المرجع السابق، ص٥٣٨.

(٣) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٥٨.

(٤) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٣٤ – ٥٣٥.

الإنترنت، فقام المجني عليه بمراقبة الشبكة، إلا أنه يبدو أن القرصان (Pirate) كان يعمل من عدة مدن، وبمراجعة المكالمات التليفونية المسجلة بمعرفة شركة التليفونات عن طريق الكومبيوتر وجد أن الجاني يقوم بالبث باستخدام (Modem) مودم متصل بتليفون محمول (Téléphone cellulaire) . ولاختراقه المدينة بارپال (هوائي) خاص متصل بجهاز الكومبيوتر محمول أمكن لفريق البحث أن يحدد المكان الذي تصدر منه النداءات وأن يقوم بالقبض على القرصان. وعلى ذلك يتضح أن استخدام المعلوماتية (الدليل الإلكتروني) في هذه الحالة كانت هي الوسيلة الوحيدة للوصول إلى المجرم(١).

## ثالثاً: موقف القانون من مشروعية وجود الدليل الإلكتروني:

القاعدة في الدعاوى الجزائية هي جواز الإثبات بكافَّة طرق الإثبات القانونيَّة؛ فيحق للمدعي أنْ يثبت دعواه بكافَّة هذه الطرق، ويحق للقاضي أنْ يُكَوِّنَ قناعته مِنْ أيِّ دليلٍ أو أمارةٍ أو إجراءٍ يُقَدَّم إليه، أو يطلع إليه بنفسه. ثم اقتضت الضرورة تقييد الوسائل بعددٍ مِنَ الطُّرق، والقيد على هذه القاعدة: أنَّ الدليل يتعيَّن أنْ يكون من الأدلة التي يقبلها القانون، وبالتالي تظهر أهميَّة اعتراف القانون بالأدلة ذات الطبيعة الإلكترونيَّة. والمعلومات وإنْ كانت قيمتها تتجاوز شيئًا فشيئًا الموجودات والطاقة؛ فإنها ليست ماديّات لتقبل بيِّنة في الإثبات، ووسائط تخزينها – غير الورق كمخرجات – لا تحظى (من حيث محتواها) بقبولها دليلا ماديًّا، من هنا كان البحث القانوني في العديد من الدول يتجه إلى الاعتراف بالحجية القانونية لملفات الكمبيوتر ومستخرجاته والرسائل الالكترونية ذات المحتوى المعلوماتي ليس بصورتها الموضوعة ضمن وعاء مادي، ولكن بطبيعتها الإلكترونيَّة المحضة(٢). وبالتالي، تظهر أهمية اعتراف القانون بالدليل الإلكتروني

---

(١) د. جميل عبد الباقي الصغير، المرجع السابق، ص١٠٠.

(٢) ورقة بعنوان: «دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول»، المرجع السابق، ص٢١.

خاصة مع احتمال ظهور أنماط جديدة لجميع الجرائم وخاصة في قطاع المعلومات المعالجة بواسطة الكومبيوتر[١].

وتذهب التشريعات المقارنة إلى قبول مصادر المعلومات الخاصة بالحاسوب أو المتحصل عليها من أنظمته، مثل مخرجات نظام المعالجة الآلية للبيانات، والبيانات المكتوبة على شاشته، والبيانات المسجلة على دعائم ممغنطة أو المخرجة داخل نظام المعالجة، كأداة يقوم عليها الإثبات الجزائي[٢].

وسندرس موقف التشريعات اللاتينية، ومن ثم موقف التشريعات الأنكلوسكسونية، وذلك كما يلي:

**أ- موقف التشريعات اللاتينية:**

يسود التشريعات اللاتينية أو ما يعرف بدول القانون الخاص وكثير من الدول الأخرى التي تأخذ بهذا النظام، مبدأ التقديم الحر أو التقييم الحر للأدلة، ففي هذه الدول يستطيع القاضي من حيث المبدأ الأخذ بجميع أنواع الأدلة ومن ثم تقييم مدى اعتماد المحكمة على تلك الأدلة، وأن الأنظمة القانونية المبنية على هذه المبادئ لا تتردد عموماً في تقديم سجلات الكومبيوتر كدليل[٣].

ومن التشريعات اللاتينية التي اعترفت بمشروعية وجود الدليل الإلكتروني، التشريع الفرنسي حيث تقوم الإجراءات الجزائية في **التشريع الفرنسي** على مبدأ أساسي هو مبدأ حرية الإثبات المنصوص عليه في المادة (٤٢٧) من قانون الإجراءات الجزائية الفرنسي.

ولم ينص **المشرع المصري** صراحة على الدليل الإلكتروني في قانون الإجراءات الجنائية المصري، ولا في مشروع قانون مكافحة الجرائم الإلكترونية لسنة ٢٠١٦م. إلا أنه يمكن تأسيس العمل بالدليل الإلكتروني في القانون المصري على

---

(١) د. ميسون خلف حمد الحمداني، المرجع السابق، ص٢٣٠.

(٢) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٢٥.

(٣) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١٢٨.

أساس مبدأ حرية الإثبات الذي يأخذ به المشرع المصري في المجال الجزائي وهذا ما نصت عليه المادة (٣٠٢) من قانون الإجراءات الجنائية المصري.

**وحبذا لو يأخذ المشرع المصري بهذا الدليل بشكل صريح في المجال الجزائي.**

وأورد **المشرع الجزائري** طرق الإثبات في المسائل الجزائية في قانون الإجراءات الجزائية الصادر بموجب الأمر رقم ١٥٥/٦٦ المؤرخ في ١٩٦٦/٧/٨م المعدل والمتمم، في الكتاب الثاني الباب الأول، الفصل الأول المعنون بـ "طرق الإثبات" من المادة (٢١٢) إلى غاية المادة (٢٣٨)، وهذه الطرق تتمثل في الاعتراف، المحاضر، الشهادة والخبرة.

أما بالنسبة **للمشرع الليبي** فلا يوجد نص صريح في قانون الإجراءات الجنائية الليبي بقبول الدليل الإلكتروني، لكن هنالك تطبيقات خاصة بقبول الدليل الإلكتروني في القانون الليبي[١].

---

(١) من ذلك مثلاً نص المادة (١/٩٧) من القانون رقم (١) لسنة ١٣٧٣ و.ر. (قانون المصارف منشور في مدونة التشريعات، العدد الرابع، السنة الخامسة، ٢٠٠٥م)، بشأن المصارف التي نصت على أنه: "يعتد بالمستندات والتوقيعات الرقمية التي تتم في إطار المعاملات المصرفية وما يتصل بها من معاملات أخرى، وتكون لها الحجية في إثبات ما تتضمنه من بيانات". فهذا النص أضفى على المستند الإلكتروني الحجية في الإثبات، والواقع أن هذا النص لا يقتصر على مجال الإثبات المدني أو التجاري كما يوحي بذلك النص في فقرته الأولى، إنما يشمل الإثبات في المسائل الجزائية أيضاً، فإثبات المعاملة المصرفية قد يصلح كدليل لإثبات واقعة إجرامية، فالتداخل في الوقائع موضوع الإثبات هو ما يمكن الاستناد إليه لتوسيع نطاق النص، كإثبات جرائم غسل الأموال التي يتم ارتكابها عن طريق المصارف، حيث تصلح المستندات الرقمية المتعلقة بالعمليات الخاصة بغسل الأموال كدليل لإثبات هذه الجريمة.

كما نصت المادة (٦) مكرر من القانون رقم (١٠) لسنة ١٤٢٨م بإضافة مادة للقانون رقم (٧٠) لسنة ١٩٧٣م، بشأن إقامة حد الزنا وتعديل بعض أحكام قانون العقوبات التي نصت على أنه: "تثبت جريمة الزنا المنصوص عليها في المادة الأولى من هذا القانون باعتراف الجاني أو بشهادة أربعة شهود أو بأية وسيلة إثبات علمية أخرى". وبالتالي فإن الدليل الإلكتروني بوصفه من ضمن

أما **المشرع السوري** فقد اعترف بالدليل الإلكتروني في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية عندما خصص الفصل الرابع منه للضابطة العدلية والدليل الرقمي، كما ذكرنا أن المشرع السوري عرف **الدليل الإلكتروني** في المادة الأولى من قانون مكافحة الجريمة المعلوماتية، وهذا يؤكد على اعتراف المشرع السوري بهذا الدليل والاعتداد به في إثبات الجرائم الإلكترونية.

كما قد حرص **المشرع الفلسطيني** على التأكيد على إمكانية استخدام الأدلة الإلكترونية كطريق من طرق الإثبات أمام القضاء، فقد أقر المجلس التشريعي في مدينتي غزة ورام الله وبالمناقشة العامة مشروع قانون المعاملات الإلكترونية بالقراءة الأولى تمهيداً لإقراره بشكل نهائي والعمل به كأول قانون من نوعه في فلسطين(١).

كما اعترف المشرع البحريني بالدليل الإلكتروني حين أعطى أدلة الإثبات الإلكتروني نفس حجية الأدلة التقليدية وككيان مستقل عنها(٢).

ولذلك يمكن القول إن المخرجات المتحصلة من الوسائل الإلكترونية (الدليل الإلكتروني) لا تمثل مشكلة في النظام اللاتيني حيث يسود مبدأ حرية القاضي الجزائي في الاقتناع(٣).

**ب- موقف التشريعات الأنكلوسكسونية:**

يقوم المشرع في التشريعات الأنكلوسكسونية بالدور الإيجابي في عملية الإثبات بالدعوى فهو الذي ينظم قبول الأدلة وينحصر دور القاضي في مراعاة

---

الأدلة العلمية بأشكاله المختلفة سيبدو ذو حجية في إثبات هذه الجريمة. انظر: أ. طارق محمد الجملي، المرجع السابق، ص٥٤ – ٥٦ – ٥٧.

(١) سهى إبراهيم داود عريقات، المرجع السابق، ص٣٣.

(٢) جاء ذلك في المادة (٢٢) من قانون جرائم تقنية المعلومات البحريني رقم (٦) لعام ٢٠١٤م.

(٣) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٢٦.

توافر الأدلة وشرائطها القانونية بحيث إذا لم تتوافر لا يجوز أن يحكم بالإدانة بل يحكم باستبعاد الدليل(١).

ويثير قبول الأدلة المتحصلة من الوسائل الإلكترونية مشكلات عديدة في ظل القواعد الأنجلو أمريكية للإثبات الجزائي، التي تعتنق – كمبدأ أساسي – الإثبات بالشهادة التي تتعلق بالواقعة محل الإثبات، ولذلك فإن قبول المستندات المطبوعة لمخرجات الوسائل الإلكترونية، التي هي إشارات إلكترونية ونبضات ممغنطة يمثل مشكلة أمام القضاء في هذا النظام، إذ لا يمكن للمحلفين أو القاضي مناظرة الأدلة المتولدة منها ووضع أيديهم عليها، وهذا يجعلها بمنزلة أدلة ثانوية وليست أصلية(٢).

لكن اتجهت بعض المحاكم في بعض التشريعات الأنكلوسكسونية أو ما يعرف بدول القانون العام إلى قبول الأوراق المطبوعة للكومبيوتر وأدرجتها ضمن الأدلة التي يمكن الأخذ بها، كما تأخذ بنسخ مستمدة من السجلات التجارية كمثال، كذلك طورت بعض الدول الأخرى قوانين جديدة تسمح بالاعتراف بسجلات الكومبيوتر كدليل إذا استوفيت بعض الشروط(٣).

**ففي الولايات المتحدة الأمريكية**، تناولت بعض القوانين الأدلة الإلكترونية، ومن ذلك – على سبيل المثال – ما نص عليه قانون الحاسوب لسنة ١٩٨٤م، الصادر في ولأية (إيوا) من أن مخرجات الحاسوب تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرامج والبيانات المخزنة فيه (المادة ٧١٦/أ/١٦)، كما يتضح من قانون الإثبات الصادر في عام ١٩٨٣م في ولأية كاليفورنيا، أن النسخ المستخرجة

---

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٢٦٨.

(٢) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٢٦.

(٣) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١٢٩.

من البيانات التي يحتويها الحاسوب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه البيانات[١].

ولقد تضمنت **القواعد الفيدرالية الأمريكية** نصاً يعتبر السجلات والبيانات المنظمة بدقة بينة مقبولة أمام المحاكم الجزائية استثناء للبينة السماعية، وبناءً على تلك القواعد تُعد التقارير والمعلومات والبيانات المحفوظة في أي شكل، وكذلك الوقائع والأحداث والآراء ونتائج التحاليل المنقولة بوساطة أصحاب المعرفة والخبرة في نطاق الأنشطة والممارسات المنظمة بيّنة مقبولة أمام المحاكم الجزائية، لكونها بيانات أكثر دقة ومحفوظة بأسلوب علمي يختلف عن غيرها من الأدلة السماعية، والأدلة الجزائية الإلكترونية من هذا القبيل، لكونها معدة بعمليات حسابية دقيقة لا يتطرق إليها الشك ويتم حفظها آلياً بأسلوب علمي[٢].

وبهذا يكون المشرع في **الولايات المتحدة الأمريكية** قد قبل مخرجات الوسائل الإلكترونية كوسائل إثبات وذلك بالنسبة للبرامج والبيانات المخزونة فيها، وبالنسبة للنسخ المستخرجة من البيانات التي يحتويها الحاسوب[٣].

كما أن **المشرع البريطاني** أصدر قانون إساءة الحاسوب في عام ١٩٩٠م، الذي لم يتناول الأدلة الناتجة عن الحاسوب، وربما كان السبب هو وجود قانون البوليس والإثبات الجنائي لسنة ١٩٨٤م، الذي تم العمل به سنة ١٩٨٦، وقد حوى تنظيماً محدداً لمسألة قبول مخرجات الحاسوب والإنترنت، كأدلة إثبات في المواد الجزائية[٤].

---

(١) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٢٩.

(٢) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٤٩ – ٥٥٠.

(٣) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٢٧.

(٤) صدر تشريع الإثبات بالحاسوب في انكلترا عام ١٩٨٣م، وركز بصفة أساسية على قبول مخرجات الحاسوب كدليل لإثبات أية حقيقة مسجلة فيه، تزود بشهادة شفوية تكون مقبولة،

**وفي كندا**، يمكن قبول السجلات الناجمة عن الحاسوب، إذا توافرت شروط معينة[١].

**ونرى مما تقدم أن الكثير من التشريعات الأنكلوسكسونية تأخذ بالبينات والسجلات الإلكترونية أي بالدليل الإلكتروني كبينة سماعية على سبيل الاستثناء من الأصل العام في هذه التشريعات، وهو عدم قبول البينة السماعية.**

وقد خلت مواد قانون مكافحة الجرائم المعلوماتية الإماراتي رقم ٢ لسنة (٢٠٠٦م)، ونظام مكافحة الجرائم المعلوماتية السعودي (١٤٢٨هـ/٢٠٠٧م) من بيان تعيين طرق إثبات الجرائم المعلوماتية وبالتالي من تحديد الدليل الإلكتروني لإثباتها.

فتتجه العديد من الدول إلى الإقرار بحجية قانونية للملفات والمستخرجات الحاسوبية والرسائل الإلكترونية ذات المحتوى المعلوماتي ليس بصورتها الموضوعة ضمن وعاء مادي ولكن بطبيعتها الإلكترونية المحضة، ذلك أن التطور العلمي قد أثر بلا شك على نظام الاقتناع القضائي[٢].

وهكذا فإن الأنظمة القانونية المختلفة قد قبلت الأدلة المتحصلة من الوسائل الإلكترونية كأداة إثبات، وإن كان النظام الأنجلو أمريكي قد أورد الكثير من الشروط لقبولها كأداة إثبات نظراً لطبيعة هذا النظام، الذي يعتمد في الأصل على النظام الاتهامي القائم على مبدأ التواجهية وإعلائه للإثبات بالشهادة وتحقيق الأدلة أمام القضاء[٣].

---

ويتم تقديرها من قبل المحكمة المختصة.: د.محمد أحمد المنشاوي، المرجع السابق، ص٥٣٣.

(١) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٥١.

(٢) د. ميسون خلف حمد الحمداني، المرجع السابق، ص٢٣٠.

(٣) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٢٨.

**ونرى أن أغلب التشريعات الأجنبية والعربية قد اعترفوا بالدليل الإلكتروني بصورة غير صريحة على أساس مبدأ حرية الإثبات. ونقترح إجراء تعديل في القوانين التي لا تأخذ بالدليل الإلكتروني في الإثبات الجزائي والنص عليه بشكل صريح.**

**وفي هذا المبحث، تحدثنا عن موقف أنظمة الإثبات من مشروعية الدليل الإلكتروني في الإثبات الجزائي، وكان لابد لنا من استعراض موقف نظام الإثبات المقيد وموقف نظام الإثبات الحر من مشروعية هذا الدليل المستحدث ومدى الاعتراف به في كل منهم، وتحدثنا أخيراً عن موقف الاتفاقيات والفقه والقضاء والقانون من مشروعية الدليل الإلكتروني في الإثبات الجزائي، فعرضنا موقف الاتفاقيات من مدى الاعتراف بالدليل الإلكتروني، ثم بحثنا في موقف الفقه والقضاء من هذا الدليل الإلكتروني، وأخيراً بحثنا موقف التشريعات من الاعتراف بمشروعية الإثبات الجزائي بالدليل الإلكتروني.**

# الفصل الثاني
# مشروعية الحصول على الدليل الإلكتروني

يُشترط في الدليل الجزائي عموماً لقبوله كدليل إثبات أن يتم الحصول عليه بطريقة مشروعة، وذلك يقتضي أن تكون الجهة المختصة بجمع الأدلة قد التزمت بالشروط التي يحددها القانون في هذا الشأن(١)، والمقصود بمشروعية الإجراءات هي أن تكون إجراءات الحصول على الأدلة متوافقة مع القانون، ولا تخرج عن روح نصوصه، وهي إجراءات تقوم بها السلطة المختصة في الدعوى العامة، لإثبات وقوع الجريمة ونسبتها إلى مرتكبها، إذ إن المبدأ الأساسي في الدساتير يقوم على أساس عدم تقييد الحرية الشخصية للإنسان إلا بموجب نص صريح في القانون، وبذلك فلا يجوز أن يباشر ضده أي إجراء من شأنه المساس بآدميته وكرامته، وعلى ذلك، فكل مالم يجزه المشرع من الإجراءات يعد غير مشروع ولا يترتب عليه أي أثر قانوني ولا يمكن التعويل على الأدلة المستمدة منه عند الحكم تأسيساً على القاعدة القاضية: "المبني على الباطل باطل"(٢).

فالحصول على الدليل يجب أن يكون بصورة مشروعة وغير مخالفة لأحكام الدستور ولا لقانون العقوبات، فصيانة كرامة الإنسان وحماية حقوقه من أهم أهداف الدستور، لذلك تتضمن الدساتير الحديثة نصوصاً تنظم القواعد الأساسية في الاستجواب والتوقيف والحبس والتفتيش وغيرها، بحيث يتقيد المشرع بها عند وضع قانون الأصول الجزائية(٣).

---

(١) خالد عياد الحلبي، المرجع السابق، ص٢٣٨ – ٢٣٩.
(٢) كوثر أحمد خالند، المرجع السابق، ص٥٨.
(٣) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٥١.

ومبدأ المشروعية في مجال إجراءات الحصول على الأدلة يشبهه البعض[١] بمثلث ذي ثلاثة أضلاع تدور في فلكه إجراءات الحصول على الأدلة وإثباتها إلى أن تصبح صالحة لإنتاج أثارها القانونية، وهذه الأضلاع هي: أن تكون الأدلة وليدة إجراءات قانونية سليمة، وأن تقوم على أسس علمية ثابتة ومستقرة، وأن تكون وليدة إجراءات تتفق والمبادئ الأخلاقية.

ومبدأ مشروعية الدليل الإلكتروني يعني ضرورة اتفاق الإجراء مع القواعد القانونية والأنظمة في وجدان المجتمع المتحضر[٢]. فلكي يكون الدليل الإلكتروني مقبولاً، يجب أن تكون وسيلة الحصول عليه مشروعة، بمعنى أنه يجب أن تكون الإجراءات التي اتبعت للحصول عليه مطابقة للإجراءات المنصوص عليها قانوناً، فإذا كان هذا الدليل قد وصل إليه بوسيلة غير مشروعة إنهار وأصبح لا قيمة له[٣].

وعلى الرغم من وجود تشابه كبير بين التحقيق في جرائم الانترنت وبين التحقيق في الجرائم الأخرى، فهي جميعاً تحتاج إلى إجراءات تتشابه في عمومها مثل المعاينة والتفتيش والمراقبة والتحريات، كما أنها تشترك في كونها تسعى إلى الإجابة على الأسئلة المشهورة لدى المحقق، ماذا حدث؟ وأين؟ ومتى؟ وكيف؟ ومَّن؟ ولماذا؟[٤].

---

(١) كوثر أحمد خالند، المرجع السابق، ص٦٠.

(٢) د. ميسون خلف حمد الحمداني، المرجع السابق، ص٢٣٤.

(٣) د. ميسون خلف حمد الحمداني، المرجع السابق، ص٢٣٥.

(٤) د. حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، منشور على الموقع الإلكتروني التالي:
http:// www.eastlaws.com، ص١.

لكن تظل الجرائم المتعلقة بشبكة الانترنت تمتاز عن غيرها من الجرائم ببعض الخصائص فأساليب التحقيق الجنائي وإجراءاته تتطور بصورة تتلاءم مع خصوصية هذه الجرائم من أجل تمكين المحقق من كشف الجريمة والتعرف على مرتكبيها بالسرعة والدقة اللازمين، فالتحقيق في هذا النوع من الجرائم يستدعي الرجوع إلى عدد كبير من السجلات التي يجب الاطلاع عليها مثل الكتيبات الخاصة بأجهزة الحاسوب كملفات تسجيل العمليات الحاسوبية، وسوف يتم ذلك في كثير من مراحله في بيئة رقمية عن طريق التعامل مع الحواسيب والشبكات ووسائط التخزين ووسائل الاتصال(١).

ويقصد بمشروعية الحصول على الدليل الإلكتروني في بحثنا هذا هو مدى مشروعية الإجراءات التقليدية والحديثة بغية الحصول على الدليل الإلكتروني(٢)، فالبحث في مشروعية الحصول على الدليل الإلكتروني لا تقتصر على الإجراءات التقليدية من خبرة ومعاينة وتفتيش وضبط بل تمتد أيضاً إلى الإجراءات الحديثة التي تبنتها بعض التشريعات لأجل الحصول على الدليل الإلكتروني.

وسنتعرض لمشروعية الحصول على الدليل الإلكتروني في الإجراءات التقليدية من خبرة ومعاينة وتفتيش وضبط، والإجراءات الحديثة سواء ما تعلق منها

---

(١) د. حسين بن سعيد الغافري، المرجع السابق، ص١.

(٢) لابد من ضرورة التمييز بين إجراءات الحصول على الأدلة أو (وسائل الإثبات) وبين عناصر الإثبات، فإجراءات الحصول على الأدلة هي عبارة عن النشاط الذي يبذل في سبيل اكتشاف حالة أو شخص أو مسألة، وكل ما يفيد في إظهار عناصر الإثبات أي الأدلة ونقلها إلى المجال الواقعي، فالاستجواب والتفتيش والمعاينة ومراقبة الاتصالات الهاتفية فهذه الإجراءات لا تعد أدلة وإنما تعد مصدراً ينتج عنه الدليل، أما عناصر الإثبات فهي الوقائع أو الظروف أو الأشياء التي تكشف عنها وسائل الإثبات من حيث وقوع جريمة معينة، وتأكيد صدورها أو نفيها من شخص معين وهذه العناصر هي التي يمكن الاستناد إليها في إصدار الأحكام، وهي التي يبني عليها القاضي اقتناعه بشأن الدعوى. كوثر أحمد خالند، المرجع السابق، ص٥٤ – ٥٥. و معمر علي إبراهيم محمد، المرجع السابق، ص٣٦.

بالبيانات الساكنة أو المتحركة، وبناء على ذلك سنقسم هذا الفصل إلى المبحثين التاليين:

**المبحث الأول: الحصول على الدليل الإلكتروني في الإجراءات التقليدية.**

**المبحث الثاني: مشروعية الحصول على الدليل الإلكتروني في الإجراءات الحديثة.**

# المبحث الأول

## الحصول على الدليل الإلكتروني في الإجراءات التقليدية

الإجراءات التقليدية هي الخبرة والمعاينة والتفتيش والضبط، وهنا سنحاول دراستها وبحث مشروعية هذه الإجراءات لغرض الحصول على الدليل الإلكتروني، ولكن قبل التعرض لمشروعية الحصول على الدليل الإلكتروني في الإجراءات التقليدية، لا بد لنا من عرض الصعوبات التي تواجه الحصول على الدليل الإلكتروني في هذه الإجراءات.

لذلك لابد لنا من تقسيم هذا المبحث إلى المطلبين التاليين:

**المطلب الأول: صعوبات الحصول على الدليل الإلكتروني في الإجراءات التقليدية.**

**المطلب الثاني: مشروعية الحصول على الدليل الإلكتروني في الإجراءات التقليدية.**

# المطلب الأول

## صعوبات الحصول على الدليل الإلكتروني في الإجراءات التقليدية

بالرغم من انتشار الأجهزة المحمولة باليد، والمتصلة بشبكات اللاسلكي يُعد بمثابة تطور نوعي كبير في عصر الكومبيوتر، إلا أن هذا الأمر يعد من أكبر تحديات البحث والتحقيق في الأنشطة الإجرامية في مجال الكومبيوتر المنتشرة على مستوى العالم، وتمثلت أغلبية هذه الصعوبات في كيفية الحصول على الأدلة من هذه الأجهزة ذات العلاقة بالواقعة محل البحث الجنائي(١).

حيث تواجه الخبير الفني وغيره، صعوبات متعددة ومختلفة، للحصول على هذه الأدلة من أجهزة الحاسوب، أو الشبكات الإلكترونية. فليس من الهين استخراج واستنباط الدليل الإلكتروني، نظراً للطبيعة الخاصة للجريمة الإلكترونية بالدرجة الأولى، وكذلك الدليل الإلكتروني، فهو دليل علمي وفني، وتقني، كما أنه يتميز بسرعة فقدانه وإتلافه، بالإضافة إلى أن المجرم الذي يقترف هذا النوع من الجرائم، أي الجرائم الإلكترونية، يتميز بالفطنة والذكاء الحادين، ويسعى بكل جهد لعدم ترك أي دليل يقود إليه(٢).

لذلك فالصعوبات التي تعترض تحصيل الدليل الإلكتروني كثيرة ومتنوعة، فمن هذه الصعوبات ما يتعلق بالجريمة الإلكترونية، ومنها ما يتعلق بالدليل الإلكتروني نفسه، وأخيراً منها ما يتعلق بأسباب متعددة، وبالتالي سندرس هذه الصعوبات في الفروع الثلاثة التالية:

**الفرع الأول: صعوبات متعلقة بالجريمة الإلكترونية.**

**الفرع الثاني: صعوبات متعلقة بالدليل الإلكتروني.**

**الفرع الثالث: صعوبات متعلقة بأسباب متعددة.**

---

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١١٩ – ١٢٠.

(٢) هلال آمنة، المرجع السابق، ص٦٩.

# الفرع الأول
# صعوبات متعلقة بالجريمة الإلكترونية

تثير الجرائم الإلكترونية وبصفة خاصة جرائم الإنترنت بعض المشاكل المتعلقة بالإجراءات الجزائية، وخصوصاً في مجال جمع الأدلة حيث توجد صعوبات عملية تتعلق لاسيما بالتفتيش[١]. ومن هذه الصعوبات ما هو متعلق أولاً، بخصائص الجريمة الإلكترونية، وثانياً، منها ما هو متعلق بالجاني والمجني عليه في الجريمة الإلكترونية، وثالثاً، منها ما هو متعلق بضعف التعاون الدولي في مكافحة الجريمة الإلكترونية.

## أولاً: صعوبات متعلقة بخصائص الجريمة الإلكترونية:

ترجع الصعوبات المتعلقة بالجريمة الإلكترونية في الحصول على الدليل الإلكتروني إلى خصائص الجريمة الإلكترونية، حيث إن ارتباط الجرائم الإلكترونية بجهاز الحاسوب وشبكة الانترنت أضفى عليها مجموعة من الخصائص المميزة لها عن باقي الجرائم التقليدية[٢]، ومن هذه الخصائص التي تكون حجر عثرة أمام الحصول على الدليل الإلكتروني، ما يلي:

### أ-ازدواجية محل الجريمة الإلكترونية:

باعتبار أن النظام المعلوماتي ليس من طبيعة واحدة فهو يتكون من عناصر مادية وأخرى غير مادية، وهذا الأمر يسمح بإمكانية أن يكون موضوع الجريمة ذو طبيعتين مختلفتين، أحدهما مادي والآخر غير مادي، كما هو الحال بالنسبة للمعلومات فقد تكون في حالة انتقال أو موجودة في ذاكرة النظام المعلوماتي أي إنها في حالة غير مادية، وقد تكون المعلومات متجسدة في صورة مادية بتخزينها على دعامة معلوماتية، حتى إن المعلومات بطبيعتها غير المادية أو المادية يمكن

---

(١) د. مدحت رمضان، المرجع السابق، ص٧٢.

(٢) هلال آمنة، المرجع السابق، ص٢٥.

أن تخضع لأكثر من نص قانوني، مما يولِّد مشكلة تعدد الأوصاف القانونية على نفس المحل[١].

## ب-الجريمة الإلكترونية جريمة نظيفة:

إنَّ الجرائم الإلكترونية هي (الجرائم النظيفة)؛ وذلك لصعوبة اكتشاف دليل ثبوتها؛ فلا أثر فيها لأيِّ عنف أو دماء، وإنما مجرد أرقام وبيانات يتم تغييرها أو محوها من السجلات المخزنة في ذاكرة الحاسبات الآلية وليس لها أثر خارجي مادي[٢].

فالجريمة الإلكترونية تتم في بيئة أو إطار لا علاقة له بالأوراق أو المستندات وإنما عن طريق الحاسوب أو الإنترنت[٣]، وبالتالي تتميز الجريمة الإلكترونية بأنها لا تترك آثاراً مادية عند القيام بها، وبالتالي من الصعب اكتشافها[٤]، فليس هناك أموال وممتلكات مفقودة، وإنما هي أرقام تتغير في السجلات، ومعظم الجرائم الإلكترونية ربما يتم اكتشافها بالصدفة، وبعد وقت طويل من ارتكابها[٥].

إذ أن هذه النوعية من الجرائم توجد في بيئة لا تعتمد التعاملات فيها – أصلاً – على الوثائق والمستندات المكتوبة، بل على نبضات إلكترونية غير مرئية لا يمكن قراءتها إلا بواسطة الحاسب والبيانات التي يمكن استخدامها كأدلة ضد الفاعل، يمكن في أقل من ثانية العبث بها أو محوها بالكامل، لذلك فإن المصادفة

---

(١) هلال آمنة، المرجع السابق، ص٢٥.

(٢) عبد الرحمن بحر، معوقات التحقيق في جرائم الإنترنت «دراسة مسحيَّة على ضباط الشرطة في دولة البحرين»، أكاديمية نايف العربية للعلوم الأمنيّة، ١٤٢٠هـ -١٩٩٩م. رامي علي وشاح، الصعوبات الماديّة التي تعترض الإثبات بالمحرّرات الإلكترونية، الأكاديمية للدراسات الاجتماعية والإنسانيَّة، ٢٠١٠م، ص٤٤ – ٥٢.

(٣) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٠٦.

(٤) هلال آمنة، المرجع السابق، ص٢٥.

(٥) ثنيان ناصر آل ثنيان، المرجع السابق، ص١.

وسوء الحظ لهما دور كبير في اكتشافها، وذلك أكثر من الدور الذي تلعبه أساليب التدقيق والرقابة[١].

كما أن وقوع الجريمة الإلكترونية في بيئة الكترونية تترتب عليها جمله نتائج تصَّعب من مهمة اكتشاف هذه الجرائم لا بل وحتى التحقيق فيها، وهذا على عكس الجريمة التقليدية التي يكون الدليل فيها مرئياً، من ذلك السلاح الناري أو الأداة الحادة المستعملة في القتل أو الضرب وكذلك المادة السامة التي استعملت في القتل، أو المحرر ذاته الذي تم تزويره أو النقود التي زيفت وأدوات تزييفها، حيث يستطيع عضو الضابطة العدلية أو سلطة التحقيق رؤية الدليل المادي وملامسته بإحدى الحواس[٢]، فرجل الشرطة الذي يقوم بجمع المعلومات في واقعة سرقة حتى يصل إلى المتهم، ويستصدر امراً بالقبض عليه وتتولى جهات التحقيق استجوابه وإحالته إلى محكمة الموضوع، فكل هذه وقائع خاضعة لسيطرة أجهزة العدالة، والدليل فيها مرئي ومقروء، على عكس الجريمة الإلكترونية التي تتم دون رؤية لدليل الإدانة[٣]، لذلك فغالبية الجرائم الإلكترونية تُكتشف مصادفة[٤] وليس بطريق الإبلاغ عنها[١].

---

(١) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٩٢.

(٢) أ.م. جاسم خريبط خلف، المرجع السابق، ص١٠.

(٣) تجدر الإشارة إلى أن انتحال الشخصية، وكذلك التسلسل الإلكتروني من أبرز أمثلة السلوك الإجرامي في الجريمة المعلوماتية، وذلك كدليل على عدم رؤية دليل الجريمة، فكلاهما يستخدم أساليب عالية التقنية في الدخول إلى المناطق المؤمنة والمحمية الكترونياً أو الوصول إلى مراكز الحاسب الآلي والدخول إلى قواعد المعلومات. أ.م. جاسم خريبط خلف، المرجع السابق، ص١١.

(٤) ففي دراسة مسحية، تمت من قبل لجنة تدعى "لجنة التدقيق" في إنكلترا، وذلك في شأن الاحتيال المعلوماتي وإساءة استعمال الحاسب، شملت (٦٠٠٠) من المؤسسات التجارية وشركات القطاع الخاص، وهي بالطبع تعتمد على الحاسب الآلي في إنجاز أعمالها، تبين أن ما يقرب من نصف حالات الاحتيال التي تمت ضد هذه المؤسسات والشركات قد اكتشفت مصادفة، وكبدتها خسائر قدرت بنحو (٦، ٥) مليون جنيه إسترليني. د. عبد الفتاح

**ومـن الأمثلـة الواقعيَّـة** علـى مـا تقدَّم مـا حَصَلَ فـي دولـة الإمـارات العربيـة المتحدة، حيث قام مُشَغِّل حاسوب بتهديد المؤسَّسة التي يعمل لديها بتنفيذ مجموعة مـن مطالبـه، وذلـك بعـد أنْ حـذف كافّـة البيانـات الموجـودة علـى الجهـاز الرئيسـي للمؤسّسـة، وقد رفضـت المؤسسـة الاسـتجابة لمطالبـه، فأقدم علـى الانتحـار، ووجدت المؤسسة صعوبة في استرجاع البيانات التي كانت قد حُذفت(٢).

بالإضافة إلى ذلك، فإن الاحتيال الذي تقوم عليه جريمة النصب قد تطور كنتيجة لاستخدام التقنية العلمية، وأصبح هذا الاحتيال كثير الوقوع في العمليات الإلكترونية، وبالنظر إلى الطبيعة غير المرئية التي يتم بها فقد يصعب إثباته(٣).

كما أن الجريمة الإلكترونية لا تترك أثراً، وإن تركت فقد يكون من الصعب تتبعها، فعلى سبيل المثال في جريمة (سرقة البنوك) بطريق الاحتيال المعلوماتي يصعب الإمساك بالمجرمين بسبب السرعة التي تتم بها عملية الحوالات النقدية(٤).

أضـف إلـى ذلـك أن الجريمـة الإلكترونيـة، تظهـر آثارهـا بعـد ارتكـاب الجريمة(٥).

وإذا كانـت المصـادفة مـن الأمـور التـي يُعَّـول عليهـا فـي كشـف الجريمـة الإلكترونيـة، فـإن وجـود أجهـزة للرقابـة والتـدقيق داخـل جهـة الإدارة، سـواء كانـت

---

بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٠٦ – ١٠٧.

(١) د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، د.ط، دار الكتب القانونية، المحلة الكبرى، مصر، ٢٠٠٢م، ص٢٤ .

(٢) د. علي حسن الطوالبه، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، المرجع السابق.

(٣) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٥٩.

(٤) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٦٧ – ١٦٨.

(٥) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١١٧.

حكومية أو خاصة أو شركة من الشركات، سوف يؤدي إلى كشف وقوع هذه الجريمة، ومن ثم إظهار الدليل الخفي الذي تتم به مثل هذه الجرائم، شريطة أن يكون الجهاز الذي يتولى هذه الرقابة ذا تخصص وخبرة عالية في التعامل مع أجهزة الحاسوب وبرامجها، وملماً بأحدثها وطرق التعامل معها والأمثلة العملية على فاعليه هذه الرقابة والتدقيق كثيرة[١].

---

(١) دلت الدراسة الميدانية التي قامت بها إدارة الصحة وخدمات الإنسان (H.H.S) بالولايات المتحدة الأمريكية عام ١٩٨٣ أن الحوادث العرضية والمصادفة مثل (الشكوى – الفضول –الانتقام من المبلغ ضده أو النشاط غير العادي للجناة) شكلت نسبة ٤٩% كعوامل ساعدت في كشف الاحتيال بواسطة الحاسب الآلي، أما الرقابة الداخلية والخارجية فكان لها ذات الأثر بنسبة ٢٦%، بينما كانت الرقابة (بكافة صورها) بما فيها الرقابة الأمنية على أجهزة الحاسب العامل المنبه لاكتشاف هذه الجرائم بنسبة ٢٥% من هذه الحالات.

– وفي دراستين تمتا بالولايات المتحدة الأمريكية عامي ١٩٨١ – ١٩٨٤ شملت الأولى الاحتيال بواسطة الحاسب الآلي للاستيلاء على المال على ٧٧ عينة، والثانية شملت ٦٧ عينة من ذات نوع الجريمة، وتبين في الحالتين أن نسبة ٥٢% في الأولى، و٤٢% في الثانية من مجموع كل حالة قد اكتشفت عن طريق الرقابة الداخلية (Internal control)، وأن ١٢% من المجموعة الأولى، و٦% من المجموعة الثانية قد كشفت عن طريق التدقيق (Internal audit).

– كذلك في دراسة نشرت في انكلترا عام ١٩٨٦، وشملت ١٩٥ حالة احتيال لاختلاس المال، وتمت عن طريق الحاسب الآلي، تبين أن ١٥% قد اكتشفت نتيجة يقظة وفطنة المراجعين الداخلين والخارجين حال قيامهم بالعمل الروتيني للفحص والتدقيق، و١٦% اكتشفت بفضل مهارة الإدارة ودقتها في عملها وقدرتها على استعمال أساليب الرقابة على تطبيقات الحاسب الآلي، كما كشفت ١٠% منها بناء على شكوى المجني عليه، و٧% على أثر تغييرات في القيادات الإدارية، و١٥% منها مصادفة، و١٥% نتيجة معلومات سرية قدمت للشرطة أو لرب العمل الذي يعمل الجاني لديه، و٣% كانت نتيجة شكوك من جهة الإدارة أو زملاء العمل أو لقيام الجاني بإنفاق المال ببذخ. راجع في ذلك:

Dr. Kan Wong, Computer Fraud in The U.K The picture, Computer fraud of security, Bulletin, Vol, 9, nal, 1986, p. 9.

ود. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٠٨.

**جـ-الجريمة الإلكترونية جريمة عابرة للحدود:**

يطلق تعبير "جرائم عابرة للدول" أو جرائم غير وطنية على تلك الجرائم التي تقع بين أكثر من دولة، بمعنى أنها لا تعترف بالحدود الجغرافية للدول كجرائم تبيض الأموال، والمخدرات وغيرها، وفي عصر الحاسوب، ومع انتشار شبكة الاتصالات العالمية (الانترنت)، أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة بحيث يغدو أمر التنقل والاتصال فيما بينها أمراً سهلاً، طالما حدد عنوان المرسل إليه، أو أمكن معرفة كلمة السر، وسواء تم ذلك بطرق مشروعة، أو غير مشروعة. وفي هذه البيئة يمكن أن توصف الجريمة الإلكترونية بأنها جرائم عابرة للدول، إذ غالباً ما يكون الجاني في بلد، والمجني عليه في بلد آخر، كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه(١).

فقد تقع الجريمة الإلكترونية في كثير من الأحيان في عدة بلدان مختلفة، فيتم الدخول إلى الأجهزة الإلكترونية من بلد معين، ويتلاعب بالبيانات في بلد أخر، وتسجل البيانات في بلد ثالث، ومن الممكن أن تخزن الأدلة الإلكترونية في أجهزة موجودة في غير البلد الذي ارتكب منها الجاني جريمته، فتقع الجريمة بذلك في عدة دول كل دولة لها القانون المختلف عن الأخرى، وهذا يشكل تعقيداً أمام الجهات القضائية في تطبيق القانون ويشكل عائقاً في عملية التحقيق والإثبات لهذه الجرائم(٢).

فالمجتمع المعلوماتي لا يعترف بالحدود الجغرافية فالشبكات تخترق الزمان والمكان، خاصة بعد ظهور شبكات المعلومات الدولية أي الإنترنت، حيث إن القائم على النظام المعلوماتي في أي دولة يمكنه أن يحول مبلغاً من المال لأي مكان في العالم مضيفاً له صفر أو بعض الأصفار لحسابه الخاص، بل يستطيع

---

(١) ثنيان ناصر آل ثنيان، المرجع السابق، ص٢٣.

(٢) أمجد خليل حمودة، الوسائل الحديثة لإثبات الجرائم التي ترتكب بواسطة الأجهزة الإلكترونية، مجلة جامعة الأزهر، عدد خاص بمؤتمر كلية الحقوق الخامس المحكّم، المجلد التاسع عشر، غزة، فلسطين، ص١٢١.

أي شخص أن يعرف كلمة السر لأي شبكة في العالم ويتصل بها ويغير ما بها من معلومات[١].

ويترتب على هذه الخاصية أن تزيد الصعوبة في إثبات الجريمة الإلكترونية متى ارتكبت خارج النطاق المكاني للإقليم، لأنه يصعب في هذه الحالة جمع الدليل الجزائي فيها[٢].

وإذا تقرر أن الجرائم الإلكترونية جرائم عابرة للدول تظهر الحاجة الملحة للتعاون الدولي في مجال مكافحة هذه الجرائم وضبط فاعليها[٣].

ولصعوبة استخلاص الدليل الإلكتروني في الجريمة الإلكترونية يرى المختصون في جرائم الحاسوب، أن هذا الجهاز وما يقع عليه من جرائم إلكترونية، يعد تحدياً هائلاً لرجال الأمن ذلك أن رجل الأمن غير المتخصص والذي انحصرت معلوماته في جرائم قانون العقوبات بصورته التقليدية من قتل وضرب وسرقة لن يكون قادراً على التعامل مع الجريمة الإلكترونية والتي تقع بطريقة تقنية عالية[٤].

**د- ضخامة كم البيانات المعلوماتية في الجريمة الإلكترونية:**

لعل من الصعوبات الكبيرة التي تواجه رجال الضبط وسلطات التحقيق الجنائي في الجريمة الإلكترونية، هو كمية المعلومات والبيانات الضخمة والتي هي في حاجة إلى فحص ودراسة كي يستخلص منها دليل هذه الجريمة، لذلك يمكن القول إن ضخامة هذه البيانات والمعلومات، تعد عائقاً في التحقيق في الجرائم الإلكترونية، ذلك أن طباعة كل ما هو موجود على الدعامات الممغنطة لحاسوب

---

(١) هلال آمنة، المرجع السابق، ص٢٥ – ٢٦.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، د.ط، دار الكتب القانونية، المحلة الكبرى، مصر، ٢٠٠٧م. ص٣١.

(٣) ثنيان ناصر آل ثنيان، المرجع السابق، ص٢٣.

(٤) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٠٧.

متوسط العمر، يتطلب مئات الآلاف من الصفحات[١]، فحجم البيانات الضخمة التي غالباً ما تستخدم في التحقيق من خلال أنظمة الكمبيوتر تشكل تحدياً، وهذا راجع إلى أن البحث عن الأدلة اللازمة للإدانة أو البراءة في قدر كبير من البيانات الإلكترونية، صعب جداً ويتطلب جهداً ومهارة عاليين[٢].

في الوقت الذي قد لا تقدم فيه هذه الصفحات شيئاً مفيداً للتحقيق، وهذا عكس ضخامة أو وفرة المعلومات في الجرائم التقليدية كالقتل أو السرقة، ذلك أن وفرة المعلومات في مثل هذه الجرائم هو أمر يساعد العدالة ويساعد رجل الضبط أو المحقق – على السواء – في استخلاص الدليل الجزائي في هذه الجريمة[٣].

## ثانياً: صعوبات متعلقة بالجاني والمجني عليه في الجريمة الإلكترونية:

هنالك صعوبات كثيرة ترجع إلى المجرم الإلكتروني تحول دون الحصول على الدليل الإلكتروني نظراً لإخفائه هويته ومحاولة تدميره لهذا الدليل، كما قد يسهم المجني عليه في الجريمة الإلكترونية في الحيلولة دون الحصول على هذا الدليل في حال إحجامه عن التبليغ عن الجريمة الإلكترونية التي وقعت عليه، وبناء على ما تقدم سندرس إخفاء المجرمين لهويتهم، ومن ثم تقاعس المجني عليه الإبلاغ عن الجرائم الإلكترونية، كما يلي:

---

١ د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٩٦.

(٢) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١١٩ – ١٢١.

٣ د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٩٦.

**أ-إخفاء المجرمين لهويتهم:**

من الصعوبات الإضافية التي يمكن أن تعترض العملية الإثباتية في مجال الجرائم الإلكترونية سهولة محو الجاني أو تدميره لأدلة الإدانة في زمن متناه القصر، فضلاً عن سهولة تنصله من مسؤولية هذا العمل بإرجاعه، حسبما تشهد بذلك وقائع عديدة سابقة، على خطأ في نظام الحاسوب أو الشبكة أو في الأجهزة(١).

فالإغراءات التي تجذب المجرمين نحو الجرائم الإلكترونية هي أنها في الحقيقة جرائم سريعة التنفيذ، إذ غالباً ما يتمثل الركن المادي فيها باستعمال جهاز الحاسوب، مع إمكانية تنفيذ ذلك عن بُعد، دون اشتراط الوجود في مسرح الجريمة، وأيضاً ضخامة الفوائد والمكاسب التي يستطيع الجاني تحقيقها في مثل هذه الجرائم، دون جهد يذكر، ودون أن يخاف أن يكتشف أمره. كما أن الجرائم الإلكترونية يمكن اعتبارها بمثابة إغراء كبير للمجرمين، لاستغلال التكنولوجيا الحديثة، بغية اقتراف الجرائم بصورها المتعددة، خصوصاً عندما يكون الجاني موظفاً في شركة تعتمد الحاسوب في عملها، إذ يكون لديه كافة المعلومات اللازمة لتحقيق اختراقات متعددة ومتتالية لأنظمة الحاسوب في الشركة، وتحقيق أرباح طائلة والواقع يثبت ذلك(٢).

وتبدأ هذه المشكلة عند تعمد المستخدم إخفاء هويته، ويخلق هذا الأمر المزيد من التحديات الأمنية، لأنه حتى عندما لا يبذل المجرمون جهداً في إخفاء هويتهم فإنهم يستطيعون الادعاء بأنهم لم يكونوا مسؤولين عن ذلك. فقد يتخذ المجرمون بعض الإجراءات لإحباط اعتقالهم، وهذا في حال بذلهم لجهد ضئيل

---

(١) د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، بحوث مؤتمر القانون والكومبيوتر والإنترنت، من ١ – ٣ مايو، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثاني، الطبعة الثالثة، ٢٠٠٤م، ص٤٢٩.

(٢) ثنيان ناصر آل ثنيان، المرجع السابق، ص٢٢ – ٢٣.

لطمس هويتهم على الإنترنت، لكي تظل أنشطتهم مجهولة، ومن هذه الإجراءات مثلاً ما يكون بسيطاً مثل استخدام كومبيوتر بمكتبة عامة، إلا أن هناك العديد من البرامج والتطبيقات التي تقدم وسائل متباينة لكيفية طمس الهوية على الإنترنت، مما يؤدي لتفاقم المشكلة بالنسبة للمحقق الجنائي أو خبير الأدلة الإلكترونية، فهذا الإخفاء يجعل الأمر صعباً على الفاحصين القائمين على تحليل الأدلة التي تم العثور عليها، وتجميعها وإدراجها بمستندات والاحتفاظ بها(١).

كما أن مرتكبي هذه الجرائم لا يتركون في غالب الأحيان آثاراً تدل على ارتكابهم لهذه الجرائم؛ إذْ تكون المعلومات محفوظة تحت رقم أو رمز سري أو مشفرة كليّاً(٢)؛ فمن الممكن وضع شيفرة لحماية المعلومات والتقيد بتعليمات مبرمجة لمنع اختراق الحاسوب، وتُعد هذه من الوسائل الفنية لحماية سرية المعلومات في نظم الحاسبات الإلكترونية(٣)، والتشفير هو عملية تتمثل في تحويل المعلومات المقروءة إلى إشارات غير مفهومة، لحماية أمن المعلومات ضد أعمال القرصنة ونشر الفيروسات والاعتداء على المعلومات، وبيانات بطاقات الائتمان الممغنطة(٤). إذْ يصعب الولوج إليها أو معرفتها، وبالتالي إقامة الدليل ضد هؤلاء الجناة(٥). وبالنظر إلى ازدياد انتشار برمجيات التشفير هذه في الدول المتقدمة وما ينجم عنها من مخاطر ، فإن بعضها استحدث تشريعات تمّ بموجبها تجريم اللجوء إلى هذه التقنيات دون ترخيص من الأجهزة المختصة، ومن هذه الدول هولندا، حيث سنّت تشريعاً يقضي بوضع ضوابط لعمليات التشفير ، ومنها ضرورة الحصول على

---

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١٢١.

(٢) ورقة بعنوان: «دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول»، المرجع السابق،، ص٢٦.

(3) LAW AND COMPUTER TECHNOLOGY: vol 5, no 2, March 1972, p 45 - 46.

(٤) خالد عياد الحلبي، المرجع السابق، ص٥٠.

(٥) ورقة بعنوان: «دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول»، المرجع السابق، ص٢٧ – ٢٨.

ترخيص من الجهات المعنية، إلى جانب إيداع مفاتيح التشفير لدى هذه الجهات [١].

وكذلك فعلت فرنسا الشيء ذاته ، ومن شأن الإقدام على هذا التشفير بدون ترخيص أن يصبح الفعل جريمة يعاقب عليها القانون ، وأيضاً معاقبة الشخص الذي أعد برنامج التشفير بدون ترخيص[٢].

**ونحن نقترح بضرورة عُد الإقدام على التشفير بدون ترخيص جريمة يعاقب عليها القانون، وأيضاً نقترح معاقبة الشخص الذي أعد برنامج التشفير بدون ترخيص.**

كما لا بد من خلق وحدات خاصة تكون مهمتها الأساسية هي مراقبة وتتبع الشبكة عن طريق الإبحار فيها، ومثل هذه المراقبة السابقة قد تعطي نتائج هامة على مستوى الحد من الجريمة قبل ارتكابها عن طريق الوقاية منها[٣].

هذا بالإضافة إلى أن الكثير من جرائم تقنية المعلومات يثير شكلاً جديداً من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية، حيث يقع الفعل الإجرامي عادة من مسافات بعيدة، وذلك باستخدام وحدات طرفية أو اتصال هاتفي يمكن للجاني من خلالها إعطاء تعليمات للحاسب الآلي تمكنه من اختراق شبكات المعلومات في مناطق أخرى والنتيجة هي صعوبة الوصول إليه ومعرفته، فقد يكون الجاني في أحد العواصم الأسيوية أو الأوربية ويخترق شبكات المعلومات في

---

(١) د. موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مقدَّم إلى : المؤتمر المغاربي الأول حول :المعلوماتية والقانون الذي تنظمه أكاديمية الدراسات العليا . طرابلس خلال الفترة ٢٨ . ٢٩ / ١٠ / ٢٠٠٩م، ص٤.

(٢) عطية عثمان محمد بوحويش ، حجية الدليل الرقمي في إثبات جرائم المعلوماتية ، رسالة الماجستير، مقدمة إلى أكاديمية الدراسات العليا، بنغازي،٢٠٠٩ م، ص٧٠ .

(٣) ورقة بعنوان: «دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول»، المرجع السابق، ص٢٧ – ٢٨.

الولايات المتحدة أو العكس، كما أنه باستطاعته أن يطمس ويلغي كل ما يدل على جريمته من خطوات[١].

وكمثال عن محاولة مرتكبو الجرائم إخفاء جرائمهم أو على الأقل إزالة آثارها، نجد أن التجسس المعلوماتي بنسخ الملفات، من النادر اكتشافهما بمعرفة الشركات التي تقع ضحية لهما، فالتدليس عادة ما يتم خفية عن طريق التلاعب بالقوائم والمعطيات التي يحتويها الجهاز أو البرامج المعلوماتية ذاتها. فالتعديلات التي يقوم بها الجاني في الملفات المعلوماتية لا تترك آثاراً على خلاف تلك التي تترتب على تزوير المستندات الورقية[٢].

**ب-تقاعس المجني عليه بالإبلاغ عن الجرائم الإلكترونية:**

قد يتقاعس المجني عليه عن الإبلاغ عن جرائم الحاسوب إلى السلطات المختصة بالكشف عن هذه الجرائم وإثباتها[٣]، ويكون بالتالي للمجني عليه دور في في صعوبة الحصول على الدليل الإلكتروني، بسبب موقفه السلبي وعدم إبلاغه عن وقوع هذا النوع من الجرائم، فالكثير من الجهات التي تتعرض أنظمتها للانتهاك تعمد إلى عدم الكشف عنها تجنباً لعدم الإضرار بسمعتها وتكتفي بالإجراءات الإدارية[٤].

ففي إحدى الوقائع تعرض أحد البنوك، هو بنك (Marchant bank city) في بريطانيا لسرقة ٨ مليون جنية إسترليني من إحدى أرصدته إلى رقم في سويسرا، وتم ضبط الفاعل متلبساً بسحب المبلغ المسروق، وبدلاً من محاكمته قام البنك بدفع مليون

---

١ د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٤٧.

٢ د. جميل عبد الباقي الصغير، المرجع السابق، ص١١٤.

(٣) د. جميل عبد الباقي الصغير، المرجع السابق، ص١١٦.

(٤) عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، د.ط، دار الجامعة الجديدة، مصر، ٢٠١٠م، ص٤٧.

جنية له بشرط التزام الفاعل بعدم الإعلام عن جريمته، وإعلام البنك عن الآلية التي نجح من خلالها في اختراق نظام الأمن بحاسوب البنك الرئيسي[١].

كما كشفت إحصائيات شركات التأمين في فرنسا عن أن نسبة الإبلاغ عن جرائم الحاسوب تتراوح بين ٥ إلى ١٠ % من مجموع الجرائم التي ارتكبت في هذا المجال، ويرجع السبب في ذلك إلى الرغبة في إخفاء ارتكاب الجريمة حتى لا يتم تقليده من جانب الآخرين من ناحية، ولأن في الإبلاغ إهدار لثقة المتعاملين مع البنوك والمؤسسات المالية من ناحية ثانية، كما أن الإبلاغ قد يسمح لسلطات البوليس بالاطلاع على معلومات اسمية لم يقم المجني عليه بالأخطار عنها فبل جمعها من ناحية ثالثة[٢].

ومن أجل تفعيل عملية الإبلاغ عن الجريمة الإلكترونية، ومن ثم المساهمة بطريقة إيجابية في منع وقوع الجريمة أو سرعة تحصيل الدليل المتعلق بها، أوصى المؤتمر الدولي الخامس عشر للجمعية العامة، والذي عقد في "ريو دي جانيرو" بالبرازيل في الفترة من ٤ – ٩ /١١/ ١٩٩٤، بضرورة تشجيع المجني عليهم في هذه الجرائم على الإبلاغ عنها فور وقوعها، وهذا بهدف تخفيض الرقم الأسود للجرائم الإلكترونية في الفضاء الافتراضي[٣].

كما طالب البعض في الولايات المتحدة الأمريكية بأن تتضمن القوانين المتعلقة بجرائم الحاسوب والمعلومات، نصوصاً تلزم موظفي الجهة المجني عليها – أياً كانت – بضرورة الإبلاغ عما يصل إلى علمهم من جرائم تتعلق بهذا المجال، وتقرير جزاءات على الإخلال بذلك الالتزام إلا أنه ولدى عرض هذا الاقتراح على "لجنة خبراء مجلس أوربا" قوبل بالرفض لسبب قانوني مؤداه أن

---

(١) عبد الناصر محمد محمود فرغلي، د. محمد عبيد سيف سعيد المسماري، المرجع السابق، ص١٠-١١.

(٢) د. جميل عبد الباقي الصغير، المرجع السابق، ص١١٦.

(٣) عائشة بن قارة مصطفى، المرجع السابق، ص٤٨.

المجني عليه – وهو الشركة التي ارتكبت في حقها جريمة إلكترونية – سوف تصبح متهمة أو جانية بعد أن كانت مجنياً عليها ولذلك وردت اقتراحات بديلة قد تكون مقبولة منها الالتزام بإبلاغ جهة خاصة، أو إبلاغ سلطات إشرافية، وتشكيل أجهزة خاصة لتبادل المعلومات، وكذلك إصدار شهادة "أمن خاصة" تمنح بعد عمل مراجعة وتدقيق من قبل هيئة خاصة من المراجعين، ويتعين على هذه الهيئة إبلاغ الشرطة بما تكشفه من جرائم(١).

**ونحن نقترح أجل تفعيل عملية الإبلاغ عن الجريمة الإلكترونية، ومن ثم المساهمة بطريقة إيجابية في منع وقوع الجريمة أو سرعة تحصيل الدليل المتعلق بها، بضرورة تشجيع المجني عليهم في هذه الجرائم على الإبلاغ عنها فور وقوعها، وذلك بإبلاغ جهة خاصة، أو إبلاغ سلطات إشرافية، وتشكيل أجهزة خاصة لتبادل المعلومات، وكذلك إصدار شهادة "أمن خاصة" تمنح بعد عمل مراجعة وتدقيق من قبل هيئة خاصة من المراجعين، ويتعين على هذه الهيئة إبلاغ الشرطة بما تكشفه من جرائم.**

## ثالثاً: صعوبات متعلقة بضعف التعاون الدولي في مكافحة الجريمة الإلكترونية:

تتعقد المشكلة عندما يتعلق الأمر بمعلومات أو بيانات تم تخزينها في الخارج بواسطة شبكة الاتصال عن بُعد، والقواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه المعلومات بحثاً عن الأدلة وتحقيقها، فمن الصعب إجراء التفتيش

---

(1) Hans G. Nilsson, Computer crimes and other crimes aginst information Technology whin the working programme of the council of Europe, R.I.D.P. 1993, p. 124.

نقلاً عن: أ. د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، المرجع السابق، ص٤٣٧.

للحصول على الأدلة في هذه الحالة في داخل دولة أجنبية، حيث إن هذا الإجراء يتعارض مع سيادة هذه الدولة الأخيرة[١].

لذلك نادى البعض بضرورة إنشاء وحدات خاصة بمكافحة الجريمة الإلكترونية بواسطة الحاسوب والإنترنت أسوة بجهات البحث الجنائي الوطنية والدولية – الإنتربول – لإثبات الجريمة عند وقوعها وتحديد أدلتها وفاعليها، وهو ما يعني كذلك إيجاد صيغة ملائمة للتعاون الدولي لمكافحة جرائم الاعتداء على المعلومات الخاصة في الإنترنت، وتبادل الخبرات والمعلومات حول هذا النوع من الجرائم ومرتكبيها وسبل مكافحتها[٢].

ورغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة الإلكترونية، إلا أن هناك عوائق تحول دون ذلك، وتجعله صعب المنال، وأهم هذه العوائق:

**أ–عدم الاتفاق على صور محددة للنشاط الإجرامي:**

حيث إن الأنظمة القانونية في بلدان العالم قاطبة لم تتفق على صور محددة يندرج في أطارها ما يسمى "بإساءة استخدام نظم المعلومات الواجب إتباعها"، كذلك ليس هناك تعريف محدد للنشاط المفروض أن يُتفق على تجريمه، وذلك نتاج طبيعي للتشريع ذاته في كافة بلدان العالم وعدم مسايرته لسرعة التقدم المعلوماتي، ومن ثم الجريمة الإلكترونية[٣].

ولعل عدم الاتفاق بين الأنظمة القانونية المختلفة على صورة موحدة للسلوك الإجرامي في الجريمة الإلكترونية يغري قراصنة الحاسوب على تنظيم أنفسهم وارتكاب جرائمهم دون تقيد بالحدود الجغرافية[٤].

---

(١) د. جميل عبد الباقي الصغير، المرجع السابق، ص١١٥.

٢ د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٨٧.

(٣) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٨٨.

(٤) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٨٩.

**ب-عدم وجود تنسيق بين الدول فيما يتعلق بالأصول الجزائية المتبعة في شأن الجريمة الإلكترونية بين الدول المختلفة:**

إن عدم التنسيق وبشكل خاص فيما يتعلق منها بإعمال الاستدلال أو التحقيق، سيما وأن عملية الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة، عن طريق الضبط أو التفتيش في نظام معلوماتي معين هو أمر غاية في الصعوبة، فضلاً عن الصعوبة الفنية في الحصول على الدليل ذاته[١].

فمثلاً في غالب الأحيان، يتعذر الحصول على الأدلة من أجهزة الكومبيوتر الموجودة في دولة أخرى حتى في حال وجود إجراءات دولية تسهل تبادل الأدلة الإلكترونية، فإن معظم هذه الإجراءات معقدة، وهي ليست عملية إلا بالنسبة للجرائم الخطيرة[٢].

**جـ- عدم وجود معاهدات ثنائية أو جماعية بين الدول للتعاون في مجال هذه الجرائم:**

إن عدم وجود معاهدات ثنائية أو جماعية بين الدول على نحو يسمح بالتعاون المثمر في مجال هذه الجرائم، وحتى في حال وجودها فإن هذه المعاهدات قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسوب وشبكة الإنترنت، ومن ثم تطور الجريمة الإلكترونية بذات السرعة على نحو يؤدي إلى إرباك المشرع وسلطات الأمن في الدول، ومن ثم يظهر الأثر السلبي في التعاون الدولي[٣].

---

(١) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٩٠.

(٢) د. ممدوح عبد الحميد عبد المطلب،المرجع السابق، ص١٢١.

(٣) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٩٠.

ولحل ذلك لابد من صدور قانون دولي في صورة اتفاقية دولية، ويمثل الحد الأدنى لمتطلبات كل دولة حتى يتم مواجهة ظاهرة الجريمة في فضاء الإنترنت، هذا من ناحية، ومن ناحية أخرى من الممكن تعزيز العلاقات الدولية الثنائية بين كل دولتين باتفاقية ثنائية أو ثلاثية في مجال التعاون الدولي في هذه الجريمة، ويكون هدف هذه الاتفاقيات:

١- التعرف على مكان الجناة وتحديده.

٢- تقديم الوثائق المثبتة للجريمة وتبادلها.

٣- الحصول على الأدلة والقرائن والأنظمة التي يجب مراعاتها.

٤- تنفيذ طلبات البحث والتحري والضبط.

٥- المساعدة فيما يتعلق بإجراءات التحقيق الجنائي(١).

**د-مشكلة الاختصاص في الجرائم الإلكترونية:**

تُعد مشكلة الاختصاص في الجرائم الإلكترونية من المشكلات التي تعرقل الحصول على الدليل في الجريمة الإلكترونية، ذلك أن هذه الجرائم من أكثر الجرائم التي تثير مسالة الاختصاص على المستوى المحلي والدولي بسبب التداخل والترابط بين شبكات المعلومات، فقد تقع جريمة الحاسوب في مكان معين، وتنتج آثارها في مقاطعة أخرى داخل الدولة أو خارجها، ومن هنا تنشأ مشكلة البحث عن الأدلة الجنائية على شبكة الإنترنت(٢).

**ونحن نرى أنه لحل مشكلة الاختصاص في داخل إقليم الدولة فأنها تحل على أساس مكان القبض على المتهم أو محل إقامته أو مكان وقوع الجريمة، فأي مكان من الأماكن المذكورة، ينعقد الاختصاص القضائي لسلطات التحقيق**

---

(١) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٢٤٩ - ٢٥٠.

(٢) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٩١.

**والمحاكمة فيه بالجريمة الإلكترونية، وذلك بتطبيق نص المادة (٣) الفقرة (١) من قانون أصول المحاكمات الجزائية السوري لعام ١٩٥٠م الذي جاء فيه: " تقام دعوى الحق العام على المدعى عليه امام المرجع القضائي المختص التابع له مكان وقوع الجريمة او موطن المدعى عليه او مكان القاء القبض عليه".**

**ولكن على المستوى الدولي فإن الأمر في حاجة لعقد اتفاقيات دولية ثنائية أو جماعية وتفعيل الإنابات القضائية.**

**كما نرى أنه لحل مشكلة ضعف التعاون الدولي في مجال الجريمة الإلكترونية ولا سيما في مجال تبادل الأدلة الإلكترونية، فإن الحاجة ماسة إلى إصدار تشريعات جزائية أكثر مرونة تسمح بسرعة التعاون المثمر في تبادل الأدلة الإلكترونية.**

## الفرع الثاني

## صعوبات متعلقة بالدليل الإلكتروني

هنالك صعوبات كثيرة متعلقة بالدليل الإلكتروني، وهي أولاً، عدم مرئية الدليل الإلكتروني، وثانياً، الحجم الكبير للبيانات التي يوجد فيها الدليل الإلكتروني، وثالثاً، سهولة أخفاء الدليل الإلكتروني، ورابعاً، الدليل الإلكتروني دليل ظرفي، وخامساً سهولة التلاعب بالدليل الإلكتروني:

### أولاً: عدم مرئية الدليل الإلكتروني:

الأدلة الإلكترونية تتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة، لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبات الألية (Hard ware)، واستخدام نظم برامجية حاسوبية (Soft ware) [١].

---

(١) عبد الناصر محمد محمود فرغلي، د. محمد عبيد سيف سعيد المسماري، المرجع السابق، ص١٤.

فليس للدليل الإلكتروني طبيعة مادية ملموسة كما هو الحال في الأدلة التقليدية، فالأجهزة التقنية لا تفرز سكيناً عليها بصمات القاتل، أو مالاً يمكن ضبطه مع السارق في جريمة السرقة وغير ذلك، فكل ما تنتجه التقنية هو عبارة عن نبضات إلكترونية يمكن أن تدل في مجموعها على أنماط السلوك الإنساني(١).

أضف إلى ذلك أن ترجمة الدليل الإلكتروني وإخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعد الدليل، بل إن هذه العملية تعد عملية نقل لتلك البيانات من مجالها إلى شكل ملموس يمكن الاستدلال بها على معلومات معينة(٢).

والواقع أن هذه الطبيعة غير المرئية للدليل الإلكتروني تلقي بظلالها على أجهزة العدالة الجزائية التي تتعامل مع هذه الجرائم المستحدثة، لأن غياب الدليل المرئي يشكّل عقبة كبيرة أمام كشفها(٣).

**ثانياً: الحجم الكبير للبيانات التي يوجد فيها الدليل الإلكتروني:**

يحتوي القرص الصلب مثلاً على حجم كبير من البيانات والمعلومات غير المرتبة، ولكن ما يتعلق بالجريمة قد يشكل جزأً صغيراً فقط من هذه المعلومات. ويمكن تشبيه حجم المعلومات هذا بموجات الراديو الموجودة في الهواء والتي تحتوي على بيانات متشابكة، الأمر الذي يجعل من الصعوبة بمكان معرفة الإشارة المطلوبة وترجمتها إلى بيانات مفهومة. فالوصول إلى الدليل الإلكتروني المطلوب يشكّل تحدياً أمام الخبير المعلوماتي(٤).

---

(١) د. محمد طارق الخن، المرجع السابق، ص١١٣.

(٢) سهى إبراهيم داود عريقات، المرجع السابق، ص١٨.

(٣) د. محمد طارق الخن، المرجع السابق، ص١١٣.

(٤) د. محمد طارق الخن، المرجع السابق، ص١١٣.

**ثالثاً: سهولة إخفاء الدليل الإلكتروني:**

حيث تضع عملية إخفاء المعلومات تحديات مماثلة لخبراء الأدلة الإلكترونية، وهم الخبراء التقنيون، مما يجعل الأمر صعباً أو مستحيلاً للعثور على البيانات الإلكترونية. فهذه العملية من شأنها خلق عدة مشاكل تتعلق بالدليل الإلكتروني ومن شأنها التأثير على سير التحقيق في سبيل الحصول على هذا الدليل.

فإخفاء المعلومات الضرورية يعني إخفاء أدلة جوهرية في القضية المراد إثباتها، وهناك عدة حالات لإخفاء المعلومات، حيث يمكن أن يجمع بين إخفاء الهوية وإخفاء المعلومات، أو البيانات المخفية لخلق نظام ملفات آمن تجعل عملية استعادة الأدلة وإعادة تركيبها أمراً في غاية الصعوبة، وفي غاية التعقيد بسبب هذا الأمر [١].

ونظراً لأن الحاسوب هو منهج متحرك تتشابك بموجبه كافة المعلومات وكافة طرق المعالجة الواحدة مع الأخرى، فإنه من السهل أن يوضع فيه برنامج تكون مهمته تعديل الإجراءات الضرورية لعمل هذا الذكاء الصناعي، والذي يهدف في النهاية إلى محو كل الدعامات التي توجد في الجهاز. يضاف إلى ذلك أن التخزين الإلكتروني للمعطيات يجعلها غير مرئية وغير مفهومه بالعين المجردة، كما أنه من السهل محو الدليل في زمن قصير الذي يعد من أهم الصعوبات التي تعترض العملية الإثباتية في مجال جرائم الحاسوب[٢].

كما أنه من المتعارف عليه أن إغلاق جهاز الكومبيوتر، يعني أن هنالك عدد ضئيل من الأدلة لا يمكن استرجاعها، وهذا في حالة عدم تخزينها بالذاكرة، ومنها المساس بسلامة الأدلة الموجودة، ولهذا لا يجب غلق الكومبيوتر فوراً حتى لا يتم مسح الأدلة. إلا أن انقطاع التيار الكهربائي المفاجئ عن جهاز الكومبيوتر يسبب الكثير من المشاكل، تتمثل في محو المعلومات من الذاكرة، بمعنى فقدان

---

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١٢٢ – ١٢٣.

(٢) د. جميل عبد الباقي الصغير، المرجع السابق، ص١١٤ – ١١٥.

كافة العمليات التي كان يتم تشغيلها، وأنظمة الملفات الثابتة، فغلق أي نظام قبل الحصول على البيانات بالذاكرة الفعلية يمكن أن يؤدي إلى فقد الأدلة الجوهرية، كما أن هذا الغلق المفاجئ من شأنه تحريف بيانات هامة(١).

**وهكذا نجد أن انعدام الدليل المرئي والواضح عقبة كبيرة أمام كشف الجرائم**، إلا أن هناك من يرى أنه توجد بعض البرامج والأنظمة التي يمكنها مواجهة هذه المشكلة، التي تشكل عائقاً أمام الحصول على الدليل الإلكتروني(٢).

**رابعاً: الدليل الإلكتروني دليل ظرفي:**

الدليل الإلكتروني هو عادة دليل ظرفي، فمعرفة عنوان الإنترنت IP مثلاً يشير إلى الحاسوب الذي ارتكبت الجريمة بواسطته فقط، دون أن يحدّد مرتكب الجريمة بالذات، الأمر الذي يجعل من الصعوبة بمكان، نسبة النشاط الجرمي إلى شخص ما، ما لم يتم القيام بالعديد من التحقيقات للتأكد من ذلك.

ففي إحدى القضايا التي عرضت على المحاكم الأمريكية، نازع المدعى عليه في جميع الأدلة التي وجدت على حاسوبه، لأن المحققين لم يستطيعوا إثبات أنه هو الشخص الذي قام بالنشاطات غير الشرعية على الإنترنت(٣).

***خامساً:* سهولة التلاعب بالدليل الإلكتروني:**

إن خاصية صعوبة التخلص من الدليل الإلكتروني قد تقابلها مسألة أخرى ذات علاقة بمسألة التطوير المستمر في تكنولوجيا المعلومات، وهي أن هذا الدليل نتيجة لمرونته وضعفه، فإنه يسهل إتلافه أو فقدانه أو كما يطلق عليه "***Spoliation of Evidence***"، بمعنى إمكانية التخلص منه بغير الحذف والإلغاء(٤).

---

(١) هلال آمنة، المرجع السابق، ص٧٠.

(٢) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١٢٢ – ١٢٣.

(٣) د. محمد طارق الخن، المرجع السابق، ص١١٤.

(٤) د. عمر محمد بن يونس، الدليل الرقمي، المرجع السابق، ص١١.

فعلى الرغم من تميز الدليل الإلكتروني بصعوبة التخلص منه إلا أن هنالك سهولة بالتلاعب به سواء أكان تعديلاً أو إتلافاً أو إدراجاً في المستندات أو البيانات الرقمية الأخرى(١).

كما يخشى كثيراً من الاستبداد واصطناع الأدلة حيث لا توجد وسيلة فعالة للآن للتأكد من البيانات الموجودة على الأجهزة هي تلك التي تم ضبطها حيث يمكن بالوسائل العلمية والتقنيات الحديثة تغيير وتعديل وتبديل ومحو البيانات الموجودة على أجهزة الكومبيوتر(٢).

وفي الحقيقة فإن مسألة إتلاف الدليل الإلكتروني على الرغم من ثبوتها في القانون المقارن كنوع من القياس على إتلاف الدليل المادي، هي في الواقع ليست مسألة حقيقية، وإنما الحقيقة أن مسألة إمكانية إتلاف الدليل الإلكتروني تعني أن هناك قصور في القدرات التكنولوجية لدى مؤسسات العدالة الجزائية، مما ينبغي معه وجوب العمل على التطوير المستمر لنظم العدالة الجزائية، بالإضافة لتطوير قدرات القائمين على مهامها وأعمالها(٣).

**نستنتج مما سبق أن هنالك عدة مشاكل أقل ما يقال عنها أنها صعبة، تعرقل عملية جمع واستخراج الدليل الإلكتروني، وهذا يرجع للطبيعة الخاصة للجريمة الإلكترونية، بالإضافة لطبيعة الدليل الإلكتروني في حد ذاته، وكذلك شدة الذكاء التي يتميز به المجرمون الذين يقترفون هذا النوع من الجرائم، فمنها مشاكل تتعلق بالحاسوب وطبيعته الخاصة والمعقدة التي تحتاج لخبرة فنية وتقنية عالية من الأشخاص الذين يتولون مهمة جمع الدليل الإلكتروني، ومشكلات تتعلق بالأشخاص المرتكبين لهذه الجرائم وقدرتهم الفائقة في إخفاء هويتهم من جهة، وإخفاء المعلومات من جهة أخرى.**

---

(١) سهى إبراهيم داود عريقات، المرجع السابق، ص١٨.

(٢) د. مدحت رمضان، المرجع السابق، ص٧٢.

(٣) د. عمر محمد بن يونس، الدليل الرقمي، المرجع السابق، ص١١.

لهذا لابد من توافر تقنيون ذو كفاءة عالية لمواجهة هذه الجرائم المستحدثة، وهؤلاء المجرمين الأذكياء، حتى تسهل عملية جمع الأدلة الإلكترونية[١].

## الفرع الثالث
## صعوبات متعلقة بأسباب متعددة

هنالك صعوبات أخرى تواجه الحصول على الدليل الإلكتروني، وترد إلى جملة من الأسباب، وهي أولاً، نقص خبرة أجهزة العدالة الجزائية، وثانياً، صعوبات فنية.

### أولاً: نقص خبرة أجهزة العدالة الجزائية:

من الصعوبات التي تواجه عملية استخلاص الدليل الإلكتروني نقص الخبرة لدى رجال الضابطة العدلية أو أجهزة الأمن بصفة عامة، وكذلك لدى أجهزة العدالة الجزائية ممثلة في سلطة الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسوب والإلمام بعناصر الجرائم الإلكترونية وكيفية التعامل معها، وذلك على الأقل في البلدان العربية، نظراً لأن تجربة الاعتماد على الحاسوب وتقنياته وانتشارها في هذه البلدان جاء متأخراً عن أوربا وكندا والولايات المتحدة الأمريكية[٢].

وبالتالي فإنَّ نقص خبرة سلطات جمع الاستدلالات والتحقيق والمحاكمة قد يؤدِّي إلى ضياع الدليل بل تدميره أحياناً[٣] ذلك أن كشف جرائم الحاسوب وتحديد فاعلها ومحاكمتهم يستلزم توافر مهارات خاصة للقائمين على التحقيق والمحاكمة تسمح لهم بتفهم نظام تشغيل الحاسبات الآلية وأساليب التلاعب التي تستخدم في

---

(١) هلال آمنة، المرجع السابق، ص٧١ – ٧٢.

(٢) وهنا يبرز الفارق بين الدول العربية ودول أوربا والولايات المتحدة الأمريكية التي اعتمدت على الحاسب الآلي منذ أكثر من عقدين وبالتالي فقد طورت تشريعاتها لتواجه الجريمة الإلكترونية.

(٣) د. علي حسن الطوالبه، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، المرجع السابق.

ارتكاب الجريمة بواسطة هذا الأخير، فنقص الخبرة في هذا المجال يحول دون كشف الجريمة وضبط مرتكبيها[١]. بل أن المحقق قد يدمر الدليل عن خطأ منه أو إهمال أو بالتعامل بخشونة مع مختلف الوسائط التي تتضمن الدليل الإلكتروني كالأقراص المرنة أو غيرها[٢].

ومن أجل حل هذه الصعوبة فإنَّ إعداد رجال الضابطة العدلية وقضاة التحقيق والحكم، للبحث عن أدلة الإثبات في ميدان الجرائم الإلكترونية، يكتسب أهمية بالغة؛ إذ لا بد لهم من الدراية الكافية لطبيعة هذا النوع من الجرائم، الذي يتسم الكشف عنه وإثباته بصعوبات بالغة، وفي عالم «المعلوماتية وشبكات الكمبيوتر» القائم على تقنية الاتصالات والتوصيلات والوسائط الإلكترونية، لا تستطيع سلطة البحث والتحري والتحقيق تطبيق الإجراءات التقليدية على غالبية جرائم تقنية المعلومات. من أجل ذلك لا بد من تدريب وتكوين رجال الضابطة العدلية والتحقيق والقضاة المختصين بجرائم تقنية المعلومات فيما يتعلق بالأساليب الفنية المستخدمة في ارتكاب الجريمة وفيما يتعلق بالكشف عنها، والقرائن والدلائل والأدلة المستحدثة في مجال إثباتها، وكيفية معاينتها والتحفظ عليها وفحصها فنيا، مع ضرورة تدريب القضاة على معالجة هذا النوع من القضايا لتمكينهم من الفصل فيها. لذا لا بد من خلق وحدات خاصة تكون مهمتها الأساسية هي مراقبة وتتبع الشبكة عن طريق الإبحار فيها، ومثل هذه المراقبة السابقة قد تعطي نتائج هامة على مستوى الحد من الجريمة قبل ارتكابها عن طريق الوقاية منها[٣].

كما ينبغي الأخذ بالأساليب المستحدثة في التدريب مثل التدريب عن بُعد، والمؤتمرات المباشرة باستخدام الواقع الافتراضي، وأخيراً فإنه من الضروري أن يكون التدريب ذو بُعد دولي، والسبب في ذلك يعود للطبيعة الخاصة للجريمة

---

(١) د. جميل عبد الباقي الصغير، المرجع السابق، ص١١٥.

(٢) عائشة بن قارة مصطفى، المرجع السابق، ص٤٩.

(٣) ورقة بعنوان: «دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول»، المرجع السابق، ص٢٦ – ٢٧ – ٢٨.

الإلكترونية وخصوصاً في جرائم الشبكة العالمية أو جرائم الإنترنيت، لذلك فإن تبادل الخبرات بين العاملين في هذا المجال أمر ضروري لفاعلية التدريب[١].

**ثانياً: صعوبات فنية:**

هنالك بعض الصعوبات الفنية التي قد تمثل عائقاً أمام الجهة المختصة بجمع الأدلة، ويمكن إجمال هذه الصعوبات فيما يلي:

**أ- وجود جهاز مزود بنظام حماية:**

يتم البحث عن الدليل الإلكتروني في وسط افتراضي يحتويه الجهاز الذي ارتكبت به أو ضده الجريمة محل البحث، وغالباً ما يكون هذا الجهاز مزوداً بنظام حماية، بحيث لا يمكن تشغيله إلا باستعمال كلمة مرور معلومة لدى مستعمل ذلك الجهاز، وهو ما قد يحول دون الحصول على المعلومات من خلاله، غير أن التقنية الحديثة قد ساهمت في تفادي هذه المشكلة، إذ بالإمكان الاستعانة بما يسمى قرص التشغيل والذي يُمكن من تشغيل الجهاز حتى لو كان مزوداً بنظام حماية[٢].

**ب-انقطاع التيار الكهربائي:**

يتم عادة جمع الدليل الإلكتروني من جداول الحالة التشغيلية للبروتوكولات والاتصالات، والمشكلة أن هذه الجداول تظل متاحة لفترة محدودة، إذ تمحى بمجرد فصل التيار الكهربائي عن الجهاز، وهذا من شأنه الحؤول دون الحصول عليها، إلا أنه يمكن التغلب على هذه المشكلة من خلال إتباع أسلوب القص واللصق ووضع تلك الجداول في ملف خاص لجمع الأدلة قبل غلق الجهاز، وهذا يقتضي

---

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٢٠٣.

(٢) أ. طارق محمد الجملي، المرجع السابق، ص٥٨.

بالضرورة أن يكون المحقق قد أدرك تلك المعلومات قبل فصل التيار الكهربائي عنها[١].

**وهكذا نجد مما تقدم أن صعوبة استخلاص الدليل الإلكتروني ترجع إلى صعوبات متعددة منها متعلقة بالدليل الإلكتروني ذاته مثل خفاء الدليل وعدم رؤيته، فضلاً عن أن الجريمة الإلكترونية في الغالب لا تترك آثاراً، وأخيراً فإن أجهزة العدالة الجنائية قد تعيق الحصول على الدليل الإلكتروني متى انعدمت أو نقصت خبرتها بشأن كيفية استخلاص هذا الدليل.**

**وأخيراً تحدثنا في هذا المطلب عن صعوبات الحصول على الدليل الإلكتروني وقسمنا هذه الصعوبات التي تواجه الحصول على هذا الدليل إلى صعوبات متعلقة بالجريمة الإلكترونية وصعوبات متعلقة بالدليل الإلكتروني وأخيراً صعوبات مردها أسباب مختلفة.**

## المطلب الثاني
## مشروعية الحصول على الدليل الإلكتروني في الإجراءات التقليدية

يثير الحصول على الدليل الإلكتروني إشكالات قانونية وذلك بالنظر إلى طبيعته الخاصة[٢]، وهناك من يذهب إلى إن ما يثيره الدليل الإلكتروني من حيث مشروعية الحصول عليه يتركز بشكل أساسي في إجراءات التفتيش للبحث عن هذا الدليل، وذلك يثير إشكاليتين رئيستين:

**الأولى:** صفة القائم بالتفتيش.

**الثانية:** مدى مشروعية التفتيش عن الدليل الإلكتروني وضبطه في الوسط الافتراضي.

---

(١) أ. طارق محمد الجملي، المرجع السابق، ص٥٨.

(٢) د. ميسون خلف حمد الحمداني، المرجع السابق، ص٢٣٥.

ومرد هاتين الإشكاليتين يتعلق بإجراء التفتيش الذي يجب أن يمارس من ذي صفة وهو عضو الضابطة العدلية أو جهة التحقيق حسب الأحوال، فهل لهؤلاء القدرة على تفتيش الوسط الافتراضي وضبط ما سيسفر عنه من أدلة؟[١].

لكن مشروعية الحصول على الدليل الإلكتروني لا تقتصر على التفتيش والضبط بل تشمل الخبرة الإلكترونية ومعاينة مسرح الجريمة الإلكترونية فهي من الإجراءات التي تهدف إلى الحصول على الدليل الإلكتروني أيضاً.
وبناء على ذلك سنقسم هذا المطلب إلى أربعة فروع:

**الفرع الأول: الخبرة الإلكترونية.**
**الفرع الثاني: المعاينة الإلكترونية.**
**الفرع الثالث: التفتيش الإلكتروني.**
**الفرع الرابع: الضبط الإلكتروني.**

## الفرع الأول
## الخبرة الإلكترونية

تُعد الخبرة وسيلة لجمع الأدلة[٢]، والأصل في الخبرة أنها من إجراءات التحقيق الابتدائي لأنها تهدف إلى الوصول إلى الحقيقة، وبالتالي فإن انتداب الخبير يُعد

---

(١) خالد عياد الحلبي، المرجع السابق، ص٢٣٩.

(٢) اختلفت الآراء حول تحديد الطبيعة القانونية للخبرة، فهناك من يرى أن الخبرة وسيلة إثبات انطلاقاً من تبني أغلب التشريعات الجزائية المعاصرة نظام الإثبات الحرّ كقاعدة عامة، فإنها لم تحدد وسائل الإثبات تاركه للقاضي حرية تقديرها وتكوين اقتناعه، ولما كانت الخبرة كغيرها من وسائل الإثبات تهدف إلى تكوين هذه القناعة من خلال النتائج التي يتوصل إليها الخبير في فحص الآثار المادية، فهي تصلح لتأسيس الحكم عليها، ويدعم هذا الرأي أن الكثير من التشريعات تدرج الخبرة في القسم الخاص بالإثبات، وهو الاتجاه الذي اعتنقه المشرع الجزائري في قانون الإجراءات الجزائية، حيث نص على الخبرة في المادة (٢١٩) في الباب الأول من الكتاب الثاني تحت عنوان في طرق الإثبات، فتنص " إذا رأت الجهة القضائية لزوم إجراء خبرة فعليها اتباع ماهو منصوص عليه في المواد ١٤٣ إلى ١٥٦". بينما يذهب الرأي الثاني إلى أن الخبرة وسيلة لاستكشاف الدليل، حيث أن الخبرة ليست

إجراءً من إجراءات التحقيق، ولابد من التمييز بين تقرير الخبير الذي يعد من الأدلة وبين إجراء ندب الخبير، الذي يُعد من إجراءات جمع الأدلة، ولذلك تحرك به الدعوى الجزائية باعتباره إجراء من إجراءات التحقيق حتى لو كانت النيابة العامة لم تباشر قبله أي إجراء(١)، ولبحث الخبرة الإلكترونية لابد من دراسة، أولاً، مفهوم الخبرة الإلكترونية، وثانياً، مشروعية الخبرة الإلكترونية.

## أولاً: مفهوم الخبرة:

إن بحث مفهوم الخبرة يقتضي منا بحث تعريف الخبرة، وكذلك آلية عمل الخبير للحصول على الدليل الإلكتروني، لذلك لابد من دراسة:

**أ-تعريف الخبرة:**

تتضمن الخبرة إبداء رأي علمي أو فني من شخص صاحب اختصاص في شأن واقعة لها أهمية في الدعوى الجزائية، ولا يستطيع القاضي البت فيها لأنه لا يتوافر لديه مثل هذا الاختصاص(٢).

**ب- آلية عمل الخبير للحصول على الدليل الإلكتروني:**

يجب على خبير الأدلة الإلكترونية التعّرف أولاً على الدليل عن طريق تحديد نوع المعلومات المخزنة، ثمّ موقع تخزينها، وكيفية تخزينها، حتى يتمكن من اختيار الطريقة التقنية المناسبة لاستخراجها، وبعد استخراج الخبير الدليل الإلكتروني يلتزم بالحفاظ عليه بتفادي إحداث أي تغيير في البيانات التي يحتويها لأنّ العكس قد

---

وسيلة إثبات، بل هي وسيلة لاستكشاف وتقدير الدليل من خلال الآثار المتخلفة عن الجريمة والمجرم في مسرح الجريمة، وهذا مانادى به الفقه الأيطالي. بهلول مليكة، المرجع السابق، ص١٩٩-٢٠٠.

(١) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص٣٢٢ و٣٢٣.

(٢) د. بارعة القدسي، المرجع السابق، ص١٤٢.

يفقد الدليل قيمته القانونية، وأخيراً يقوم الخبير بتحليل الدليل بتفسير البيانات بطريقة واضحة ومفهومة[١].

كما يتوجب على الخبير الإلكتروني أن يوثق جميع مراحل عملية البحث، بحيث يشير إلى زمان البحث ومكان المعلومة وكيفية الحصول عليها، وأن يستخدم البرمجيات التي تحافظ على مواقع الويبّ التي عمل بها؛ لأنه من المعروف أن المعلومات تتغير على الإنترنت من لحظة إلى أخرى[٢].

## ثانياً: مشروعية الخبرة الإلكترونية:

إن دراسة مشروعية الخبرة الإلكترونية، يقتضي بيان الأساس القانوني لمشروعية إجراءها، وكذلك ضمانات مشروعية إجراءها، لذلك لا بد من دراسة:

أ-الأساس القانوني لمشروعية الخبرة الإلكترونية.

ب-ضمانات مشروعية الخبرة الإلكترونية.

### أ-الأساس القانوني لمشروعية الخبرة الإلكترونية:

أكد القانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات في المادة (٢٣) منه على وجوب الاستعانة بالخبرة في الإجراءات الجنائية المتعلقة بالجريمة الإلكترونية حيث نص فيها على أنه: " يجب الاستعانة في الإجراءات الجنائية المتعلقة بالجريمة المعلوماتية بخبير بيانات متخصص في البرامج واستخدام الإنترنت تلافياً لحدوث أضرار بالبرامج والبيانات المخزنة بالحاسب". أما قانون أصول المحاكمات الجزائية السوري لم يتضمن بشكل عام أحكاماً مستقلة بالخبرة، وإنما اعترف بها من ضمن الإجراءات التي يستطيع قاضي التحقيق اللجوء إليها إذا رأى ضرورة لذلك[٣]. وبالتالي أجاز المشرع السوري

---

(١) بهلول مليكة، المرجع السابق، ص١٧٦.

(٢) د. محمد طارق الخن، المرجع السابق، ص١١٥-١١٦.

(٣) د. بارعة القدسي، المرجع السابق، ص ١٨٠.

لجهات التحقيق ندب الخبراء إذا كانت طبيعة الجريمة محل التحقيق تقتضي الاستعانة بذوي الخبرة لحسم مسألة فنية معينة أو للبحث عن أدلة[١].

**ونحن نرى بضرورة جعل ندب الخبرة في الجريمة الإلكترونية وجوبياً من أجل الحصول على الدليل الإلكتروني نظراً لأن طبيعة هذه الجريمة تستلزم التعامل معها بطريقة حرَّفية أو فنية تفوق قدرات فريق التحقيق غير المؤهل، وذلك عن طريق تعديل قوانين الأصول الجزائية التي تجعل من ندب الخبراء أمراً جوازياً.**

ويلاحظ أن للخبرة أهمية خاصة في الجريمة الإلكترونية نظراً لأن الحاسبات وشبكات الاتصال تحتوي على أنواع ونماذج متعددة، كذلك فإن العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتنوعة، كما أن التطورات في مجالها سريعة ومتلاحقة لدرجة قد يصعب معها على المتخصص تتبعها واستيعابها[٢].

كما تتجلى أهمية الخبرة الإلكترونية بكونها وسيلة من وسائل الوصول إلى الدليل الإلكتروني في أنها تكشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية[٣].

فتشكيل فريق خبراء من الاعتبارات التي لا مناص منها وله أهمية خاصة نظراً للطبيعة الخاصة التي تتميز بها الجرائم الالكترونية عن غيرها من الجرائم، وذلك لأن هذه الجرائم مرتبطة بمسائل فنية وعلمية بحتة، لذلك يصبح لزاماً على القائم بالتحقيق الاستعانة بالخبراء والمختصين، لأن تصدي المحقق لفحص شيء وإبداء الرأي فيه دون أن تتوافر لديه المعرفة اللازمة يجعل قراره معيباً يضر بمصلحة التحقيق ويعوق الوصول إلى الحقيقة، وكل هذا يصب في أهمية التقارير التي

---

(١) د. عيسى مدالله المخول، المرجع السابق، ص١٦٠.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص١٦٧.

(٣) محمد نافع فالح رشدان العدواني، المرجع السابق، ص٨٧.

يُنجزها خبراء تقنية المعلومات في مجال الجرائم الالكترونية ويُعطيها مكانة متميزة من حيث الإلزام[١].

ويمكن إجمال المسائل التي يحتاج رجل الضابطة العدلية أو المحقق في وصفها إلى خبير معلوماتي، كمايلي:

١-وصف تركيب الحاسب وصناعته وطرازه ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها، بالإضافة إلى الأجهزة الطرفية الملحقة به وكلمات المرور أو السر ونظام التشفير وغيرها من الأمور المماثلة.

٢- وصف طبيعة بيئة الحاسوب أو الشبكة من حيث التنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية للمعلومات ونمط وسائط الاتصالات وتردد موجات البث وأمكنة اختراقها.

٣- وصف الموضع المحتمل لأدلة الإثبات والشكل أو الهيئة التي تكون عليها.

كذلك يحتاج رجل الضابطة العدلية إلى معونة الخبير المعلوماتي لبيان كيفية القيام بالآتي:

١-القيام عند الاقتضاء بعزل النظام المعلوماتي دون إتلاف الأدلة، أو تدميرها أو إلحاق ضرر بالأجهزة.

٢- كيفية نقل أدلة الإثبات إلى أوعية ملاءمة بغير أن يصيبها تلف.

٣- كيفية تجسيد الأدلة في صورة مادية بنقلها إذا أمكن إلى أوعية ورقية بحيث يتاح للقاضي مطالعتها وفهمها، مع إثبات أن المسطور على الورق مطابق لذلك المسجل على الحاسوب أو النظام أو الشبكة أو الدعامة الممغنطة[٢].

---

(١) م.م. حسين خليل مطر، إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية، بحث مقدم الى مؤتمر (الاصلاح التشريعي طريق نحو الحكومة الرشيدة ومكافحة الفساد) الذي اقامته مؤسسة النبأ للثقافة والاعلام وجامعة الكوفة، كلية القانون، في الفترة بين ٢٥-٢٦/٤/٢٠١٨م، ص٢٦-٢٧.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص١٦٩-١٧٠

## ب- ضمانات مشروعية الخبرة الإلكترونية:

إن الخبرة كغيرها من الإجراءات تخضع لما تقتضيه قواعد الشرعية الإجرائية التي تتطلب أن يكون القانون المصدر الوحيد لكل الإجراءات التي تتخذ ضد المتهم وإلا ترتب عليها البطلان، فلا متابعة جزائية ولا إجراء إلا بقانون(١).

وهنالك ضمانات معينة تكفل مشروعية إجراء الخبرة الإلكترونية أهمها:

**١- أن يقوم بالخبرة شخص مختص:**

يشترط في الخبرة بشكل عام أن تصدر عن شخص يتمتع بمؤهلات فنية وعلمية تسمح له بدراسة المسألة المستعصية على القاضي في سبيل تنويره، ولما كان لا يمكن لشخص واحد أن يختص بإبداء الرأي في جميع المسائل الفنية على اختلاف أنواعها بل تقتضي الضرورة أن يكون الخبير مختصاً في مجال معين من مجالات العلوم والفنون المتعددة(٢).

وإن البحث والتحقيق في هذا النوع من الجرائم (الإلكترونية)، يتطلب اللجوء إلى المختصين ذوي الخبرات في العلوم البيانية الرقمية، وفي هذا الإطار ظهر للوجود فرع علمي جديد هو علم " الأدلة الجنائية الحاسوبية أو الرقمية""، الذي يُعد من العلوم الحديثة والمعاصرة وقد بدأ الاهتمام به يزداد بازدياد الاعتماد على الأجهزة الرقمية بمختلف أنواعها، الحاسوب الآلي، الهاتف النقال، الكاميرات الرقمية، وغيرها من الأجهزة التي باستطاعتها تخزين معلومات، ويُعرف هذا العلم بأنه أحد فروع علم الأدلة الجنائية الذي يهتم بالتعّرف على الأدلة الرقمية وحفظها وتحليلها ثم تقديمها للقضاء(٣).

---

(١) بهلول مليكة، المرجع السابق، ص١٩٦.

(٢) بهلول مليكة، المرجع السابق، ص١٩٦.

(٣) بهلول مليكة، المرجع السابق، ص١٧٥.

لذلك يرى جانب من الفقه الجزائي[١] أن متطلبات العدالة الجنائية تفرض على الأجهزة الحكومية أن تتحمل كامل مسؤولياتها نحو اكتشاف الجرائم وضبط المجرمين ومحاكمتهم ، وهذا يقتضي توفير الإمكانيات التقنية اللازمة للتحقيق في الجرائم المعلوماتية، وبمعنى أخر يتعين استقطاب وجذب الكفاءات المهنية المتخصصة في هذا المجال ، للاستعانة بها في التحقيق في هذه الجرائم، ويتعين عدم التذرع بالميزانيات المالية كسبب يحول دون قيام الدولة بواجباتها نحو تحقيق العدالة الجزائية، وحتى يتم ذلك لابد من ضرورة الاستعانة بالنبضة المتخصصة في الحاسوب الآلي حال التحقيق في الجرائم المعلوماتية وذلك لضبط هذه الجرائم واكتشافها، وتقديم أدلة الإدانة فيها وشرح هذه الأدلة وابعادها أمام المحاكم ، ويجب أن يتم ذلك في إطار القانون الجزائي وخصوصاً قواعد الخبرة أمام المحاكم الجنائية والتي ينظمها قانون الإجراءات الجنائية.

**٢- تحليف الخبير يميناً قانونياً:**

لابد أن يحلف الخبير يميناً بأن يبدي رأيه بالذمة والصدق وأن يقدم تقريره كتابة، ويكون أداء اليمين من قبل الخبير أمام المحقق وقبل مباشرته لمهمته[٢].

ونص المشرع الجزائري في المادة (١٤٥) من قانون الإجراءات الجزائية على أداء الخبير القضائي اليمين القانونية، ويعد أداء اليمين إجراءاً جوهرياً يؤدي اغفاله الى بطلان ذلك الاجراء وما يترتب عليه.

كما نص المشرع السوري على هذه الضمانة في المادة (٤١) من قانون أصول المحاكمات الجزائية السوري، حيث يجب أن يحلف الخبير اليمين القانونية أمام القاضي قبل قيامه بالمهمة الموكولة إليه، وإذا لم يحلف اليمين، فإن تقريره ينقلب إلى مجرد رأي تستعين به المحكمة على سبيل المعلومات.

---

(١) أ.م. جاسم خريبط خلف، المرجع السابق، ص١٠.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص١٣٤.

**٣-حق الخصوم في الحضور:**

هناك من يرى[١] أن للخصوم الحق في الحضور أثناء مباشرة الخبير لمهمته، لكن يجوز له مباشرة مهمته في غياب هؤلاء وأن يمنعهم من الحضور إذا كان ذلك مبرراً.

ونص المشرع الجزائري في المادة (٤/١٥١) من قانون الإجراءات الجزائية على ضرورة حضور المتهم ومحاميه أعمال الخبرة.

وأغفل المشرع السوري هذه الضمانة وكان عليه أن ينص عليها.

**٤-حق الخصوم في رد الخبير:**

قد توجد أسباب قوية تشكك في حيدة الخبير المندوب من قبل المحقق، ويُخشى معها عدم التزامه بالموضوعية في القيام بمهمته، كما لو كان قريباً أو صديقاً لأحد الخصوم أو وكيلاً له في أعماله الخاصة[٢]، ويجوز رد الخبراء للأسباب نفسها التي تسوغ ردة القضاة[٣].

## الفرع الثاني
## المعاينة الإلكترونية

في هذا الفرع سنتطرق أولاً، إلى مفهوم المعاينة في الجريمة الإلكترونية كوسيلة للحصول على الدليل الإلكتروني، وثانياً، سندرس ضمانات مشروعية المعاينة للحصول على الدليل الإلكتروني.

---

(١) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص١٦٨.

(٢) د. جلال ثروت، نظم الإجراءات الجنائية، د.ط، دار الجامعة الجديدة، القاهرة، مصر، ٢٠٠٣م، ص٤٢٧. وقد نص على هذه الضمانة قانون الإجراءات الجنائية المصري في المادة (٨٩) منه.

(٣) د. بارعة القدسي، المرجع السابق، ص ١٤٥.

**أولاً: مفهوم المعاينة الإلكترونية:**

يقتضي بيان مفهوم المعاينة الإلكترونية تعريفها ثم بيان مدى صلاحية مسرح الجريمة الإلكتروني للمعاينة، وأخيراً بيان الآلية المتبعة فيها للحصول على الدليل الإلكتروني.

**أ-تعريف المعاينة:**

يقصد بالمعاينة: "إثبات حالة الأماكن والأشياء والأشخاص، وكل ما يفيد في كشف الحقيقة، والمعاينة بهذا المعنى تستلزم الانتقال إلى محل الواقعة أو إلى أي محل آخر توجد به أشياء أو آثار يرى المحقق أن لها صلة بالجريمة، غير أن انتقال المحقق قد يكون لغرض آخر غير المعاينة، كما في انتقال المحقق إلى مسكن المتهم أو غيره لتفتيش أو لسماع الشهود"(١).

**وبرأينا أن المعاينة هي عبارة عن إعادة تركيب الجريمة وربط مشاهدها، وإعادة تسلسل إحداثها.**

وإذا كانت المعاينة تتم بالانتقال إلى محل الواقعة الإجرامية كقاعدة عامة إجرائية مقررة في هذا الشأن إلا أنه في إطار جرائم الإنترنيت، فإن الانتقال يُعد من الموضوعات الجديدة، وذلك أن مسألة الانتقال هذه لا تكون بالضرورة عبر العالم المادي، وإنما يجب أن يكون بالضرورة عبر العالم الافتراضي فيستطيع عضو سلطة التحقيق أن يقوم بالمعاينة في مكتبه بالمحكمة من خلال الحاسوب الخاص به. كما يمكن أن يلجأ إلى مقهى الانترنت أو أن ينتقل إلى مقر مزود الخدمة الذي يعد أفضل مكان من خلاله لإجراء المعاينة، ذلك أنه في كل الأحوال يلزم أن يقوم المحقق بالمعاينة من خلال حاسوب أو حاسوب خادم ومن ثم فإن مشكلة الانتقال المادي إلى محل ارتكاب الواقعة الإجرامية لا تشكل عائقاً أمام عضو سلطة التحقيق وإنما المشكلة تكون من خلال الانتقال إلى العالم الافتراضي

---

(١) د. عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، ج١، د.ط، دار النهضة العربية، القاهرة، مصر، ١٩٨٥م، ص٣٧١.

حيث يلزم أن يكون هذا الانتقال بالسرعة الكافية التي تمنع زوال أثر الجريمة. ولهذا يجب أن يعجل بإجراء المعاينة خشية ضياع الأدلة[١].

**ب- مدى صلاحية مسرح الجريمة الإلكتروني للمعاينة:**

لكي نقرر مدى صلاحية مسرح الجريمة الإلكتروني للمعاينة، فإنه يجب التفرقة بين حالتين:

**١- الحالة الأولى: الجرائم الواقعة على المكونات المادية للحاسب:**

ومن أمثلة هذه الجرائم تلك الواقعة على أشرطة الحاسوب والكابلات الخاصة به، وشاشة العرض الملحقة به ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسب ذات الطابع المادي المحسوس وسرقة الأقراص المرنة بما فيها من معلومات[٢].

وليس هناك صعوبة مادية لتقرير صلاحية مسرح الجريمة الذي يضم هذه المكونات لمعاينته من قبل أعضاء الضابطة العدلية والتحفظ على الأشياء التي تُعد أدلة مادية على ارتكاب الجريمة ونسبتها إلى شخص معين، وكذلك وضع الأختام في الأماكن التي تمت المعاينة فيها، وضبط كل ما استعمل في ارتكاب الجريمة، والتحفظ عليها، والسبب في سهولة المعاينة في هذه الحالة، أنها تتم على مكونات مادية محسوسة كانت محلاً للجريمة أو تخلفت عنها[٣].

---

(١) أ. نزيهه مكاري، المرجع السابق، ص١٢٥.

(٢) د. عفيفي كامل عفيفي، جرائم الكومبيوتر، د.د.ن، القاهرة، مصر، ٢٠٠٠م، ص٣٣٦.

(٣) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٨٢-١٨٣.

**٢-الحالة الثانية: الجرائم الإلكترونية الواقعة على المكونات الغير المادية أو بواسطتها:**

وفي مقدمة هذه الجرائم، تأتي الواقعة على برامج الحاسوب أو بياناته أو تتم بواسطتها، وكذلك الجرائم التي تتم بطريق الإنترنت، ومنها كذلك جرائم التزوير المعلوماتي والتخريب الذي يتم بطريق الفيروس المعلوماتي(١).

وفي هذه الفروض تظهر عدة صعوبات تحَّول دون فاعلية المعاينة أو فائدتها، يمكن تلخيصها فيما يلي:

- الصعوبة الأولى تتمثل في ندرة الآثار المادية التي تتخلف عن الجرائم التي تقع على أدوات المعلوماتية بصفة عامة، وبرامج الحاسوب وبياناته بصفة خاصة.
- الصعوبة الثانية تتمثل في الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال الفترة من زمان وقوع الجريمة وحتى اكتشافها أو التحقيق فيها، وهي فترة طويلة نسبياً، الأمر الذي يعطي الفرصة للجاني أو للآخرين أن يغيروا أو يتلفوا أو يعبثوا بالآثار المادية للجريمة إن وجدت، الأمر الذي يورث الشك بدلالة الأدلة المستقاة من المعاينة في الجريمة الإلكترونية (٢).
- الصعوبة الثالثة تتمثل في مشكلة زوال الدليل الإلكتروني الذي يمكن تعديله أو تغييره أو محوه في بضع ثواني(٣).

---

(١) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٨٣.

(٢) د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص ٦٠-٦١.

(٣) د. نزيهة مكاري، إثبات جرائم الاعتداء على حق المؤلف عبر الإنترنت في التشريع الجزائري، دراسة مقارنة، الطبعة الأولى، دار هومة، الجزائر،٢٠٠٩م، ص١٢٥.

**جـ-آلية معاينة الدليل الإلكتروني:**

هناك من يرى[١] – ونحن نؤيده – أن الانتقال والمعاينة في الجرائم الإلكترونية تستوجب على القائم بالتحقيق أن يتعامل مع مكان وقوعها على أنه يتكون من مكانين أحدهما تقليدي والآخر افتراضي، والأول مثل غيره من أماكن وقوع الجريمة التقليدية يتكون بشكل أساسي من مكونات مادية ملموسة مثل أجهزة الكومبيوتر وشاشاتها وملحقاتها، والذي يمكن أن يترك الجاني فيه الكثير من الآثار المادية كبصمات أصابعه أو بعضا من مقتنياته الشخصية، وهو بصورة عامة يقع خارج البيئة الإلكترونية وتنطبق عليه كافة القواعد المتبعة في معاينة مكان وقوع الجريمة التقليدية، أما الثاني فانه يقع داخل البيئة الالكترونية ويتكون من بيانات رقمية (الكترونية) موجودة في داخل كمبيوترات أو على شبكة الانترنت وهو الذي يثير الجانب الأكبر من المشاكل في مجال التحقيق في الجرائم الإلكترونية.

وبالتالي يجب على أعضاء الضابطة العدلية أن يأخذوا في اعتبارهم مجموعة من الضوابط خلال معاينة مسرح الجريمة الإلكترونية من أجل الحصول على الدليل الإلكتروني، وتقسم هذه الضوابط إلى:

**١- ضوابط قبل التحرك إلى مسرح الجريمة الإلكترونية:**

- وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوبة معاينتها وشبكاتها.
- وجود خريطة توضح الموقع الذي ستتم معاينته، وتفاصيل المبنى أو الطابق موضوع الإخبار، وعدد الأجهزة والخزائن والملفات، ويحدد ذلك من خلال مصادر سرية لجهات الأمن.
- تحديد الأجهزة المحتمل تورطها في الجريمة الإلكترونية حتى يتم تحديد كيفية التعامل معها فنياً قبل المعاينة، سواء من حيث الضبط أو التأمين أو حفظ الأوراق والمستندات المتداولة.

---

(١) أ. م. جاسم خريبط خلف، المرجع السابق، ص١٩ – ٢٠.

- تأمين الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة سواء كانت أجهزة أو برامج صعبة أو لينة.
- إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء ورجال الضبط والأمن.
- إخطار الفريق الذي سيتولى المعاينة، قبل تمامها بوقف كافً حتى يستعد من الناحية الفنية والعملية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها.
- تحديد البيانات والمهام والاختصاصات المطلوبة من كل عضو في فريق المعاينة على حده، وذلك حتى لا تتداخل الاختصاصات.
- إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكلف تنفيذها على الوجه الأكمل.
- أن تتم كل هذه الإجراءات وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين الجزائية.
- تأمين عدم انقطاع التيار الكهربائي لأن معاينة الأجهزة وما بها من برامج وشبكات وأنظمة تشغيل لا جدوى منها في ظل عدم وجود التيار الكهربائي[١].

**٢- ضوابط أثناء معاينة مسرح الجريمة الإلكترونية:**

هنالك ضوابط يتعين أخذها في الحسبان عند معاينة مسرح الجريمة الإلكترونية، ومن أهمها:

- تحديد أجهزة الحاسوب الموجودة في مكان المعاينة وتحديد مواقعها بأسرع فرصة ممكنة وفي حالة وجود شبكة اتصالات يجب البحث عن خادم الملف ( File

(١) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٤٤ - ١٤٥.

server)، وذلك لتعطيل الاتصالات لمنع تخريب الأدلة الموجودة أو محوها[١]، وكذلك إثبات الحالة التي تكون عليها توصيلات وكابلات الحاسوب والمتصلة بمكونات النظام[٢].

- فصل التيار الكهربائي من مكان خارج الموقع قبل دخوله، فهذا الإجراء يمنع المستخدم من التلاعب في المعلومات أو محوها، وإن كان لذلك أثره في فقد المعلومات المخزنة في الذاكرة العشوائية لأجهزة الحاسبات الآلية، وأيضاً فصل خطوط التليفون خشية استعمال مودم في جهاز المعالجة الآلية للمعلومات المراد ضبطها[٣].
- فصل خطوط التليفون، حتى لا يسيء الجاني استعمالها كما في حالة التيار الكهربائي، والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعمليات الاستدلالات لأنهم قد يسيئون استغلالها، كما في الهاتف العادي لطمس البيانات[٤].
- القيام بتصوير الحاسوب الذي ترتكب عن طريقه الجرائم وما قد يتصل فيه من أجهزة طرفية ومحتوياته وأوضاع المكان الذي يوجد به بصفة عامة مع العناية بتصوير أجزاءه الخلفية وملحقاته الأخرى على أن يراعي تسجيل زمان ومكان والتاريخ الذي التقطت فيه كل صورة[٥].

---

(١) أ. م. جاسم خريبط خلف، المرجع السابق، ص١٨ – ١٩.

(٢) ورقة بعنوان: «دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول»، المرجع السابق،، ص٢٩.

(٣) د. جميل عبد الباقي الصغير، المرجع السابق، ص١٢٠.

(٤) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٢٣٨ – ٢٣٩.

(٥) أ. نزيهه مكاري، المرجع السابق، ص١٢٦.

- التأكد من سلامة الحاسوب أو الحاسوب الخادم بحيث تكون سلطة التحقيق قد احتفظت بما يسمح بالتأكد من دقة مصدر الدليل الإلكتروني[١]، كما ينبغي التأكد من عدم استخدام خاصية تحويل المكالمات، والتأكد من أن رقم الهاتف يخص جهاز الحاسوب المستهدف[٢]، فقد لوحظ أنه من الخدع المعتمدة لدى الهاكرز عند الاختراق، أن يتم ذلك بخط هاتف مسروق تم الدخول عليه، عن طريق الدخول إلى شبكة الهاتف ذاتها والتلاعب فيها، وذلك لأجل تضليل أجهزة المراقبة وأجهزة البحث بعد ذلك[٣].
- وضع حراسة كافية على مكان المعاينة، ومراقبة التحركات داخل مسرح الجريمة بل ورصد الاتصالات الهاتفية من وإلى مكان مسرح الجريمة[٤]، حيث من الممكن أن يتدخل الجاني من خلال وحدة طرفية لإتلاف المعلومات المخزنة في الجهاز (الوحدة الأم)[٥].
- إبعاد الموظفين عن أجهزة الحاسوب، بعد الحصول منهم على كلمات السر (Pass word) وكذلك الشفرات في حال وجودها، وكذلك إبعادهم عن الأماكن الأخرى التي توجد بها أجهزة حاسوب أخرى[٦].
- ملاحظة الطريقة المعد بها النظام المعلوماتي والآثار التي يخلفها، ومعرفة السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز المتصل عن طريق الدخول إلى النظام أو الموقع أو الدخول معه

---

(١) أ. نزيهه مكاري، المرجع السابق، ص١٢٦.

(٢) د. جميل عبد الباقي الصغير، المرجع السابق، ص١٢٠.

(٣) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٢٣٩.

(٤) أ. م. جاسم خريبط خلف، المرجع السابق، ص١٨ – ١٩.

(٥) د. جميل عبد الباقي الصغير، المرجع السابق، ص١٢٠.

(٦) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٢٣٩.

فـي حـوار، وبروتوكـولات الاتصـال عبـر الإنترنـت وإن تعلقـت الجريمـة بهـذه الشبكة والتي تعرف اختصاراً بـ (ip)[١] .

- عدم نقل المواد المعلوماتية خارج مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي للحاسوب من مجالات القوى المغناطيسية – الممرات المغناطيسية – التي قد تتسبب في محو البيانات[٢] .
- الـتحفظ علـى محتويـات سـلة المهمـلات[٣]، والـتحفظ علـى مسـتندات الإدخـال والمخرجات الورقية للحاسوب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليها من بصمات[٤].
- عدم التسرُّع في نقل أي مادّة معلوماتيّة من مكان وقوع الجريمة خشية إتلاف البيانات المخزنة[٥].

**ونرى أن هنالك اختلاف كبير بين معاينة الجرائم التقليدية الذي يتم في العالم المادي عنه في معاينة الجرائم الإلكترونية الذي يتم في العالم الافتراضي**

---

(١) يعرف (ip) وهو اختصار كلمة "internet protocol" أنه وسيلة لنقل البيانات من مكان على الإنترنت إلى مكان آخر، أما (ip adress) فهو عنوان مكون من أربعة أرقام = ويستخدم لتحديد هوية كل جهاز يتصل بالإنترنت.

(٢) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٤٨.

(٣) فمن فحص بعض البطاقات المثقبة المعثور عليها بسلة مهملات في موقع الحاسب أمكن كشف غموض جريمة شهيرة لسرقة البرمجيات عن بعد وقعت في سانتا كلارا بالولايات المتحدة الأمريكية. أ. د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، المرجع السابق، ص٤٨٦.

(٤) أ. د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، المرجع السابق، ص٤٨٧.

(٥) ورقة بعنوان: «دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول»، المرجع السابق،، ص٢٩.

**حيث يقتضي ذلك السرعة في إجراء هذه المعاينة خشية زوال الدليل الإلكتروني والتخصص الدقيق فيمن يقومون بإجراء هذه المعاينة.**

**ثانياً: ضمانات مشروعية المعاينة الإلكترونية للحصول على الدليل الإلكتروني:**

هنالك ضمانات يجب أن تتوافر بالمعاينة الإلكترونية حتى يكون الدليل الإلكتروني الناتج عنها مشروع، ومن أهم هذه الضمانات:

**أ-وقوع جريمة:**

من المؤكد أنه لا يمكن إجراء المعاينة قبل وقوع الجريمة لأن الواقعة قد تكون مجرد أعمال تحضيرية غير معاقب عليها(١).

والمعاينة إجراء جائز في كل الجرائم شرط أن يتفق وطبيعة الجريمة ذاتها لكنه إجراء جوازي في الجنح والمخالفات، ووجوبياً في الجنايات(٢).

لكن السؤال الذي يطرح نفسه هو: ما هي الوسائل التي يتم بها الإخبار والتحري والاستقصاء عن الجرائم الإلكترونية؟ كما لابد من معرفة ما هي كيفية تحديد نطاق الجريمة؟ وبناء على ذلك سندرس وسائل إثبات وقوع الجرائم الإلكترونية، ومن ثم كيفية تحديد نطاق الجريمة.

**١- وسائل إثبات وقوع الجرائم الإلكترونية:**

في الجريمة الإلكترونية يوجد وسيلتين للإخبار والاستقصاء عن وقوع الجرائم الإلكترونية، وهما:

**الوسيلة الأولى: تقديم الإخبار أو الشكوى عن الجرائم الإلكترونية:**

لا تختلف أحكام الإخبار أو الشكوى في الجرائم الإلكترونية كثيراً عما هو عليه الحال في الجرائم التقليدية. فمن الممكن أن يتم الإخبار عن الجرائم

---

(١) بهلول مليكة، المرجع السابق، ص٢٣.

(٢) د. عفيفي كامل عفيفي، المرجع السابق، ص٣٣٥.

الإلكترونية **بالأسلوب المادي**، كأن يتوجه مقدم الإخبار بنفسه إلى أقرب قسم للشرطة أو للنيابة العامة للإدلاء بإخباره. كما يمكن أن يتم الإخبار **بالأسلوب المعنوي** عن طريق الهاتف أو البريد العادي.

وإلى جانب هذين الأسلوبين، ظهر أسلوب ثالث في إطار الجرائم الإلكترونية وخاصة جرائم الإنترنت، وهو **الأسلوب الرقمي**، حيث أصبح من الممكن تقديم الإخبار أو الشكوى عن طريق الإنترنت بإحدى الطريقتين التاليتين:

**الطريقة الأولى:** وهي كتابة رسالة إلكترونية تتضمن الإخبار عن جريمة إنترنت، وإرسالها إلى عنوان البريد الإلكتروني العائد لأحد الأجهزة المختصة بمكافحة جرائم الإنترنت، كالقيام بكتابة رسالة إلكترونية تتضمن الإخبار عن وجود مواقع إلكترونية أُعدت للاحتيال أو مواقع إباحية مثلاً، وإرسالها إلى عنوان البريد الإلكتروني للجهة المختصة، كما هو الحال في أميركا حيث يرسل إلى موقع المباحث الفيدرالية الأمريكية FBI، أو موقع إدارة العدل الأمريكية USDJ، أو موقع وكالة المخابرات المركزية الأمريكية CIA، أو موقع هيئة حماية البرمجيات الأوربية APP، أو غيرها من المواقع الأخرى[١].

**الطريقة الثانية:** وهنا يتم التبليغ عن طريق ملء بيانات الاستمارة الرقمية، التي تكون متوفرة عادةً على المواقع الإلكترونية المخصصة لتلقي الإخبارات والشكاوى، كما هو متبع في المواقع التالية:

* الموقع الإلكتروني لمركز تلقي شكاوى جرائم الإنترنت IC3.
* الموقع الإلكتروني لمركز جرائم الياقات البيضاء NW3C.
* الموقع الإلكتروني العائد للمكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات في فرنسا. فبعد أن يتم تلقي الإخبارات عن طريق هذا الموقع الفرنسي، تتم عملية تحليل ودراسة تلك الإخبارات، للتأكد من صحة ما ورد فيها من معلومات حول واقعة الجريمة، ثم يتم إخبار مصالح الدرك

---

(١) د. محمد طارق الخن، المرجع السابق، ص٩٦ – ٩٧.

والشرطة حسب الاختصاص الإقليمي؛ كما يتم إعطاء مقدم الإخبار رقم الاستمارة الرقمية الخاصة به حتى يتمكن من معرفة مستجدات التحقيقات.

* موقع إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، العائد للحكومة المصرية.

ولابدّ من الإشارة إلى الدور الهام الذي يلعبه مقدم الإخبار أو الشاكي في إطار جرائم الإنترنت، لأنه في كثير من الأحيان يكون هذا الإخبار هو الوسيلة الوحيدة لعلم السلطات المختصة بوقوع الجريمة[١].

وهناك من يرى[٢] – ونحن نؤيده – أن تقديم الإخبار أو الشكوى عبر الإنترنت يسّهل عملية إعلام السلطات المختصة بوقوع الجريمة، كما يؤمّن الحماية لمقدم الإخبار الذي يظلّ مجهولاً في أغلب الأحيان.

**ولم يعالج المشرع السوري هذه المسألة ونرى أنه على أجهزة العدالة السورية أن تنشأ مواقع إلكترونية متخصصة في تلقي الإخبارات والشكاوى المتعلقة بالجرائم الإلكترونية.**

**وتثير مسألة الإخبار عن الجريمة الإلكترونية مسائل تتعلق بمدى ما هو متاح من نصوص في التشريعات الجزائية التي توجب الأخبار وترتب عقوبة على ذلك.**

فقد جعل المشرع في دولة الإمارات العربية المتحدة الإخبار عن الجرائم إلزامي كقاعدة عامة، ومن يخالف ذلك يتعرض للجزاء الجزائي. فقد أوجبت المادة (٣٧) من قانون الإجراءات الجزائية الاتحادي رقم ١٩٩٢/٣٥ "على كل من علم بوقوع جريمة مما يجوز للنيابة العامة أو أحد مأموري الضبط القضائي أن يبلغ عنها"، كما نصت المادة (٣٨) من ذات القانون على أنه: "يجب على كل من علم من الموظفين العموميين أو المكلفين بخدمة عامة أثناء تأديته عمله أو بسبب

---

(١) د. محمد طارق الخن، المرجع السابق، ص٩٧.

(٢) د. محمد طارق الخن، المرجع السابق، ص٩٧.

تأديته بوقوع جريمة من الجرائم التي يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب أن يبلغ فوراً النيابة العامة أو أقرب مأموري الضبط القضائي". ورتب المشرع على الإخلال بهذا الواجب عقوبة جزائية إذ نصت المادة (١/٢٧٢) من قانون العقوبات الاتحادي على أنه: "يعاقب بالغرامة كل موظف غير مكلف بالبحث عن الجرائم أو ضبطها أهمل أو أرجأ إبلاغ السلطة المختصة بجريمة علم بها في أثناء أو بسبب تأديته وظيفته، ولا عقاب إذا كان رفع الدعوى معلقاً على شكوى". ومؤدى ذلك معاقبة الموظف جزائياً على عدم الأخبار أو الإهمال فيه حتى ولو لم يكن مكلفاً بالبحث عن الجريمة أو ضبطها[١].

**ونرى أنه قد أحسن المشرع الإماراتي في ذلك لأن اعتبار عدم إخبار الموظفين عن جريمة إلكترونية جريمة ومعاقب عليه يسهم بشكل كبير في عدم التقاعس عن كشف الجرائم الإلكترونية وكشف أدلتها.**

كما نص المشرع السوري في قانون أصول المحاكمات الجزائية السوري لعام ١٩٥٠ م في المادة (٢٥) منه على أنه: " على كل سلطة رسمية او موظف علم اثناء اجراء وظيفته بوقوع جناية او جنحة ان يبلغ الامر في الحال إلى النائب العام المختص، وأن يرسل إليه جميع المعلومات والمحاضر والأوراق المتعلقة بالجريمة".

وكذلك نص المادة (٢٦) من نفس القانون الذي جاء فيه: " ١- من شاهد اعتداء على الأمن العام أو على حياة أحد الناس أو على ماله يلزمه أن يعلم بذلك النائب العام المختص.

٢- لكل من علم في الأحوال الأخرى بوقوع جريمة أن يخبر عنها النائب العام".

وهذين النصين يتعلقان بالأخبار عن جريمة عادية (تقليدية) ونرى أنهما يشملان الأخبار عن الجرائم الإلكترونية أيضاً.

---

(١) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٦٢ - ١٦٣.

**الوسيلة الثانية: الإرشاد الجنائي عبر الإنترنت:**

يقصد **بالإرشاد الجنائي** "قيام عنصر الضابطة العدلية أو الغير، بالولوج إلى الإنترنت، والدخول في حلقات النقاش والدردشة، مستخدماً اسماً أو صفةً مستعارة أو وهمية، وذلك بقصد البحث عن الجرائم ومرتكبيها، وإلقاء القبض عليهم، وإحالتهم إلى القضاء".

والفارق بين نظام الإرشاد الجنائي في الجرائم التقليدية ونظام الإرشاد الجنائي في الجرائم الإلكترونية، هو أن المرشد أو المخبر في الجرائم التقليدية غالباً ما يكون من الغير، أي ليس من رجال الضابطة العدلية، أما المرشد في الجرائم الإلكترونية، فمن الممكن أن يكون أحد رجال الضابطة العدلية، إذ إن الأمر لا يتطلب منه سوى الحصول على إذن رسمي من رؤسائه للقيام بهذه المهمة، ثم يلج بواسطة حاسوبه إلى شبكة الإنترنت، حيث يدخل إلى حلقات الدردشة والنقاش مثلاً، مستخدماً اسماً مستعاراً أو صفة وهمية، فيتناول الأحاديث العادية مع الغير، دون أن يدفعه إلى ارتكاب الجريمة، فيظهر وكأنه يسعى لإضاعة الوقت والهروب من الملل، إلى أن يبرز هذا الغير مشروعه الإجرامي، كأن يدور الحديث حول طريقة الحصول على أرقام بطاقات الائتمان بصورة احتيالية، أو كيفية إعداد المواقع الخلاعية، أو المواقع المعدة لبيع المسروقات، أو كيفية اختراق المواقع، أو زرع الفيروسات...الخ. ويمكن للمرشد أيضاً أن يقوم بطرح الأسئلة على الغير، حتى يتمكن من الحصول على أكبر قدر ممكن من المعلومات، وعندما تتضح الصورة كاملةً، يقوم المرشد – إذا كان من الغير – بإيصال هذه المعلومات إلى الجهات المختصة، التي تباشر عملها في تعقب هذا المجرم والقبض عليه، مستخدمة في ذلك برمجيات معينة تقودها إلى مزود خدمة الإنترنت الذي يتحرك فيه هذا المجرم؛ أما إذا كان المرشد أحد رجال الضابطة العدلية، فيقوم باستدراج المجرم حتى يتم القبض عليه.

ومن أمثلة الإرشاد الجنائي، قيام مكتب التحقيقات الفيدرالي FBI، بضبط أفراد عصابة "فاستلان" Fastlan المنتشرين حول العالم، الذين امتهنوا قرصنة البرمجيات وتحميلها على مواقع للهكرة، وجنوا أرباحاً وصلت إلى مليون دولار في فترة زمنية قصيرة، حيث تم إلقاء القبض على تسعة منهم في الولايات المتحدة الأمريكية، وتمّت إدانتهم أمام هيئة المحلفين العليا في شيكاغو. وقد استعملت المباحث الفيدرالية في هذه القضية أسلوب الإرشاد الجنائي، عندما دسّت أحد عناصرها في هذه العصابة إلى أن تمّ إلقاء القبض عليهم.

والحقيقة أن نظام الإرشاد الجنائي عبر الإنترنت هو من أهم وسائل تحري واستقصاء الجرائم الإلكترونية، وهو نظام لا بدّ من الأخذ به في جميع الدول التي تسعى للحدّ من هذه الجرائم(١).

**ونرى أنه يعدّ الإرشاد الجنائي من أهم الوسائل التي يمكن أن يعتمد عليها رجال الضابطة العدلية في عملية تحري واستقصاء الجرائم الإلكترونية.**

**الوسيلة الثالثة: التزام الشاهد المعلوماتي بالإعلام عن الجريمة الإلكترونية:**

يُعرَّف الشاهد المعلوماتي بأنه هو: " الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي، والذي تكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات متى كانت مصلحة التحقيق تتطلب التنقيب عن المعلومات داخله، ولذلك يطلق على ذلك الشخص اسم الشاهد – المعلوماتي– تمييزاً له عن الشاهد– التقليدي"(٢).

ويمكن القول إن الشاهد المعلوماتي ينحصر في عدة طوائف وفئات هي:

---

(١) د. محمد طارق الخن، المرجع السابق، ص٩٨ – ٩٩.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص٣٣٩.

**- مشغلوا الحاسوب:**

عامل تشغيل الحاسوب هو ذلك الشخص المسؤول عن تشغيل الجهاز والمعدات المتصلة به، ولا بد أن يكون لديه خبرة كبيرة في استخدام الحاسوب ومكوناته عن طريق استخدام هذه البيانات وكيفية إدخال البيانات ثم استخراجها، وهو يقوم بنقل البيانات من الوثائق إلى وسائط التخزين التي تجري معالجتها بواسطة الحاسوب ويجب كذلك أن تكون لديه خبرة واسعة في الكتابة السريعة عن طريق لوحة مفاتيح الحاسوب [١].

**- خبراء البرمجة:**

أو مخططو البرامج وهم الأشخاص المتخصصين، في كتابة أوامر البرامج، وهم فئتين، الأولى هم مخططوا برامج التطبيقات والثانية هم مخططوا برامج النظم.

**- المحللون:**

والمحلل هو الشخص الذي يحلل الخطوات، ويقوم بتجميع البيانات الخاصة بنظام معين، ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقة الوظيفية بين هذه الوحدات، كما يتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات، واستنتاج الأماكن التي يمكن مكننتها بواسطة الحاسب.

**- مهندسوا الصيانة والاتصالات:**

وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسوب بمكوناته وشبكات الاتصال المتعلقة به.

---

(١) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص٣٣٩.

**- مديرو النظم:**

وهم الذين توكل لهم أعمال الإدارة في النظم المعلوماتية[١].

وفي الحقيقة أنه ثمة أشخاصاً آخرين يعدون بمثابة الشهود في الجريمة الإلكترونية، وهم مقدمي الخدمات الوسيطة في مجال المعلوماتية والإنترنت ومن هؤلاء متعهدي الوصول[٢] ومتعهدي الإيواء[٣] والمنتج[٤] وناقل المعلومات[٥]

---

(١) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص٣٤٠.

(٢) يقصد بمتعهد الوصول بأنه : "أي شخص طبيعي أو معنوي يقوم بدور فني لتوصيل المستخدم – الجمهور – إلى شبكة الإنترنت، وذلك بمقتضى عقود الاشتراك (Abonement) تضمن توصيل العميل إلى المواقع التي يريدها". د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص٣٩.

(٣) يقصد بمتعهد الإيواء بأنه: "شخص طبيعي أو معنوي يعرض إيواء صفحات الويب (Web) على حاسباته الخادمة مقابل أجر، فهو بمثابة مؤجر لمكان على الشبكة، للمستأجر (الناشر) والذي ينشر عليه ما يريد من نصوص أو صور أو ينظم مؤتمرات مناقشة أو ينشئ روابط معلوماتية مع المواقع الأخرى". د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص٣٩.

(٤) ويقصد به: "منتج الخدمة المعلوماتي في وسائل الاتصال السمعي والبصري"، ولأنه وفقاً للمادة (٩٣ – ٣) من القانون الفرنسي الصادر في ٢٩ يوليو ١٩٨٢ أنه إذا ارتكبت جريمة مما نص عليه في الباب الرابع من القانون الصادر في يوليو ١٨٨١ بواسطة وسيلة للاتصال السمعي أو البصري فإن مؤلف الرسالة – المادة المعلوماتية – غير المشروعة، ومتى تم تحريك الدعوى الجنائية ضده، فإن منتج الخدمة يعاقب كفاعل أصلي، وذلك دون اشتراط سبق تسجيل المادة المعلوماتية حتى يقال بأنه مارس حقه في الرقابة كما هو الحال في مسؤولية متعهد الإيواء. د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٩-٤٠.

(٥) يعرف ناقل المعلومات بأنه: "العامل الفني الذي يقوم بالربط بين الشبكات، وذلك بمقتضى عقد نقل معلومات – في هيئة حزم – من جهاز المستخدم إلى الحاسب الخادم لمتعهد الوصول، ثم نقلها من هذا الحاسب الأخير إلى الحاسبات المرتبطة بمواقع الإنترنت أو بمستخدمي الشبكة الآخرين، وذلك من خلال الحاسبات المرّحلة". د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص٤٠.

ومتعهد الخدمات[١]، وكذلك مورد المعلومات[٢] ومؤلف الرسالة[٣]، وهؤلاء جميعهم بحكم دورهم في توصيل – طالب الخدمة – أو المستهلك إلى شبكة الإنترنت[٤].

والتزام الشاهد بالإعلام عن الجريمة الإلكترونية يعني وباختصار أنه في الجرائم الإلكترونية ومتى كان الشاهد حائزاً على معلومات جوهرية لازمة لاختراق نظام المعالجة الآلية بحثاً عن أدلة للجريمة داخله تتطلبها مصلحة التحقيق، فإنه يكون مطالباً بأن يعلم بها سلطات التحقيق والتحري على سبيل الإلزام، وإلا تعرض للعقوبات المقررة للامتناع عن الشهادة، وذلك في غير الأحوال التي يجيز له القانون فيها ذلك[٥].

---

(١) يُعرف متعهد الخدمات بأنه: "ناشر الموقع، وهو المسؤول الأول عن المعلومات التي تعبر الشبكة، لأنه الوحيد صاحب السلطة الحقيقية في مراقبة المعلومات التي يجري بثها". د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت ، المرجع السابق، ص٤٠.

(٢) يعرف مورد المعلومات بأنه: "ذلك الشخص الذي يقوم بتحميل الجهاز أو النظام بالمعلومات التي قام بتأليفها وجمعها حول موضوع معين، ومن ثم تكون له سيطرة كاملة على المادة المعلوماتية التي تثبت عبر الشبكة، فهو الذي يقوم بالاختيار ثم التجميع والتوريد حتى تصل إلى الجمهور في صورة مادة معلوماتية على الشبكة". وبذلك المعنى تتحقق له السيطرة كاملة على هذه المعلومات لأنه يملك جمعها من عدمه، ويملك توريدها أو الامتناع عن ذلك.
د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٤٠-٤١.

(٣) مؤلف الرسالة هو المسؤول الأول عن أي معلومات غير مشروعة تتضمنها هذه الرسالة، فإن تضمنت مثلاً عبارات القذف أو السب التي يرسلها أو ينشرها على أحد المؤثرات، فإن مؤلف الرسالة يسأل جزائياً عن هذه العبارات، كما أنه يمكن أن يسأل كشاهد عن المعلومات التي وصلت إليه من خلال دوره في خدمة العميل أو المستهلك على الشبكة المعلوماتية.
د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص٤١.

(٤) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٨-٣٩.

(٥) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٤٠-٣٤١.

والتزام الشاهد بالإعلام في الجريمة الإلكترونية له مجموعة من السمات الجوهرية هي:

**-الالتزام بالإعلام في الجرائم الإلكترونية لا بد أن يكون التزاماً قانونياً:**

فمن المنطقي ألا نطالب المهنيين والحرفيين وغيرهم من مستخدمي الحاسوب، الإعلام بالمعلومات والبيانات الجوهرية التي لديهم إلى سلطات التحقيق لمساعدتهم في المهام المنوطة بهم بمناسبة جريمة إلكترونية مالم يكن هناك نصاً صريحاً يقضى بهذا الالتزام(١).

**وذلك النص غير موجود في القانون السوري لذلك نقترح على المشرع السوري التدخل وتقنين هذه المسألة.**

**-الالتزام بالإعلام في الجريمة الإلكترونية، هو التزام مستقل وله ذاتيته الخاصة به:**

إن الالتزام بتأدية الشهادة لا يشمل أو يتضمن التعاون الفعال المتمثل في القيام بطبع ملفات البيانات المخزنة في ذاكرة الحاسوب أو في الإفصاح عن كلمات المرور السرية أو الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج، وذلك أن هذا الالتزام يزيد على نطاق الشهادة(٢).

وبالتالي يمثل هذا الالتزام واجباً جديداً مفروضاً بواسطة القانون لا سيما على بعض الفنيين أو الحرفيين من الشهود أو مستخدمي الحواسيب وذلك بتقديم المعلومات الجوهرية والمهمة والتي تتصل بموضوع النظام المعلوماتي محل البحث والتحقيق، وخاصية هذا الاستقلال، تجعل هذا الالتزام مستقلاً عن غيره من

---

(١) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص٣٤١.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص٣٤٤.

الالتزامات التي تقترب منه أو تتشابه معه وهو ما يضفي عليه ذاتية خاصة تستوجب أن يكون لها نص تشريعي خاص بها[١].

وهناك عدة شروط لالتزام الشاهد المعلوماتي بالإعلام عن الجريمة الإلكترونية، وهي تشكل ضمانات لهذا الالتزام، وهي:

**-أن نكون بصدد جريمة إلكترونية وقعت بالفعل سواء كانت جناية أو جنحة:**

حتى يلتزم الشاهد المعلوماتي بالإعلام عن الجريمة الإلكترونية، فلا بد أن تكون هذه الجريمة قد وقعت بالفعل، فذلك الالتزام- وحسب القواعد العامة- لا يمكن تصوره لضبط جريمة مستقبلية حتى ولو كانت التحريات الجدية قد أثبتت أن هذه الجريمة سوف تقع بالفعل، ولا يكفي وقوع أية جريمة وإنما لا بد وأن تكون جناية أو جنحة أما المخالفات فإنها تستبعد لأنها هينة الأثر[٢].

**-أن يكون الشاهد المعلوماتي على علم ومعرفة بالمعلومات الجوهرية المتصلة بالنظام المعلوماتي محل الواقعة:**

إن معرفة الشاهد بمضمون المعلومات الجوهرية المتصلة بالنظام المعلوماتي محل الواقعة تمثل شرطاً مهماً لنشأة وميلاد الالتزام بالإعلام في الجرائم الإلكترونية[٣].

**-أن تقتضي مصلحة التحقيق الحصول على هذه المعلومات الجوهرية:**

لابد حتى يقوم الشاهد بأداء التزامه بالإعلام في الجريمة الإلكترونية، أن تتطلب مصلحة التحقيق الحصول على المعلومات الجوهرية، خاصة إذا كان الأمر يتطلب اختراق النظام المعلوماتي لأجل البحث عن أدلة الجريمة الكائنة بداخله[٤].

---

(١) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص٣٤١-٣٤٢.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٤٩.

(٣) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٤٩.

(٤) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٥٠.

**٢- كيفية تحديد نطاق الجريمة:**

يمكن القول إن عدم وضع التشريعات الجنائية معايير لتحديد النطاق المكاني لمسرح الجريمة، الغرض منه ترك المجال للباحث والمحقق لتقدير نطاق نشاطه الإجرائي بشرط عدم تجاوز حدود اختصاصه الإقليمي، طالما أن توسيع دائرة مسرح الجريمة لا يشكل مساساً ولا خرقاً لأسرار الأفراد وحرمتهم، بل على العكس من ذلك قد يفسح المجال لتوسيع دائرة البحث عن الآثار المترتبة عن الجريمة[١].

ويبدو أن محكمة النقض الفرنسية[٢] أكثر تسامحاً في الاختصاص الإقليمي لأعضاء الضابطة العدلية، ففي أحدى القضايا التي ترجع إلى ١٠ يناير سنة ١٩٩٢ كان أحد أعضاء الضابطة العدلية يتلقى – منذ توليه وظيفته – تليفوناً أو بالفاكس من العديد من الأشخاص من خارج دائرة اختصاصه معلومات مفيدة في التحقيق الأولي (Enquête préliminaire) الذي كان يتولاه وكانت المعلومات التي يتلقاها تلفونياً يقوم بكاتبتها ويرفقها بالإجراءات، كما كان يحدث بالنسبة للمستندات التي يحصل عليها بطريق الفاكس، فقام المتهم بالطعن في هذا الإجراء أمام غرفة الاتهام (Chambre d'accusation) على أساس أن عضو الضابطة العدلية قد تجاوز اختصاصه الإقليمي وخالف الأحكام المتعلقة بسماع الشهود، إلا أن غرفة الاتهام رفضت هذا الطعن، لأنها ترى أن الإجراء الذي قام به عضو الضابطة العدلية لا يعني انتقاله إلى خارج اختصاصه التي يمارس فيها وظائفه عادة، وعلاوة على ذلك فإن جمع المعلومات عن طريق التلكس أو التليفون لا يمكن تشبيهها بسماع الشهود، وإنما هي مجرد رسائل لا تعدو قيمتها مجرد معلومات تخضع لرقابة قاضي التحقيق، وتلى ذلك أن قام المتهم بالطعن في قرار غرفة

---

(١) بهلول مليكة، المرجع السابق، ص٢٢.

(2) Crim, 10 Janvier 1995, Dr. Pén, Rev. Mensuelle, Juin 1995, P 11.

الاتهام بالبطلان أمام محكمة النقض والتي قضت برفض هذا الطعن على أساس أنه "طبقاً للمادة (١/١٨) من قانون الإجراءات الجنائية الفرنسي فإن أعضاء الضابطة العدلية ليس لهم اختصاص – من حيث المبدأ – إلا في حدود دوائر اختصاصهم الإقليمي، حيث يمارسون وظائفهم المعتادة، فليس هناك ما يمنعهم من جمع المعلومات من خارج دوائر اختصاصهم بواسطة التليفون أو الفاكس أو أي وسيلة أخرى للاتصال، حيث أن قيمة المعلومات التي يتم جمعها بهذا الطرق تخضع للمناقشة الحضورية للأطراف وتخضع لتقدير محكمة الموضوع". وطبقاً لهذا القضاء لمحكمة النقض الفرنسية فإن الانتقال غير المادي للمعلومات (Transfert immatérielle d'information) من مكان يقع خارج الحدود الإقليمية لاختصاص عضو الضابطة العدلية إلى دائرة اختصاصه لا يخالف القانون، وبالتالي يمكن الاعتماد عليها كدليل إثبات فالمادة (١/١٨) من قانون الإجراءات الجنائية الفرنسي لا تنطبق إلا في حالة الانتقال المادي ( Déplasseement physique) لعضو الضابطة العدلية خارج حدود اختصاصه الإقليمي.

وكذلك – فإنه بحسب محكمة النقض الفرنسية – يمكن الحصول على المعلومات بأي وسيلة للاتصال، وبالتالي يكون لعضو الضابطة العدلية أن يطلع على الملفات عن بُعد (Consultation des fichiers à distance)[١].

**ب–وجود مشتبه به في الجريمة:**

السؤال الذي يطرح نفسه هنا هو: **كيف يتم تعقب المشتبه به في الجرائم الإلكترونية؟**

للإجابة عن هذا السؤال سنلقي الضوء على آلية تعقب المشتبه به في الجرائم الإلكترونية، ثم نتعرض لأشهر الشركات التي تقوم بعملية التتبع، ومن ثم معرفة كيفية تتبع البريد الإلكتروني المزيف.

---

(١) د. جميل عبد الباقي الصغير، المرجع السابق، ص١٠٢ – ١٠٣.

**١- آلية تعقب المشتبه به في الجرائم الإلكترونية:**

تتيح البنية التحتية للإنترنت إمكانية التعرف على عنوان الحاسوب المستخدم في ارتكاب الجريمة فقط، وهو ما يعرف بعنوان Internet Protocol (IP)، الذي يشير إلى رقم يتم بموجبه تحديد الحاسوب الذي تمّ النفاذ من خلاله إلى الإنترنت. وبعد تحديد هوية الحاسوب المستخدم بارتكاب الجريمة، تبدأ عملية اتخاذ الإجراءات اللازمة لإلقاء القبض على المشتبه به.

ويمكن تشبيه عنوان الإنترنت الرقمي (ip adress) بأرقام الهواتف. فعنوان الإنترنت يزودنا بالمنطقة الجغرافية التي انطلقت منها الرسالة (البلد والمدينة، واسم المضيف Hostname، وتحديد الموقع التقريبي)، وبفضل هذه المعلومات يمكن في أغلب الأحوال تعيين المشتبه به[١].

ويعرف عنوان (ip adress) بأنه : "عنوان مكون من أربعة أرقام ويستخدم لتحديد هوية كل جهاز يتصل بالإنترنت"[٢].

ويمكن الاستفادة عما يكشف عنه الرقم (ip) في البحث والتحقيق الجنائي، ذلك أنه عندما يزور شخص ما موقعاً على الشبكة، يسجل الموقع (ip) العائد للكومبيوتر الذي اتصل به، وعند إرسال بريد إلكتروني كذلك، يمكن لمستلم الرسالة معرفة عنوان الكومبيوتر المرسل، كذلك عند استخدام برنامج (الأوت لوك)، فيكفي النقر على أوبشن (option) بعد أن يفتح الرسالة، فيتم الاطلاع على عنوان المرسل. وذلك أنه عندما يتجول مستخدم الإنترنت في حوار إنترنت، فإنه يترك آثار أقدامه في كل مكان يزوره، ذلك أن الموقع الذي يمر به يفتح سجلاً خاصاً به يسجل عنوان الموقع الذي جاء منه، نوع الحاسوب والمتصفح الذي يستخدمه، وعنوان رقم "ip "الدائم والمتغير للحاسوب الذي يتصل منه، ويمكن تحت ظروف

---

(1) www.WhatIsMyIPAddress.com

وهو موقع مخصص للتعرف على بروتوكول الـ IP.

(٢) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٤٦ – ١٤٧.

معينـة، أن يـتمكن الموقـع مـن الحصـول علـى عنـوان البريـد الإلكترونـي، والاسـم الحقيقي، ويقول بعض خبراء الحاسوب، أنـه يمكن باستخدام برمجيات "جافا"، أو "جافا سكريبت"، أو "أكيث أكس" معرفة عنوان البريد الإلكتروني للمتصل وبعض المعلومات الأخرى عنه، رغم عدم قانونية هذا العمل إلا إذا كان بتصريح خاص من النيابة أو القاضي المختص، وذلك للبحث عن الأدلة في نطاق عمل الضابطة القضـائية لرجـال القـانون، وأسـهل طريقـة لمعرفـة مـا تسـجله المواقـع التـي يزورهـا مستخدم الإنترنت هو التوجه لموقع (www.Consumer.net/analyze)، والانتظار قليلاً، قبل أن يكتشف هذا الموقع المعلومات ويعرضها أمام عضو الضابطة على الشاشة، إلا أنه قد توجد على شبكة الإنترنت عدة مواقع سرية تحفظ سرية تحركات المستخدم، ومثال ذلك موقع (www.Ananymizer.Net) حيث يوفر للمستخدم من خلال خدمة إمكانية إخفاء رقم (ip) عن المواقع التي يرغب في زيارتها ويوصلها إليه، دون أن يمكنه من تسجيل أي معلومات حقيقية عنه، حيث سيبدو للموقع الذي يزوره أنه قادم من عنوان آخر، ولكن الاشتراك في الخدمات المذكورة لا يضمن إخفاء هوية المستخدم بشكل كامل أثناء استخدام الإنترنت، لأن الجهة الوسيطة التي تقدم هذه الخدمات، تحتفظ بسجل عن كافة تحركات المستخدم، لكن لا تكشفه إلا عند وقوع جريمة إلكترونية مصدرها الكومبيوتر المستخدم كإرسال رسالة لآخرين أو غيرها من التصرفات التي تخالف القوانين[١].

وعنوان الإنترنت الرقمي يمكن الحصول عليه عن طريق مزود خدمة الإنترنت، إذ إن مزود الخدمة يقوم بالحصول على مجموعة كبيرة من العناوين عن طريق الجهات المسؤولة جغرافياً عن إدارة وتخصيص هذه العناوين. فمثلاً الريب

---

(١) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٤٧.

RIPE NCC [١] وهي إحدى الجهات المرخص لها من قبل الآيكان ICANN، تقوم بتخصيص عناوين النفاذ لمنطقة أوربا والشرق الأوسط وبعض دول آسيا وإفريقيا. وسورية تنتمي إلى هذه المنطقة حسب ترتيبات الآيكان، وتدير المؤسسة العامة للاتصالات في سورية حالياً النطاق العلوي السوري، حيث تقوم بتخصيص أسماء النطاقات الداخلية للراغبين في الحصول عليها لقاء رسوم سنوية[٢].

وتجدر الإشارة إلى أن بروتوكول الإنترنت المشار إليه، الذي يحدد هوية الحاسوب، لا يتم منحه بطريقة واحدة على المستوى العالمي. ففي الولايات المتحدة الأمريكية وكندا وبعض الدول المتقدمة، يقوم الشخص باقتناء IP خاص به، ومن ثم يمكن تحديد هويته بسهولة عند ارتكابه جريمة إنترنت. أما في بعض الدول الأخرى – ومنها أغلب الدول العربية – فإن العنوان الرقمي يكون محلاً للتغير بين عدة مشتركين، وبالتالي فإن تحديد هوية المشتبه به تكون أكثر صعوبة. ويمكن القول إنه بمجرد وجود شخص في سورية على الإنترنت، فإنه يملك فوراً هوية رقمية محددة IP، إلاّ أنه إذا حدث وانقطع الإرسال، فإن الشخص إذا عاود الاتصال من جديد، فإن الهوية السابقة قد لا تبقى له، بل لغيره، وقد يظهر بهوية جديدة، أي بـ IP جديد[٣].

كما تجدر الملاحظة بأن الشبكات الداخلية تعد من الأمور الشائعة في مجال الشركات، حيث يحتاج العاملون في هذه الشركات إلى التواصل وتبادل الملفات فيما بينهم. ويمكن استخدام عنوان خارجي واحد لتشغيل عدد من الحواسيب المرتبطة فيما بينها عن طريق شبكة داخلية[٤].

---

(١) وهو اختصاص لـ Reseau IP Europeans Network Coordination Center ومتوفر على الموقع www.ripe.net

(٢) د. محمد طارق الخن، المرجع السابق، ص١٠٢ – ١٠٣.

(٣) د. محمد طارق الخن، المرجع السابق، ص١٠٣ – ١٠٤.

(4)Anthony Reys and others, Cyber Crime Investigations, Bridging The Gaps Between Security Professional Law, Enforcement and Prosecutors. Published by Elsevier Since and Technology, 2007, P . 203.

وفي حال ارتكاب جريمة إنترنت، عن طريق أحد الحواسيب الموصولة إلى شبكة داخلية، فإن على موظف الضابطة العدلية أن يتوصل إلى رقم العنوان الخارجي، ثم يتم تحديد الحاسوب المطلوب عن طريق العنوان الداخلي، ومن ثم يتم معرفة الشخص المقصود(١).

**- تتبع البريد الإلكتروني المزيف:**

يقوم بعض المجرمين بتزييف أو تزوير البريد الإلكتروني، بغية إخفاء هويتهم الحقيقية. وكثيراً ما تخفق هذه المحاولات في إخفاء الهوية؛ لأن الرسائل المزيفة أو المزورة تحتوي على عناوين الإنترنت العائدة للمرسلين. ومن الملاحظ أن معظم المجرمين عبر الإنترنت يستخدمون هذا الأسلوب لإخفاء هويتهم الحقيقية.

ولمعرفة كيفية التلاعب بعناوين الإنترنت، لا بدّ لنا من التعرف على الآلية التي تتم بها عملية إرسال الرسائل الإلكترونية. فالبريد الإلكتروني يشبه البريد العادي في العديد من الجوانب. فعندما يتم إرسال رسالة إلكترونية، يقوم وكيل نقل الرسائل MTA (٢) – وهو يشبه مكتب البريد العادي – بختم هذه الرسالة مع وضع وقت الإرسال، واسم وكيل نقل الرسائل، ومعلومات تقنية أخرى، وتكون هذه المعلومات موجودة في ترويسة الرسالة الإلكترونية، ويتم وضع هذه المعلومات من قبل جميع وكلاء نقل الرسائل التي تمرّ الرسالة الإلكترونية عبرهم، إلى أن تصل إلى الجهة المقصودة.

ومن أجل إخفاء عناوين الإنترنت، يقوم مزيفو البريد الإلكتروني بإدخال عناوين وهمية إلى ترويسة الرسالة الإلكترونية لتضليل المحققين، التي تحوي عادة على عناوين المُخدّمات التي مرّت عبرها الرسالة كما ذكرنا. إلاّ أن الخبير التقني يستطيع

---

(١) د. محمد طارق الخن، المرجع السابق، ص١٠٤.

(٢) وهو اختصار لـ Message Transfer Agents ويقصد به الحاسوب أو المخدم المسؤول عن نقل الرسائل الإلكترونية.

عن طريق التدقيق الجيد اكتشاف عدم التناسق بين العنوان الوهمي وباقي العناوين الصحيحة في ترويسة الرسالة. ناهيك عن أن الرسالة الإلكترونية ستحمل كحد أدنى العنوان الصحيح الذي تمّ من خلاله إرسال الرسالة الإلكترونية[١].

وهناك من يرى[٢] بأهمية توفير الأجهزة التقنية والخبرات الفنية لدى موظفي الضابطة العدلية، حتى يتمكنوا من تتبع الأثر الافتراضي للجاني، وتحديد مكانه وإلقاء القبض عليه.

**جـ-إجراء المعاينة من قبل سلطات مختصة مؤهلة:**

لضمان مشروعية الدليل الإلكتروني الناتج عن إجراء المعاينة، لابد من إجراءها من قبل سلطات مختصة، كما لابد أن تكون هذه السلطات مؤهلة.
أي لابد من السلطة التي تجري المعاينة من أن تكون مختصة نوعياً ومكانياً.

**١- بالنسبة للاختصاص النوعي:**

إن حماية الحرية الشخصية تفرض تحديد الأشخاص المصرح لهم بالإطلاع على هذه المعلومات الحساسة، فيجب أن تكون إحدى الجهات مختصة بالاطلاع على المعلومات، بمعنى لابد من أن تتوافر صفة خاصة فيمن يطلع على هذه المعلومات الحساسة، ويُعد هذا الدليل مجرد وهم إذا لم يتم وضع حواجز تقنية بهدف التأكد من صفة القائم بالاطلاع على المعلومات قبل الاطلاع عليها، فقصر الاطلاع على هذه المعلومات على أشخاص معينين ومختصين هو الشرط الأساسي لقبول الأدلة التي يتم الحصول عليها بطريق مباشر أو غير مباشر من هذه الملفات[٣].

---

(١) د. محمد طارق الخن، المرجع السابق، ص١٠٤ - ١٠٥.
(٢) د. محمد طارق الخن، المرجع السابق، ص١٠٥.
(٣) د. جميل عبد الباقي الصغير، المرجع السابق، ص١٠١ - ١٠٢.

**٢- بالنسبة للاختصاص المكاني:**

يجب أن يكون عضو الضابطة العدلية عند إجراءه المعاينة مختصاً مكانياً في إجراءها وإلا كان الدليل الناتج عن المعاينة غير مشروع.

لكن ذهب القضاء الفرنسي في إحدى القضايا التي حدثت في فرنسا وتحديداً في ١٠ يناير ١٩٩٢ كما ذكرنا سابقاً، حيث جاء في قرار محكمة النقض الفرنسية إن الانتقال غير المادي للمعلومات (Transfert immaterielle d'information) من مكان يقع خارج الحدود الإقليمية لاختصاص عضو الضابطة العدلية إلى دائرة اختصاصه لا يخالف القانون، وبالتالي يمكن الاعتماد عليها كدليل إثبات، ذلك أن المادة (١/١٨) من قانون الإجراءات الفرنسي لا تنطبق إلا في حالة الانتقال المادي لعضو الضابطة العدلية خارج نطاق اختصاصه المكاني – كما يمكن لعضو الضابطة العدلية– حسب هذا القضاء – الاطلاع على الملفات عن بُعد[١].

**ونؤيد موقف اجتهاد القضاء الفرنسي فيما ذهب إليه، فلا ضير من انتقال عضو الضابطة العدلية غير المادي للاطلاع على المعلومات ومعاينتها للحصول على الدليل الإلكتروني حيث يبقى هذا الدليل مشروع ويجوز الاعتماد عليه بالحكم.**

ولايكفي أن يتم إجراء المعاينة من سلطات مختصة نوعياً ومكانياً بل لابد من أن تكون هذه السلطات مؤهلة لإجراء هذه المعاينة، وهذا يتطلب تدريب القائمين على المعاينة على تكنولوجيا الحاسبات حتى يستطيعوا أن يتعاملوا بشكل صحيح مع المعلومات المخزنة في ذاكرة الحاسوب ومخرجاته والاسطوانات الممغنطة التي تسجل عليها المعلومات للحفاظ على سلامة الأدلة المتحصلة من الجرائم الإلكترونية من كل تلف أو محو، فإذا لم تتوافر هذه الخبرة يستحيل على سلطات الضابطة العدلية معرفة كلمة السر أو الشفرات الخاصة بالدخول إلى

---

(١) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٦٩.

البرامج والأوعية المعلوماتية محل الواقعة، مع ما في ذلك من أخطار تهدد العدالة الجزائية وشبكة الاتصالات ذاتها[١].

فيجب أن تقتصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات والشبكات واسترجاع المعلومات، وتلقوا تدريباً كافياً على التعامل مع نوعية الآثار والأدلة التي يمكن أن يحويها مسرح الجرائم الإلكترونية[٢].

وهناك من يرى[٣] أنه ليس بالضرورة أن يكون المحقق خبيراً في مجال الحاسوب، ولكن لا بد من الإلمام ببعض المسائل الأولية التي تمكنه من التفاهم مع خبراء الحاسوب وحسن استغلالهم في كشف الجرائم وجمع الأدلة، كما أنه من الضروري أن يكون المحقق ملماً بالإجراءات الاحتياطية التي ينبغي اتخاذها نحو مسرح الجريمة الإلكترونية، والتدابير اللازمة لتأمين الأدلة.

وأمام التزايد المستمر للجرائم الإلكترونية، لم تَسلم الضابطة العدلية من ضرورات التطور التقني والتكنولوجي. ونتيجةً لهذا التحدي قامت معظم الدول بإحداث أجهزة مختصة بمكافحة هذا النوع من الإجرام المستحدث، وقد حملت هذه الأجهزة تسميات مختلفة، منها شرطة الإنترنت، أو درك الإنترنت، أو متحري الإنترنت، وغير ذلك من التسميات. وتختلف هذه الأجهزة عن الأجهزة المختصة بضبط الجرائم التقليدية من حيث طريقة التكوين، فهي لا تعتمد على التدريبات الجسدية التي يتلقاها عادةً رجال الشرطة، وإنما تعتمد على البناء العلمي

---

(١) د. جميل عبد الباقي الصغير، المرجع السابق، ص١١٧.

(٢) أ. د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، المرجع السابق، ص٤٨٧.

(٣) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٩٣ – ٩٤.

والتكنولوجي لأفرادها، وهي تتولي مهمة التحري عن جرائم العالم الافتراضي لكشف النقاب عنها[١].

وينبغي أن تتضمن عملية التدريب برامج تطبيقية وعملية لكيفية التعامل مع مسرح الجريمة الإلكتروني وطرق جمع الأدلة الإلكترونية وحفظها وكيفية تحليل الدليل الإلكتروني وإعادة بناء الأدلة المهمشة واستخلاص الأدلة الإلكترونية وتحليلها وكيفية إعداد التقارير الجنائية وصياغتها وكيفية تقديمها في قالب إثبات تعتمده أجهزة العدالة الجزائية[٢].

وقد اتجهت بعض الدول مثل كندا سن ١٩٨٠، وفرنسا سنة ١٩٨٣، وانجلترا سنة ١٩٨٧، وفنلندا سنة ١٩٩٠، إلى إعطاء دورات تدريبية لأعضاء الضابطة العدلية عن كيفية تحقيق الجرائم الإلكترونية. كما ينظم البوليس الدولي (Interpol) دورات تدريبية في مجال شبكات الحاسبات الآلية، من أجل تحسين أداء الأعضاء من رجال الشرطة في مجال الكشف عن الجريمة وجمع المعلومات ومتابعة الجناة وإقامة الدليل في الجرائم التي ترتكب في هذا المجال[٣].

كما أن المشرع الجزائري أجاز لضابط الشرطة القضائية أن يستعين بأشخاص مؤهلين لذلك وهذا ما نصت عليه المادة (٤٩) فقرة (١) حيث جاء فيها: "إذا اقتضى الأمر إجراء معاينات لا يمكن تأخيرها فلضابط الشرطة القضائية أن يستعين بأشخاص مؤهلين لذلك"[٤].

---

(١) نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٠٧م، ص٣٠.

(٢) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٢٠٣.

(٣) د. جميل عبد الباقي الصغير، المرجع السابق، ص١١٨.

(٤) ففي الجزائر، وفي نطاق عمل مخابر الشرطة العلمية الجزائرية الذي كان في اتساع وتنوع دائم تماشياً مع ظهور أنماط جديدة للإجرام الإلكتروني، الأمر الذي دفع هذه المخابر إلى الوقوف له بالمرصاد من خلال تكوين كفاءات متخصصة في علم الأدلة الجنائية الحاسوبية، وهذا ماقامت به الأجهزة الأمنية الجزائرية بتكوين إطارات في علوم البيانات الرقمية بجامعات

وهناك من يرى[١] أنه حتى لا يقال أنه من الصعب تدريب كل رجال الشرطة فيوصي بإنشاء ضابطة عدلية متخصصة للبحث عن الجرائم في هذا المجال. وهذا ما ذهب إليه **القانون السوري حيث** نصت المادة (٢٤) من قانون مكافحة الجريمة المعلوماتية على ما يلي:

(أ – تُحدث في وزارة الداخلية ضابطة عدلية مختصّة تكلَّف باستقصاء الجرائم المعلوماتية، وجمع أدلتها الرقمية، والقبض على فاعليها، وإحالتهم على المحاكم الموكول إليها أمر معاقبتهم.

ب – تستعين الضابطة العدلية المشار إليها في الفقرة (أ) من هذه المادة بخبراء، دائمين أو مؤقتين، من وزارة الدفاع، ووزارة العدل، ووزارة الاتصالات والتقانة، لتنفيذ المهام الموكلة إليها. ويقسم هؤلاء الخبراء اليمين القانونية).

وتنفيذاً لهذا النص فقد أصدر وزير الداخلية القرار ٥٦٤/ ق تاريخ ٢٠١٢/٣/٢٢ المتضمن إحداث فرع خاص في إدارة الأمن الجنائي يسمى **(فرع مكافحة جرائم المعلوماتية)** لمكافحة هذه جرائم والتحقيق فيها، وجمع أدلتها الجنائية الرقمية، وضبط مرتكبيها وتقديمهم للقضاء. كما أصدر وزير العدل القرار رقم ٥٤١٣ تاريخ ٢٠١٢/٣/٢٩ المتضمن تسمية قاضي كممثل لوزارة العدل في اللجنة المختصة بالتعاون مع هذا الفرع.

**ونرى بضرورة تأهيل رجال الضابطة العدلية على التعامل مع مسرح الجريمة الإلكتروني، كما له أثر كبير في سهولة الحصول على الدليل الإلكتروني وكذلك في عدم اتلافه. ونقترح بجواز أن يلتمس المشتبه به في المعاينة من القاضي أن يصرح له بتعيين خبير فني متخصص في الانترنت**

---

العالم خاصة البريطانية، وأنشأت فرع الأدلة الجنائية الحاسوبية التابع لجهاز الشرطة العلمية الجزائرية وهذا الفرع الذي يطلق عليه فرع الإلكترونيك والإعلام الآلي يهتم بدراسة نوعية خاصة من الأدلة هي الأدلة العلمية الرقمية. بهلول مليكة، المرجع السابق، ص١٧٦.

(١) د. جميل عبد الباقي الصغير، المرجع السابق، ص١١٩.

**ليكون بصحبة المحقق في حال كان غير مؤهلاً، ذلك حتى يمنع أي تشكيك في صحة الدليل المستمد من المعاينة.**

**د- إبلاغ المشتبه به بإجراء المعاينة:**

يجب على المحكمة أن تعلم المشتبه به بقرار إجراء المعاينة، إذا لم يكن حاضراً كما يجب تمكينه من الحضور أثناء المعاينة، ولو كانت جلسات المحاكمة سرية [١].

**ونحن نرى أن في إبلاغ المشتبه به بإجراء المعاينة أو تمكينه من الحضور فيه ضمانة أكيدة لنتائج المعاينة الواقعة على نظم الحاسوب والإنترنت، لأنه يتيح للمشتبه به فرص مواجهة الدليل المستمد منه، وبالتالي يجعله رقيباً على الشخص القائم بالمعاينة وعلى مشروعية الدليل المستمد منها.**

**وهكذا نستنتج أن من أهم ضمانات مشروعية المعاينة الإلكترونية للحصول على الدليل الإلكتروني هي وقوع جريمة ووجود مشتبه به وإجراء المعاينة من الجهات المختصة والمؤهلة وإبلاغ المتهم بإجراء المعاينة.**

## الفرع الثالث

## التفتيش الإلكتروني

يُعد التفتيش من أهم الأعمال التي يقوم بها رجال التحقيق الجنائي لكونه الفيصل بين نجاح جهود التحقيق الجنائي في العثور على دليل يفيد إثبات وقوع الجريمة أو خيبة أملهم في عدم العثور عليه هذا من ناحية أما من ناحية أخرى فقد ينجح رجال التحقيق في العثور على الدليل المفضي لوقوع الجريمة ولكن يفلت

---

(١) آمال عبد الرّحمن يوسف حسن، المرجع السابق، ص١٤٤.

الجاني من قبضة العدالة بسبب عدم إتباعهم للقواعد والإجراءات الصحيحة الواجب مراعاتها عند القيام بالتفتيش[١].

وتبدو أهمية مشروعية التفتيش للحصول على الدليل الإلكتروني في أن ما يثيره الدليل الإلكتروني من حيث مشروعية الحصول عليه يتركز بشكل أساسي في إجراءات التفتيش للبحث عن هذا الدليل[٢].

ومن أجل دراسة التفتيش الإلكتروني لابد من عرض مفهوم التفتيش الإلكتروني، ومن ثم عرض ضمانات مشروعية التفتيش الإلكتروني للحصول على الدليل الإلكتروني.

## أولاً: مفهوم التفتيش الإلكتروني:

تقتضي دراسة مفهوم التفتيش الإلكتروني من تعريفه، ومن ثم التعرض لمحل التفتيش، وأخيراً آلية تنفيذ التفتيش الإلكتروني.

### أ- تعريف التفتيش:

يُعرف التفتيش بشكل عام بأنه: "إجراء من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة موضوع التحقيق، وما يفيد في كشف الحقيقة، وبالتالي هو ليس من الإجراءات التي تتبع في كشف الجرائم قبل وقوعها"[٣].

كما يُعرف بأنه: "هو: "الاطلاع على محل منحه القانون حماية خاصة، باعتباره مستودع سر صاحبه، ويستوي في ذلك أن يكون المحل مسكناً أو ما هو في حكمه أو أن يكون شخصاً"[٤].

---

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١٨٣.

(٢) أ. طارق محمد الجملي، المرجع السابق، ص٥٩.

(٣) د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، الطبعة السادسة، دار النهضة العربية، القاهرة، مصر، ١٩٩٣م، ص٣٤٣.

(٤) يعود هذا التعريف إلى الدكتور أحمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، القاهرة، مصر، ١٩٥٩م، ص٤٤٩.

ومما يمكن ملاحظته من هذه التعريفات أن التفتيش هو إجراء من إجراءات التحقيق ووسيلة للبحث عن الأدلة، وبالتالي فهو ليس دليل إثبات بحد ذاته[١].

في حين يُعرف تفتيش نظم الحاسوب والإنترنت بأنه:" الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو نظمه أو الإنترنت"[٢].

وبالتالي فإن التفتيش في مدلوله القانوني بالنسبة للجرائم الإلكترونية لا يختلف عن مدلوله السائد في فقه الأصول الجزائية، فهو إجراء من إجراءات التحقيق تقوم به سلطة مختصة، لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات ومخرجات، لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة، أي قد تمت بالفعل وتشكل جناية، أو جنحة، والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى الفاعل[٣].

وأهم خصائص تفتيش نظم الحاسوب والإنترنت التي تميزه عن غيره من إجراءات التحقيق الأخرى، وهي:

١-يحوي التفتيش في مضمونه على قدر من الجبر والإكراه حيث أنه تعرض قانوني لحرية المتهم الشخصية أو لحرمة أسراره الموجودة على جهاز الحاسوب خاصته أو على برامج خاصة به أو على بريده الإلكتروني عبر شبكة الإنترنت.

٢-إن التفتيش يُعد قيداً على حرمة أو حصانة الشخص الذاتية، ويُعد قيداً على حرمة أسراره الشخصية، أي فيه مساس بحق السر.

---

(١) د. أحمد فتحي سرور، الوسيط في الإجراءات الجنائية، المرجع السابق، ص٣٥٩.

(٢) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، الطبعة الأولى، عالم الكتب الحديث، إربد، الأردن، ٢٠٠٤م، ص١٣.

(٣) د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، ١٩٩٧م، ص٧٣.

٣- يمتاز التفتيش بهذه الصورة بأنه وسيلة للبحث عن الأدلة المادية والمعنوية للجريمة وضبطها، وتشير الخاصية الأخيرة إلى أن الهدف من التفتيش هو ضبط الأدلة التي تفيد في كشف الحقيقة(١).

**ب- محل التفتيش:**

إن محل التفتيش بشكل عام يوجب البحث في أماكن لها حرمة خاصة كالمساكن ومكاتب المحامين.. إلخ، وهذا يعني المساس بحقوقهم ولو لفترة قصيرة(٢).

أما محل التفتيش الإلكتروني فهو كل مكونات الحاسوب سواء أكانت مادية أو معنوية، وشبكات الاتصال الخاصة به، بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش وتشمل برامج النظام وبرامج التطبيقات سابقة التجهيز طبقاً لاحتياجات العميل(٣).

وجدير بالذكر أن مثل هذا المحل لا يمكن أن يكون قائماً بذاته، وإنما يشمله مكان أو عقار ما، أو يكون بصحبة مالكه أو حائزه، أي إن الحرز الذي يوجد فيه الحاسوب هو بطبيعته حرز مادي كالمنزل أو شخصه، كما هو الشأن في الحاسوب المحمول سواء أكان شخصياً أو هاتفاً نقال(٤).

لذلك لابد من دراسة مدى قابلية هذه المكونات للتفتيش، بالإضافة لذلك سندرس مدى خضوع المتهم المعلوماتي للتفتيش، وكذلك مدى قابلية التفتيش بالنظر إلى مكان وجود الجهاز المراد تفتيشه.

---

(١) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٣.

(٢) خالد عياد الحلبي، المرجع السابق، ص١٤٩

(٣) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٨٨.

(٤) عبد العزيز خنفوسي، ورقة بحثية بعنوان" مدى حجية أدلة الإثبات الجنائي التقليدية في إثبات جرائم الإرهاب المعلوماتي، كلية الحقوق والعلوم السياسية، جامعة سعيدة. ص١٤٧.

**١- المكونات المادية والمعنوية:**

تتكون نظم الحاسوب من مكونات مادية (Hardware) ومكونات معنوية (Software) [١]. لذا فقد ثار تساؤل حول مدى خضوع مكونات الحاسب المستخدمة للتفتيش وفي هذا الصدد يجب التفريق بين حالتين:

**الحالة الأولى: مدى جواز تفتيش مكونات الحاسوب المادية:**

يتكون جهاز الحاسوب من مكونات مادية، وتعرف بأنها: "وسيلة لإدخال الأوامر، والقدرة على استقبال النتائج من هذا الحاسوب"[٢]، وهذه المكونات هي:

- **وحدات الإدخال (Input Units):** وهذه الوحدات هي: **(الفأرة، مشغل الأقراص الممغنطة، الماسح الضوئي، مشغل الأسطوانات).**

- **وحدات المعالجة المركزية (Central Processing Unit CPU):** وهذه الوحدات هي: (وحدات الذاكرة الرئيسية، وحدة الحساب والمنطق، وحدات التحكم).

- **وحدات الإخراج (Output Units):** ومن أمثلة هذه الوحدات: (الراسمات، الطابعات، الشاشات، مشغل الأقراص، وحدات تركيب الأصوات أو السماعات).

- **وحدات التخزين (Storage Devices):** ومن الأجزاء التي تستخدم لتخزين المعلومات، وتشمل: **(الأقراص الصلبة، الأقراص المرنة، أقراص الليزر).**

- **المودم (Modem).**

- **الكروت أو البطاقات (PCMCIA Cards).**

- **البطاقات الممغنطة،** وبطاقات الائتمان القديمة والمواد البلاستيكية المستعملة في إعداد هذه البطاقات، وكلها قرائن لإثبات الجرائم الإلكترونية[١].

---

(١) د. نزيهة مكاري، المرجع السابق، ص١٢٧.

(٢) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٠٠.

وبعد استعراضنا لمكونات الحاسوب المادية التي يمكن الاستفادة منها في التحقيق من أجل إثبات دليل الإدانة أو البراءة، سنبحث في مدى جواز تفتيش المكونات المادية للحاسوب.

إن التفتيش المتعلق بمكونات الحاسوب، يسهل إجراءه على المكونات المادية[٢]، وتأتي سهولة هذا التفتيش لأنه يقع على أشياء مادية منصوص عليها في أغلب القوانين الإجرائية[٣]، حيث يرى جانب من الفقه[٤] أنه لا مشكلة في تفتيش نظام الحاسوب، متى كان التفتيش ينصب على المكونات المادية، أي على معدات الحاسوب وشاشة العرض ولوحة المفاتيح وغيرها، ففي هذا الفرض تطبق القواعد التقليدية للتفتيش.

والواقع أن تفتيش المكونات المادية للحاسوب بأوعيتها المختلفة بحثاً عن شيء يتصل بجريمة إلكترونية يدخل في نطاق التفتيش طالما تم وفقاً للإجراءات القانونية المقررة، بمعنى أن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجودة فيه، هل هو من الأماكن العامة أم من الأماكن الخاصة. إذ إن صفة المكان لها أهمية خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه، فلا يجوز تفتيشها إلا في الحالات

---

(١) للتوسع في تعريف هذه المكونات انظر: د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٩-٢٠-٢١-٢٢-٢٣.
د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص ١٨-١٩-٢٠-٢١-٢٢.

(٢) خالد عياد الحلبي، المرجع السابق، ص١٥١.

(٣) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٢٨.

(٤) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص ٣٨٤.

التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونياً في التشريعات المختلفة[١].

وبالنسبة للأماكن العامة، فإذا وجد الشخص في هذه الأماكن وهو يحمل مكونات الحاسوب سالفة الذكر أو كان مسيطراً عليها أو حائزاً لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا الصدد[٢].

**الحالة الثانية: مدى جواز تفتيش مكونات الحاسوب المعنوية:**

تشمل المكونات المعنوية للحاسوب، الأنظمة الأساسية كأنظمة التشغيل، والكيانات المنطقية التطبيقية كالبرامج التي تستخدم للقيام بعمل معين، والبيانات المخزنة في الحاسوب بأنواعها [٣]، وكذلك المعلومات المنطقية[٤].

وبما أن التفتيش بالمعنى الفني هو إجراء تحقيقي ووسيلة للإثبات المادي، فهو إجراء يستهدف ضبط أشياء مادية تتعلق بالجريمة أو تفيد في كشف الحقيقة، وهذا ما يتعارض مع الطبيعة غير المادية لبرامج وبيانات الحاسوب، وكذلك الشبكات الإلكترونية، فهي برامج وبيانات إلكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي[٥]. وهذا ما يطرح السؤال حول: **مدى قابلية تفتيش هذه المكونات المعنوية والوسط الافتراضي للحصول على الدليل الإلكتروني؟**

إن الإشكالية التي تطرح في شأن قابلية تفتيش المكونات المعنوية أو الوسط الافتراضي ترجع في الواقع إلى تحديد المقصود بمصطلح (الشيء) الذي يفترض

---

(١) د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب وضمانات المتهم المعلوماتي، المرجع السابق، ص٧٤.

(٢) د. نزيهة مكاري، المرجع السابق، ص١٢٧.

(٣) د. محمد طارق الخن، المرجع السابق، ص١٠٦.

(٤) عبد العزيز خنفوسي، المرجع السابق، ص١٤٧.

(٥) عبد العزيز خنفوسي، المرجع السابق، ص١٤٦ – ١٤٧.

أن يكون محلاً للتفتيش والضبط، فإذا كان التفتيش ينصب على شيء فإن التساؤل يثور حول مدى انطباق لفظ (الشيء) على المكونات المعنوية "الوسط الافتراضي"؟ ولذلك أهمية عملية، فإذا كانت هذه المكونات لا تكتسب صفة الشيء بالمعنى الذي يعبر عنه النص القانوني، لذلك لا يمكن أن تكون محلاً للتفتيش، والمشكلة لا تقتصر على مشروعية التفتيش وإنما أيضاً تمتد لمشروعية ضبط البيانات التي توجد في الوسط الافتراضي، إذ النص القانوني ينصرف إلى تفتيش الأشياء وضبط ما يوجد بها من أشياء، فما المقصود بلفظ الشيء؟ وبكلمة أوضح فهل يُعد الوسط الافتراضي وما به من بيانات شيئاً في تطبيق أحكام التفتيش والضبط؟[١].

ويستشعر الفقه صعوبة هذه المسألة نظراً لغياب الطبيعة المادية للمعلومات في ذاتها مجردة عن دعامتها المادية[٢]، وقد ذهب الفقه في مدى جواز تفتيش المكونات المعنوية إلى ثلاثة اتجاهات:

**- الاتجاه الأول: الاتجاه الرافض:**

ويرى أن المقصود بلفظ الشيء هو ما كان مادياً أي ملموساً، ولذا فإن الوسط الافتراضي والبيانات غير المرئية أو الملموسة لا يمكن اعتبارها شيئاً، ومن ثم سينحسر عنها النص القانوني الذي استعمل مصطلح شيء، ما يجعل تفتيش الوسط الافتراضي وضبط محتوياته مخالفاً للقانون[٣]،لأن طبيعة البيانات المعالجة تتطلب قواعد خاصة تحكمها بدلاً من محاولة تطويع القواعد التقليدية وتوسيع نطاقها، وهذا يتأتّى من خلال إجراء تعديل عليها من شأنه توسيع نطاق الأشياء التي تكون مشمولة بالتفتيش والضبط وتضمينها من الأحكام بما يتلاءم ومتطلبات

---

(١) خالد عياد الحلبي، المرجع السابق، ص٢٤٠.

(٢) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٢٩.

(٣) خالد عياد الحلبي، المرجع السابق، ص٢٤٠ – ٢٤١.

هذه التقنية الجديدة. فالنصوص الخاصة بالتفتيش بمعناه التقليدي لا ينبغي إعمالها بشأنها مباشرة ، باعتبار أن هذه النصوص تمثل قيداً على الحرية الفردية، ومن ثَم يصبح القياس على الأشياء المادية محظوراً لمنافاته الشرعية الإجرائية[١].

كما يذهب هذا الاتجاه إلى أن المعلومات – المبرمجة في جهاز الحاسوب– أو على أسطوانة أو شريط قد يصعب انطباق وصف المحرر عليها، ويضربون مثال على ذلك ليؤيدوا وجهة نظرهم بأن المحرر الذي يحميه تجريم التزوير هو ذلك المحرر الذي يصح الاحتجاج به، وهذا لا يتحقق إلا باستعماله في التعامل، وهذا لا يتحقق بالنسبة للمعلومات المبرمجة قبل طباعتها على أوراق[٢].

ولذلك يقترح هذا الرأي لمواجهة هذا القصور التشريعي أن يتم تعديل النصوص الخاصة بالتفتيش وذلك بأن يضاف إليها ما يجعل التفتيش يشمل البحث في الوسط الافتراضي وضبط المواد المعالجة عن طريق الحاسوب أو بيانات الحاسوب [٣].

وقامت بعض الدول بإجراء تعديل على قوانينها الإجرائية، ففي **الولايات المتحدة الأمريكية** جرى تعديل القاعدة رقم (٣٤) وهي من القواعد الفيدرالية الخاصة بالإجراءات الجزائية عام ١٩٧٠م، حتى تنص على السماح بإمكانية تفتيش أجهزة الكومبيوتر والكشف عن الوسائط الإلكترونية بما في ذلك البريد الإلكتروني والبريد الصوتي والبريد المنقول عن طريق الفاكس[٤]. كما نظم المشرع الأمريكي إجراءات

---

(١) أ.د. موسى مسعود أرحومة، المرجع السابق، ص ٧.

(٢) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٥٣ – ٥٤.

(٣) خالد عياد الحلبي، المرجع السابق، ص٢٤١.

(٤) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٨٠.

تفتيش وضبط المكونات البرمجية للحاسوب، من خلال القوانين الإجرائية الفيدرالية المتعلقة بجرائم الحاسوب المنصوص عليها في القسم 2000 42usc[١].

**وفي بلجيكا**، أصدر المشرع البلجيكي القانون المؤرخ بـ ٢٠٠١/١١/٢٨ المتضمن تعديل قانون التحقيق الجنائي، الذي أضاف المادة /٨٨/ إلى هذا القانون، والتي سمحت لقاضي التحقيق أن يصدر إذن بتفتيش نظم المعلومات.

**- الاتجاه الثاني: الاتجاه المؤيد:**

ويذهب هذا الاتجاه إلى أن التفتيش والضبط لا يقتصران على الأشياء بمفهومها المادي، لأن الغاية من التفتيش هي البحث عن دليل بشأن جريمة وقعت، ولذا فإن إعمال قواعد التفسير المنطقي تجعل من الكيانات المنطقية مما يمكن تفتيشها وضبط ما بها من محتويات[٢].

ووصولاً لذات النتيجة يرى البعض[٣] أن تحديد كلمة شيء أو مادة يجب أن نرجع في شأنه إلى مدلول هذه الكلمة في العلوم الطبيعية، حيث تعني كل ما يشغل حيزاً مادياً في فراغ معين، ولما كانت الكيانات المنطقية والبرامج تشغل حيزاً مادياً في ذاكرة الحاسوب ويمكن قياسها بمقياس معين، وهي أيضاً تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد، فإنها ذات كيان مادي وتتشابه مع التيار الكهربائي الذي اعتبره الفقه والقضاء في فرنسا ومصر وسورية من قبيل الأشياء المادية، ومن ثم فهي تعد أشياء بالمعنى العلمي للكلمة ومن ثم تصلح لأن تكون محلاً للضبط.

وتأييداً لذلك يرى البعض[٤] أن القواعد التقليدية للتفتيش، تطبق على أدلة الجرائم التي يكون محلها برامج الحاسوب كالسرقة أو الإتلاف أو استعمال هذه البرامج كأداة في ارتكاب بعض الجرائم كالتزوير أو التلاعب في البيانات أو الإتلاف الفني للأنظمة المعلوماتية، وإن القواعد التقليدية كافية لمواجهة هذه

---

(١) د. محمد طارق الخن، المرجع السابق، ص١٠٦.

(٢) خالد عياد الحلبي، المرجع السابق، ص٢٤١.

(٣) خالد عياد الحلبي، المرجع السابق، ص٢٤١ - ٢٤٢.

(٤) د. عفيفي كامل عفيفي، المرجع السابق، ص٣٤٤.

الأحوال أياً كانت الوسيلة المستخدمة لارتكاب الجريمة، سواء كانت تقليدية أو غلب عليها الطابع الفني.

إذاً فالمعلومات المبرمجة هي من عداد المحررات مادامت أنها مدونة على أسطوانة أو شريط أو مسجلة بجهاز الحاسوب نفسه، وذلك استناداً إلى أنه يمكن الاطلاع عليها بالوسيلة المناسبة لذلك(١).

وأيد هذا الاتجاه المجلس الأوربي في التوصية رقم ر (٩٥) ١٣ في ١٩٩٥/٩/١١م، حيث نصت على أن تسمح الإجراءات الجزائية لجهات التفتيش بضبط برامج الكومبيوتر والمعلومات الموجودة بالأجهزة وفقاً لذات الشروط الخاصة بإجراءات التفتيش العادية(٢)، وهو ما نصت عليه أيضاً اتفاقية بودابست لسنة ٢٠٠١م، في المادة (١/١٩ – ٣)(٣).

فضلاً عن أن الاتفاقية الأوروبية للجريمة الافتراضية (اتفاقية بودابست) **لعام ٢٠٠١م**، تقضي في المادة (١٩) منها بإلزام الدول الأطراف في هذه الاتفاقية بضرورة تبني التدابير والإجراءات التشريعية التي تخول السلطات المختصة ولوج البيئة المعلوماتية، وذلك من أجل تيسير إثبات هذه الجرائم(٤). وبالتالي فقد أجازت هذه الاتفاقية تفتيش وضبط البيانات المخزنة في الحاسوب بالمادة (١٩) من هذه الاتفاقية(٥).

وبهذا الاتجاه أخذت بعض التشريعات فنصت صراحة على أن إجراءات التفتيش تشمل أنظمة الحاسوب، وهذا ما نُص عليه في قانون إساءة استعمال الحاسوب في تشريع **المملكة المتحدة**، بالقسم الرابع عشر من قانون إساءة

---

(١) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٥٤.

(٢) د. مدحت رمضان، المرجع السابق، ص٨٠.

(٣) خالد عياد الحلبي، المرجع السابق، ص٢٤١.

(٤) أ.د. موسى مسعود أرحومة، المرجع السابق، ص ٧-٨.

(٥) د. محمد طارق الخن، المرجع السابق، ص١٠٦.

استخدام الحاسوب لعام ١٩٩٠م، وذلك بعد الحصول على إذن بالتفتيش من القاضي المختص.

**وفي الأردن**، نصت المادة (٨١) من قانون أصول المحاكمات الجزائية الأردني على أنه لا يجوز دخول المنازل وتفتيشها، إلا إذا كانت هناك أشياء تتعلق بالمجرم، وكلمة أشياء تنطبق على المكونات المادية والمعنوية للحاسوب، وهنا يمكن تطبيق القواعد العامة للتفتيش على الجرائم الإلكترونية(١).

وفي **البحرين**، أورت المادة (٢٢) من قانون جرائم تقنية المعلومات البحريني رقم (٦) لعام ٢٠١٤م، نصاً وهو: "في تطبيق أحكام هذا القانون تشمل معنى كلمة (شيء) أو (أشياء) الواردة في قانون الإجراءات الجنائية عبارة (نظام) و(تقنية المعلومات) أو (أي جزء منه) و(بيانات وسيلة تقنية المعلومات) و(أي من وسائط تخزين بيانات وسيلة تقنية المعلومات الواردة في هذا القانون".

ومن هذا النص نلاحظ أن المشرع البحريني قد وسع من مفهوم الشيء ليشمل جميع المكونات المعنوية.

**وأيضاً في سورية** فقد عدت الفقرة (ب) من المادة (٢٦) من قانون مكافحة الجريمة المعلوماتية البرمجيات الحاسوبية من الأشياء المادية التي يجوز تفتيشها وضبطها، وفق القواعد المنصوص عليها في قانون أصول المحاكمات الجزائية.

ومن الأمثلة الواقعية لتفتيش برامج الحاسوب، أنه بعد تفجير بُرجي مركز التجارة العالمي في الولايات المتحدة الأمريكية في ٢٠٠١/٩/١١م، ولدى تفتيش الحاسوب النقال العائد للمشتبه به "رمزي يوسف" تبيّن – بحسب رأي الـ FBI – بأن هذا الحاسوب كان يحوي الخطط اللازمة للقيام بعمليتي التفجير، كما أدّى هذا التفتيش إلى الكشف عن دور المدعو "زكريا الموسوي" في عملية التفجير الثانية. وقد تمّ فحص وتفتيش أكثر من مئة قرص صلب في هذه التحقيقات.

---

(١) خالد عياد الحلبي، المرجع السابق، ص١٥١.

وفي قضية أخرى، تتلخص وقائعها بأن السيدة "شارون لوباتكا" غادرت منزلها بقصد زيارة صديقتها، إلا أنها تغيبت عن المنزل لعدة أيام، ولدى تفتيش الحاسوب الشخصي العائد لها، وجدت الشرطة مئات الرسائل الإلكترونية بين السيدة "شارون" وشخص يدعى "روبرت غلاس"، وقد تضمنت هذه الرسائل تخيلات عن التعذيب والموت. ولدى قيام الشرطة بالتحقيق مع "غلاس"، اعترف بأنه قتل شارون خطأً أثناء نومه معها، كما قام بإرشاد الشرطة إلى مكان جثتها في شمال كاليفورنيا، حيث وجدت الشرطة أيدي وأرجل شارون مربوطة، ثم تبين أنها ماتت خنقاً[١].

**- الاتجاه الثالث: الاتجاه التوفيقي:**

ويرى ضرورة إهمال الجدال الدائر حول مصطلح الشيء والعبرة عنده بالواقع، فالضبط لا يمكن وقوعه عملياً إلا على أشياء مادية، ولذلك فإن المشكلة ليست مشكلة مصطلح عبر عنه النص القانوني، وإنما هي تتعلق بإمكانية اتخاذ الإجراء، وترتيباً على ذلك فإن تفتيش الوسط الافتراضي يكون صحيحاً إذا أسفر عن وجود بيانات اتخذت فيما بعد شكلاً مادياً، وهذا الاتجاه قد أخذ به قانون الإجراءات الألماني في القسم (٩٤) حيث نص على أن: "الأدلة المضبوطة يجب أن تكون ملموسة"، ولذلك فإن البيانات إذا تمت طباعتها تعد أشياء ملموسة وبالتالي يمكن ضبطها[٢].

وهناك من يرى[٣] إلى جواز ضبط البيانات الإلكترونية بمختلف أشكالها سواء كانت (محسوسة أو غير محسوسة) حيث يعد حلاً يتلاءم مع طبيعة جرائم

---

(١) د. محمد طارق الخن، المرجع السابق، ص١٠٦ – ١٠٧.

(٢) د. هلالي عبد الله أحمد، تفتيش نظم الحاسب وضمانات المتهم المعلوماتي، المرجع السابق، ص٢٠٢. و خالد عياد الحلبي، المرجع السابق، ص٢٤٢.

(٣) د. ميسون خلف حمد الحمداني، المرجع السابق، ص٢٣٦ – ٢٣٧.

الانترنت، إذ أن الدليل الإلكتروني يمكن التعويل عليه لإثبات وقوع الجريمة ويمكن الاعتماد على الأدلة الإلكترونية إذا قُدمت أيضاً على شكل رقمي أو ورقي.

**ونرى أنه يمكن تفتيش المكونات المعنوية أو الوسط الافتراضي وذلك لأن كلمة شيء تشمل الأشياء المادية والمعنوية وذلك حسب التفسير الغائي للنص دون التفسير الحرفي له، وبالتالي فإن تفتيش الوسط الافتراضي يعد صحيحاً وفقاً للقانون كما أن البيانات بذلك الوسط يصح ضبطها.**

**كما نرى بضرورة تدخل قوانين الأصول الجزائية بشكل واضح لأجل تطبيق الإجراءات الخاصة بالوثائق التقليدية وتطبيقها على المعلومات الموجودة في أجهزة الكومبيوتر**(١).

**٢- مدى خضوع المتهم المعلوماتي للتفتيش:**

يقصد بشخص المتهم المعلوماتي كمحل للتفتيش بأنه: "تحسس جسمه وملابسه وفحصه بدقة وإخراج ما يخفيه فيه من محصلات جريمة الإنترنت، وإذا كانت معه أمتعة جاز تفتيشها بحثاً عن أجزاء تتعلق بوحدات معلوماتية محل البحث، سواء أكانت بين يديه أو كانت في سيارته"(٢).

ويجوز تفتيش المتهم المعلوماتي بناء على رضائه، ومثال ذلك كما لو قام أحد مستخدمي الإنترنت بترديد عبارات أمام الجهات المختصة تفيد أن مشترك بالبريد الإلكتروني مع أحد الأشخاص الناشطين في تنظيم إرهابي معين، وأنه يتبادل معهم الرسائل الإلكترونية في كل مايتعلق بنشر أفكار ومبادئ هذا التنظيم

---

(١) وهذا ما دعا إليه المجلس الأوربي في التوصية رقم ر (٩٥) ١٣ في ١١/٩/ ١٩٩٥م التي جاء فيها أنه: "إذا كان القانون يوازي من الناحية العملية بين المعلومات الواردة على أجهزة الكومبيوتر والوثائق التقليدية تعين أن يوضح قانون الإجراءات أن الإجراءات الخاصة بالوثائق تنطبق في شأن المعلومات الموجودة بأجهزة الكومبيوتر". د. مدحت رمضان، المرجع السابق، ص٨١.

(٢) عبد العزيز خنفوسي، المرجع السابق، ص١٤٩.

الإرهابي، فتطلب منه السلطات المختصة أن تقوم بتفتيش جهازه فإن وافق فإن التفتيش والضبط يكون صحيحاً[١].

وإذا كان المتهم المعلوماتي أنثى، فإن غالبية التشريعات اتفقت على وجوب تفتيش الأنثى من قبل أنثى وذلك مراعاة للقيم والعادات[٢].

**وقد أثار الفقه الجنائي سؤالاً مهماً حول: مدى جواز إجبار الأشخاص على الإدلاء ببيانات مخزنة في الحاسوب الآلي وتشكل جريمة أو مدى إمكانية الحصول منهم على شفرات الدخول لهذه المعلومات المجرمة متى كان يعلموا بها؟**

ذكرنا فيما سبق من هذا البحث أن تشفير البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال عن بُعد قد يشكل عقبة كبيرة أمام إثبات الجريمة والبحث عن الأدلة، فقد يقوم المرسل أو المرسل إليه بتشفير المعلومات على شبكة الحاسبات الآلية بهدف منع الغير من الاطلاع عليها أو استنساخها كما في حالة نقل المعلومات المتعلقة بغسيل الأموال أو تهريب المخدرات أو جرائم الإرهاب[٣].

ففي حال كانت المعلومات التي تشكل جريمة توجد مخزنة في ذاكرة الحاسوب الآلي أو على أحد الأقراص الصلبة أو المرنة، فإن التساؤل الذي يثور هو: **ما مدى إمكانية الحصول من الأشخاص على شيفرات الدخول إلى هذه المعلومات إذا كانوا يعلموا بها؟ أو بالأحرى هل يمكن إكراههم على الإفصاح عن كلمة السر وما في حكمها من أجل تسهيل الولوج إلى البيئة المعلوماتية؟**

في الحقيقة لابد من التمييز بين المتهم المعلوماتي والشاهد المعلوماتي، كمايلي:

---

(١) عبد العزيز خنفوسي، المرجع السابق، ص١٤٩.

(٢) معمر علي إبراهيم محمد، المرجع السابق، ص١٤٩.

(٣) د. جميل عبد الباقي الصغير، المرجع السابق، ص١١٥.

– **بالنسبة للمتهم المعلوماتي:** هنا تباينت الآراء بصدد هذه المسألة، فهناك رأي في الفقه[١] يرى أنه لا يجوز قانوناً إجبار المتهم على طباعة ملفات بيانات مخزنة داخل نظام المعالجة الآلية للمعلومات، أو إلزامه بالكشف عن الشفرات أو كلمات السر الخاصة بالدخول إلى هذه المعلومات، أو إجباره على تقديم الأمر اللازم لوقف الفيروس أو القنبلة المنطقية، ذلك أن القاعدة الأساسية أنه لا يجوز إلزام الشخص باتهام نفسه، سواء عن طريق الشهادة، أو عن طريق تقديم عناصر الإثبات، كما أنه من حق المتهم الامتناع عن الإجابة أو الاعتصام بالصمت دون أن يؤخذ ذلك على أنه إقرار بصحة الاتهام والتسليم بأدلته[٢].

ونتيجة لذلك فالمتهم له الحرية في عدم الكلام وعدم الإجابة على الأسئلة الموجهة إليه، وهو غير ملزم بالكلام[٣].

وهناك من يرى [٤] أن هذه الضمانة كما هي مقررة للمتهم في الجريمة التقليدية، لا يمنع من الأخذ بها في الجريمة الإلكترونية، ويجب مراعاتها بغرض الحصول على الدليل الإلكتروني.

---

(1) DARAGON (E); Droit de la preuve, Thèse, Grenoble,France, 1996, N 422, p 242.

د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، الطبعة الأولى، مكتبة الآلات الحديثة، أسيوط، مصر، ١٩٩٤م، ص٨٢. د. جميل عبد الباقي الصغير، المرجع السابق، ص١٠٤ – ١٠٥. وسهى إبراهيم داود عريقات، المرجع السابق، ص٢٢.

(٢) من حقوق المتهم أثناء إستجوابه، حق المتهم في الصمت، وهو مبدأ جوهري يفرض نفسه على جميع إجراءات الدعوى الجزائية، وهو النظر إلى المتهم على أنه بريء حتى يثبت العكس بحكم قضائي بات. د. محمد سامي النبراوي، استجواب المتهم، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، ١٩٦٨م، ص ١٤٩.

(٣) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٤١٢.

(٤) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٤١٤.

إلا أنه إذا كان الراجح أنه لا يجوز إجبار الشخص على الإدلاء بأقوال لها دلالة الشهادة ضد نفسه، إلا أنه يجوز إجباره على تسليم مفتاح خزينة مثلاً، يضاف إلى ذلك أن هناك وسائل للضغط يمكن استعمالها في الواقع العملي ضد المتهم، فرفض التعاون مع سلطات الحكم قد يلعب دوراً في تكوين عقيدة القاضي ضده، كما أن هذا الرفض قد يدفع سلطات التحقيق إلى توقيفه احتياطياً بحجة عدم التأثير على سير التحقيق أو كشف الأدلة، وذلك بشرط أن تكون الجريمة موضوع المحاكمة مما يجيز فيها المشرع التوقيف الاحتياطي، كذلك قد توحي سلطات التحقيق للمتهم بأن عدم تعاونه الإيجابي معهم أثناء التفتيش قد يؤدي إلى عدم ضبط النظام المعلوماتي في مجموعه(١).

بينما يذهب رأي آخر إلى القول بأنه، وإن كان لا يجوز إجبار الشخص على الإدلاء بأقواله ضد نفسه ، بيد أن ذلك لا ينبغي أن يكون حائلاً دون إجباره على تقديم معلومات يقتضيها ولوج النظام المعلوماتي للسلطات المختصة ، متى كانت هذه المعلومات بحوزته ، قياساً على إجبار الشخص على تسليم مفتاح الخزنة الذي بحوزته(٢).

ولكن هذا الرأي الأخير أياً كانت المبررات التي يقوم عليها، لا يمكن القبول به، فقياس المعلومة التي بحوزة المتهم على مفتاح الخزنة وما في حكمه قياس غير صحيح. ذلك أن المعلومة (المتمثلة في كلمة السّرّ وما في حكمها) هي أمر معنوي بخلاف المفتاح الذي هو شيء مادي محسوس قابل للتسليم. هذا من ناحية، ومن ناحية أخرى فإن هذا الرأي الأخير لا يتفق مع الأصول المستقرة في الإثبات الجزائي، ويتنافى مع مقتضيات حق الدفاع أمام القضاء الجزائي (٣).

---

(١) د. جميل عبد الباقي الصغير، المرجع السابق، ص١٠٥.

(٢)عطية عثمان محمد بوحويش، المرجع السابق، ص١٠٠ . ١٠١ .

(٣) أ.د. موسى مسعود أرحومة، المرجع السابق، ص ٨.

ومن ناحية ثالثة، وحتى على فرض التسليم بجواز إكراه المتهم أو المشتبه به على تقديم مفاتيح الشفرة التي تمكّن من ولوج النظام المعلوماتي، فإن الأمر تكتنفه صعوبات عملية لا يمكن التغلب عليها، لعل أبرزها أن المتهم يستطيع التذرع بنسيان المعلومة أو عدم إمكان تذكرها أو ما شابه ذلك[١].

ونحن نرى أن الرأي الأول أدعى إلى القبول، وقد أيدته أغلبية التشريعات حيث أعطى التشريع في بولندا المتهم بارتكاب الجرائم الحق في عدم إفشاء كلمات السر المستخدمة أو حتى الأكواد الخاصة بالبرنامج[٢] ، كما أن القانون الياباني يحظر على الأجهزة المختصة إكراه مالك الحاسوب على الإفصاح عن كلمة المرور أو السر Password [٣].

**ونرى بإنه لا يجوز قانوناً إجبار المتهم على طباعة ملفات بيانات مخزنة داخل نظام المعالجة الآلية للمعلومات، أو إلزامه بالكشف عن الشفرات أو كلمات السر الخاصة بالدخول إلى هذه المعلومات، ذلك أن القاعدة الأساسية أنه لا يجوز إلزام الشخص باتهام نفسه، سواء عن طريق الشهادة، أو عن طريق تقديم عناصر الإثبات، ومن حق المتهم الامتناع عن الإجابة أو الاعتصام بالصمت دون أن يؤخذ ذلك على أنه إقرار بصحة الاتهام والتسليم بأدلته، إلا أنه يجوز إجباره على تسليم مفتاح الخزنة التي يوجد فيها النظام المعلوماتي.**

**- بالنسبة للشاهد المعلوماتي:**

**قد أثار الفقه الجزائي سؤالاً مهماً حول: ما مدى جواز إجبار الشاهد المعلوماتي بالإدلاء ببيانات مخزنة في الحاسوب وتشكل جريمة أو مدى إمكانية الحصول من الشاهد المعلوماتي على شفرات الدخول لهذه المعلومات المجرمة متى كان يعلم بها؟**

---

(١) أ.د. موسى مسعود أرحومة، المرجع السابق، ص ٩.

(٢) معمر علي إبراهيم محمد، المرجع السابق، ص ٦٩.

(٣) أ. د. موسى مسعود أرحومة، المرجع السابق، ص ٨.

تثور مسألة الاستعانة ببعض الأشخاص المضطلعين بحكم وظيفتهم على أسرار استخدام الحاسوب لتزويد المحقق بكلمة السر الخاصة بالجهاز، وذلك بصفتهم شهود إثبات[١]، فقد تكون البيانات موجودة على ذات الأجهزة ولكنها مشفرة ولا يعرف فك الشفرة سوى شخص أو أكثر من العاملين فيثور التساؤل عن مدى مشروعية إجباره على فك الشفرة[٢].

اختلف الفقه في ذلك، وكان هناك اتجاهين:

**الاتجاه الأول:** يرى أن الشاهد ليس ملزماً بإفشاء أسرار مهنته، فالشهادة بصفة عامة وظيفة اختيارية من حيث مضمونها، فلا يُلزم الشاهد بالإدلاء ببيانات معينة هو لا يرغب في الإدلاء بها[٣]، وإذا كانت الشهادة تنصب على ما رآه الشاهد بإحدى حواسه فإنه من الصعب أن نطلب منه أن يقدم مساعدته للكشف عن الدليل أو الوصول إليه، فلا يجوز مثلاً إجبار العامل الفني لأحد الأنظمة المعلوماتية أن يقوم – لحساب البوليس – بطباعة أو تحليل ذاكرة النظام المعلوماتي ليكشف له عن آثار بعض البيانات، فهذا البحث يدخل في اختصاص الخبير القضائي[٤].

**الاتجاه الثاني:** يرى أنصاره أنه يمكن إلزام الشاهد بالإدلاء بالمعلومات المتعلقة بموضوع الجريمة ومن ذلك الكشف عن كلمة المرور، على اعتبار أنه ليس هناك نص قانوني يمنع من ذلك[٥]، وبالتالي يجوز إجبار غير المتهم على تقديم المعلومة التي من شأنها تيسير الدخول إلى المنظومة كمقدم الخدمة مثلاً ، وذلك بحمله على الإفصاح عن كلمة السر التي بحوزته للوصول إلى المصدر أو شبكة

---

(١) أ. طارق محمد الجملي، المرجع السابق، ص٥٨.

(٢) د. مدحت رمضان، المرجع السابق، ص٧١.

(٣) أ. طارق محمد الجملي، المرجع السابق، ص٥٨.

(4) VERGUCHT (P);La répression des délits informatiques dans une perspective international, Thèse, Montpellier 1, 1996, N321, p387, 398 et399.

(٥) أ. طارق محمد الجملي، المرجع السابق، ص٥٨.

الاتصالات ؛ لأن الإكراه الواقع على غير المتهم لا يمس حقوق الدفاع خلافاً للوضع بالنسبة للمتهم[١].

وذهب بعض الفقه العربي[٢] إلى أنه يجب على الشاهد الكشف عن مفاتيح الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة.

كما يرى جانب من الفقه في فرنسا أنه في غياب النص التشريعي يكون الشاهد مكلفاً بالكشف عن كلمات المرور السرية التي يعرفها وشفرات تشغيل البرامج، ماعدا حالات المحافظة على سر المهنة، فإنه يكون في حل من الالتزام بإداء الشهادة[٣].

وفي التشريع الفرنسي وحسب المواد (١٠٩-٦٢) من قانون الإجراءات الجنائية الفرنسي، يمكن إلزام الشاهد المعلوماتي- حسب القواعد العامة- بالإفصاح عن كلمات السر التي يعلمها، ويعاقب جزائياً متى رفض إعطاء هذه الكلمات – مباشرة التزامه بالإعلام- في مرحلة التحقيق الابتدائي والمحاكمة[٤].

وفي **اليونان** كذلك يمكن الحصول من مشغل نظام الحاسوب على كلمة المرور السرية للولوج في النظام المعلوماتي كما يمكن الحصول منه على بعض الإيضاحات الخاصة بنظامه الأمني، لكن ليس على الشاهد أي التزامات بالنسبة لطباعة ملفات بيانات مخزنة في ذاكرة الحاسوب، وذلك لأنه يجب أن يشهد على

---

(١) أ.د. موسى مسعود أرحومة، المرجع السابق، ص ٩.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص٣٤٦.

(٣) معمر علي إبراهيم محمد، المرجع السابق، ص١٥٣-١٥٤.

(٤) ومما لاشك فيه أن الدخول إلى النظام المعلوماتي في هذه الحالة لا يمثل جريمة لأنه يتم بناءً على إذن قضائي. د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٥٠.

معلومات تمت حيازتها بالفعل وليس الكشف عن معلومات جديدة، وذلك حسب المادة (١/٢٢٣) من قانون الإجراءات الجنائية اليوناني[١].

وأخذ بهذا الاتجاه أيضاً بعض الدول كالسويد وفنلندا والنرويج حيث تنص تشريعاتها على أنه يقع على عاتق الشهود واجب بأن ينعشوا الذاكرة بفحص الأماكن والمستندات التي توجد تحت سيطرتهم إذا لم يترتب على ذلك أضرار خطيرة.

وفي قانون بعض الدول القانون الانجلوسكسونية فإن الالتزام بالتعاون يتسع ليس فقط لمجرد إصدار الأمر بإحضار الشهود، أو لإحضار بعض المستندات، ولكن إلزام الغير بتقديم المساعدة للسلطة القضائية عن طريق تقديم الأدلة أو المساعدة في الوصول إليها. فالقانون الانكليزي الصادر في عام ١٩٨٤ م، بشأن البوليس والأدلة الجنائية يعطي للمحققين أن يطلبوا من الغير أن يمكنوهم من الدخول إلى المعلومات المخزنة في الحاسوب أو الاطلاع عليها أو قراءتها[٢].

وتجيز المادة (I - 125) من قانون الإجراءات الجنائية الهولندي لقاضي التحقيق أن يأمر أي شخص، يفترض فيه أنه على علم بكيفية الدخول إلى المعلومات المخزنة في الحاسبات الآلية، المساهمة مع سلطات التحقيق في الكشف عن الحقيقة، طالما أن هذه المعلومات تم تخزينها أو معالجتها أو نقلها عن طريق نظام المعالجة الآلية للبيانات، أو تمكين قاضي التحقيق من الدخول إلى هذه المعلومات. والأمر هنا يقتصر على المعلومات التي استخدمت في ارتكاب الجريمة فحسب.

---

(١) Vassilaki (Irini); Computer crimes and other crimes against information technology in Greece, R.I.D, 1993, p.371.

مشار إليه لدى: د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٥٠-٣٥١.

(2) VERGUCHT (P) ; op.cit;, p387, 398 et399.

وطبقاً للمادة (k - 125) من نفس القانون إذا كانت مصلحة التحقيق تقتضي فك شفرة البيانات يكون لقاضي التحقيق أن يأمر أي شخص يفترض فيه معرفة تشغيل نظام أمن المعالجة الآلية – أثناء التفتيش – أن يُمَّكنه من الدخول إلى أنظمة المعالجة الآلية أو في جزء منها، أو أن يقوم بفك الشيفرات، ويجب أن يوجه الأمر إلى الشخص الذي يفترض فيه العلم بكيفية فك الشيفرة[١].

كما يتضمن التشريع الأمريكي قانون خاص بتعاون متعهدي خدمات الرسائل في مجال الاتصالات الإلكترونية المسجلة.

وفي الواقع العملي هناك بعض شركات الخدمات المعلوماتية المباشرة (على الخط) مثل شركة كمبيوسرف سبق أن تعاونت مع سلطات التحقيق لوقف البريد الإلكتروني، وفي حالة تحديد هوية المشتركين في الانترنت والذين يقومون بالتحرش الجنسي أو يرتكبون جرائم ضد القصر[٢].

وبالنتيجة فالشاهد أو القائم على تشغيل النظام المعلوماتي يلتزم بالكشف عن الشفرات أو كلمات السر التي يكون على علم بها، ولا يعفيه من هذا الالتزام سوى الاعتصام باحترام السر المهني[٣]، ومع ذلك فليس ثمة جزاء جزائي يوقع على الشاهد إذا رفض تقديم المعلومات المطلوبة إلا إذا وقع ذلك في مرحلتي التحقيق الابتدائي والمحاكمة[٤].

**ونقترح بضرورة تدخل المشرع السوري بوضع نص قانوني يُلزم الشاهد والعاملين على النظم المعلوماتية بالمعاونة الفعالة مع سلطات التحقيق، عن طريق إمدادهم بالشفرات أو كلمات السر اللازمة لتفتيش البيانات اللازمة لأجل الحصول على الدليل الإلكتروني على أن يستثني من ذلك حالة التزامهم بالمحافظة على السر المهني.**

---

(1) VERGUHT (P); op.cit, P 401.
(2) VERGUHT (P); op.cit, N325, P 402 et 403.
(3) VERGUHT (P); op.cit, N320, P397.
(٤) د. جميل عبد الباقي الصغير، المرجع السابق، ص١٠٨.

**٣- مدى قابلية التفتيش بالنظر إلى مكان وجود الجهاز المراد تفتيشه:**

كثيراً ما يقوم مرتكب الجريمة بتخزين معلوماته في حواسيب أو مُخدّمات أخرى؛ بهدف عرقلة التحقيقات [١]. وهنا يثور التساؤل حول إمكانية تفتيش الأنظمة المتصلة بالنظام المأذون بتفتيشه إذا تواجدت في دوائر اختصاص مختلفة، فهل يمتد تفتيش حاسوب معين إلى الأجهزة المرتبطة به؟

في هذه الصورة يمكن التفرقة بين الفرضين التاليين:

**الفرض الأول: أن يكون حاسوب المتهم متصلاً بحاسوب أو مُخدّم موجود في مكان آخر داخل الدولة:**

إن تفتيش الوسط الافتراضي يأخذ حكم المكان الذي يوجد فيه الجهاز، فإذا وجد في مكان ينطبق عليه وصف المسكن وجب الالتزام في تفتيشه بالأحكام الخاصة بتفتيش المساكن[٢].

**لكن أثير تساؤل مهم يتعلق بمدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسوب في منزل المتهم متصل بحاسوب آخر مملوك لشخص آخر غير متهم، فهل يمكن تفتيشه في هذه الحالة؟**

في الحقيقة هنالك اتجاهين في هذا الفرض، اتجاه مؤيد واتجاه معارض.

**- الاتجاه المؤيد:**

يرى **الفقه الألماني** بشأن إمكانية امتداد الحق في التفتيش، أنه في هذه الحالة يمكن أن يمتد التفتيش إلى سجلات البيانات التي تكون في موقع آخر استنادا إلى القسم (١٠٣) من قانون الإجراءات الجزائية الألماني[٣].

---

(١) د. محمد طارق الخن، المرجع السابق، ص١٠٧.

(٢) أ. طارق محمد الجملي، المرجع السابق، ص٢٧. و خالد عياد الحلبي، المرجع السابق، ص٢٤٤.

(٣) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٨١.

ويسمح المجلس الأوربي في التوصية رقم ر (٩٥) ١٣ في ١١/٩/ ١٩٩٥م أثناء عملية تنفيذ التفتيش للجهات القائمة بالتنفيذ، ومع احترام الضمانات المقررة بمد التفتيش إلى أنظمة الحاسوب الأخرى، في دائرة اختصاصهم، والتي تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات لكن بشرط أن يكون هذا الإجراء ضرورياً[١].

كما تسمح الاتفاقية الأوروبية لجرائم الإنترنت لعام ٢٠٠١ م، للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز الحاسوب المعين إلى غيره من الأجهزة المرتبطة به في حال الاستعجال إذا كان يتواجد به معلومات يتم الدخول إليها في هذا الجهاز من خلال محل التفتيش فتنص الفقرة الثانية من المادة (١٩) من القسم الرابع على أنه:

"من حق السلطة القائمة بتفتيش الحاسوب المتواجد في دائرة اختصاصها أن تقوم في حال الاستعجال بمد نطاق التفتيش إلى أي جهاز آخر إذا كانت المعلومات المخزنة يتم الدخول إليها من الكومبيوتر الأصلي محل التفتيش"[٢].

ولقد حسمت بعض القوانين هذه المسألة بإجازة التفتيش في هذه الحالة، حيث وجدت بعض التشريعات المقارنة حلاً لهذه المشكلة كما في **الولايات المتحدة الأمريكية** عندما أجازت التوجيهات الداخلية الخاصة بإجراءات التفتيش الصادر لمقر شركة معينة إلى فروعها الكائنة في نفس العقار[٣].

وفي **هولندا** نص مشروع قانون جريمة الحاسوب الهولندي الذي نص في المادة (١٢٥) (J) على أن: ( تفتيش المسكن يمكن أن يمتد إلى تفتيش نظام

---

(١) د. مدحت رمضان، المرجع السابق، ص٨٠ – ٨١.

(2) VERBIEST(THIBAULT); cyber consommateur, Litec, Paris, 2002, p.127.

(3) د. محمد طارق الخن، المرجع السابق، ص١٠٧.

آلي موجود في مكان آخر بغية التوصل إلى بيانات يمكن أن تفيد بشكل معقول في كشف الحقيقة، وإذا ما وجدت هذه البيانات، يجب تسجيلها)[١].

كما أن قانون تحقيق الجنايات البلجيكي الصادر في ٢٣ نوفمبر ٢٠٠٠م، أجاز امتداد التفتيش إلى نظام معلوماتي آخر غير مكان البحث الأصلي، ولكن ليس بصورة مطلقة وإنما بقيود معينة، يمكن إجمالها في أن تكون ثمة ضرورة لكشف الحقيقة فيما يخص الجريمة موضوع البحث أو أن تكون الأدلة معرضة لمخاطر معينة كالإتلاف أو التدمير وما شابه [٢].

وأيضاً المادة (١٧) فقرة (أ) من القانون الفرنسي رقم ٢٣٩ لسنة ٢٠٠٣ بشأن الأمن الداخلي الصادر في ١٨ آذار ٢٠٠٣ اعترفت بأنه يمكن لرجال الضابطة العدلية أن يدخلوا من الجهاز الرئيسي على البيانات التي تهم عمليات البحث والتحري، فنصت المادة (١٧) منه على أنه: "يجوز لرجال الضابطة العدلية من درجة ضباط وغيرهم من رجال الضابطة العدلية أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم التفتيش على البيانات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر مادامت هذه البيانات متصلة في شبكة واحدة مع النظام الرئيسي أو يتم الدخول إليها أو تكون متاحة ابتداءاً من النظام الرئيسي"[٣].

كما أن المشرع الأردني قد أعطى لموظفي الضابطة العدلية الدخول إلى أي مكان تشير الدلائل في استخدامه لارتكاب أي من الجرائم الإلكترونية، أي اعترف

---

(1) Kaspersen (W.K.Henril):"computer crime and other crimes against information Technology in the Netherlands"R.I.D.p1993, p.479-498.

مشار إليه لدى: د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٤٣.

(٢) أ.د. موسى مسعود أرحومة، المرجع السابق، ص ١٠.

(3) Loi 18mars 2003pour la sécurité intérieure article 17/2 www.legifrance Gour.fr/w.Aspaid/un texte De gorf? Numjo 2/6/ 2003.

بامتداد التفتيش لحاسوب أو نظام معلوماتي لغير المتهم متى وجدت دلائل في استخدامها لارتكاب جرائم إلكترونية[١].

كما أعطى المشرع البحريني بموجب المواد (١٦ – ١٥) من قانون جرائم تقنية المعلومات البحريني رقم (٦) لعام ٢٠١٤م، للنيابة حق الدخول إلى حواسيب كل من له علاقة بالجريمة حتى لو كان موجوداً في بلد أجنبي، وبغض النظر عن جنسيته.

أيضاً التشريع السوري نص في الفقرة (ج) من المادة (٢٦) من قانون مكافحة الجريمة المعلوماتية السوري على جواز تفتيش الأجهزة والبرمجيات الحاسوبية المتصلة بأجهزة المشتبه به.

**- الاتجاه المعارض:**

على العكس من ذلك فإن هناك من يرى[٢] أن هذا الحكم لا يمكن تطبيقه لأن هذا النوع من التفتيش ينطوي في الحقيقة على معنى تفتيش غير المتهم، ولذلك فإنه لا يجوز تطبيقه إلا في الأحوال التي يجوز فيها للقائم بالتفتيش بتفتيش غير المتهم أو منزله.

كما أن هناك عدد من التشريعات المقارنة مثل سويسرا وبلجيكا ما قصرت أثر إذن التفتيش على الأجهزة الموجودة في مكان محدد دون امتدادها إلى الأجهزة المرتبطة[٣].

---

(١) حيث نص المشرع الأردني في المادة (١٢ الفقرة أ) من قانون جرائم أنظمة المعلومات الأردني لسنة ٢٠١٠م، على أنه: "مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكي عليه الشخصية حيث يجوز لموظفي الضابطة العدلية بعد الحصول على إذن من المدعي العام المختص، أو من المحكمة المختصة الدخول إلى أي مكان تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضراً بذلك ويقدمه إلى المدعي العام المختص".

(٢) خالد عياد الحلبي، المرجع السابق، ٢٤٥.

(3) VERBIEST(THIBAULT); op.cit, p.127.

لكن يشترط لإعمال هذا القيد (أي لا يجوز تفتيش غير المتهم) أن يكون الدخول للنهاية الطرفية الخاصة بغير المتهم يحتاج لكلمة مرور خاصة لا يستعملها غيره (شفرة)، إذ بدون هذه الشفرة يمكن القول أن النظام المعلوماتي، المراد تفتيشه سيبدو باعتباره جزءاً واحداً وهو ما يبرر تفتيشه اعتباراً لصفة المتهم التي تمتد لتشمل النهاية الطرفية لمنزل غير المتهم(١).

**ونميل إلى تأييد جواز تفتيش حاسوب المتهم المتصل بحاسوب أو مُخدّم موجود في مكان آخر داخل الدولة إذا كان هناك أساس يدعو إلى الاعتقاد بأن البيانات المطلوبة قد تمّ تخزينها في نظام ذاك الحاسوب، لكن بشرط أن يكون الدخول للنهاية الطرفية الخاصة بغير المتهم لا يحتاج لكلمة مرور خاصة لا يستعملها غيره (شفرة)، وأن يكون نظام الحاسوب الآخر ضمن النطاق الإقليمي للدولة وأن يكون ذلك التفتيش ضرورياً لإظهار الحقيقة، ولا بد أن يكون أمر هذا التفتيش مسبب بإيراد الأسباب الذي دعت له.**

**الفرض الثاني: أن يكون حاسوب المتهم متصلاً بحاسوب أو مُخدّم آخر موجود في مكان آخر خارج الدولة:**

من المتصور طبقاً لهذا الفرض أن يقوم مرتكبي الجريمة الإلكترونية بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكات الاتصالات البصرية بهدف عرقلة سلطات الادعاء في جمع الأدلة(٢).

فالبيئة المعلوماتية غالباً ما تكون مؤلفة من شبكات منتشرة في كافة أرجاء المعمورة ومرتبطة ببعضها البعض عن طريق شبكة الانترنيت، بحيث تتيح الفرصة أمام مجرمي المعلوماتية للولوج عن بُعد إلى البيانات الالكترونية المخزونة في أية

---

(١) أ. طارق محمد الجملي، المرجع السابق، ص٦٤.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق،ص٣٨٢.

بقعة من بقاع العالم[١]، وقد تكون البيانات التي تثبت حصول الفعل جزءاً من نظام حاسوب يقع خارج الحدود في دولة أخرى[٢].

وتتعقد المشكلة عندما يتعلق الأمر بمعلومات أو بيانات تم تخزينها في الخارج بواسطة شبكة الاتصال عن بُعد، والقواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه المعلومات بحثاً عن الأدلة وتحقيقها، فمن الصعب إجراء التفتيش للحصول على الأدلة في هذه الحالة في داخل دولة أجنبية، حيث إن هذا الإجراء يتعارض مع سيادة هذه الدولة الأخيرة[٣].

فقد يظهر أحياناً في أثناء التحقيقات أنه من الضروري تفتيش جهاز حاسوب متواجد في الخارج كما لو تعلق الأمر بشركة وفروعها في الخارج حيث ترتبط أجهزة الشركة بعضها ببعض، وأحياناً ترتبط بعض الأجهزة بقاعدة بيانات متواجدة في الخارج[٤].

فمن القواعد المتفق عليها أن نطاق تطبيق قانون أصول المحاكمات الجزائية يرتبط بنطاق تطبيق قانون العقوبات، فكلما كان هذا الأخير واجب التطبيق طبق الأول، ومن القواعد المتفق عليها أيضاً أنه لا تلازم بين تطبيق قانون العقوبات وارتكاب الجريمة على إقليم الدولة، إذ قد ترتكب خارج إقليمها ومع ذلك قانونها واجب التطبيق، كالاختصاص وفقاً لمبدأ العينية والشخصية والعالمية الجزائية، فضلاً عن ذلك فإن الجريمة قد ترتكب في إقليم دولة ما وتمتد أثارها إلى إقليم دولة أخرى، فإذا كانت هذه الدولة مختصة بالتحقيق في هذه الجريمة لأن قانون

---

(١) أ. م. جاسم خريبط خلف، المرجع السابق، ص٩

(٢) خالد عياد الحلبي، المرجع السابق، ص١٥٠.

(٣). د. جميل عبد الباقي الصغير، المرجع السابق، ص١١٥ .

(٤) د. نزيهة مكاري، المرجع السابق، ص١٢٩.

عقوباتها واجب التطبيق، فإن التساؤل يثار حول مدى إمكانية تفتيش تلك الآلة الموجودة خارج الإقليم بواسطة السلطات التابعة لهذه الدولة[١].

إذاً قد ترتكب الجريمة بواسطة منظومة لمجموعة من أجهزة الحاسوب تتوزع في أكثر من دولة، والسؤال الذي يطرح نفسه هنا هو: هل يمكن تفتيش تلك الحواسب للبحث عن الدليل الإلكتروني المتعلق بتلك الجريمة بما في ذلك تلك الأجهزة الموجودة في إقليم دولة أخرى؟

في الواقع هنالك اتجاهين لحل هذه المشكلة:

**- الاتجاه الأول: الاتجاه الرافض لتفتيش الحاسوب أو المُخدّم الموجود في مكان آخر خارج الدولة:**

تبنى هذا الاتجاه المجلس الأوربي حيث جاء في تقرير له أن هذا الاختراق المباشر يعد انتهاكا لسيادة دولة أخرى، مالم توجد اتفاقية دولية في هذا الشأن، ويؤيد ذلك الفقه في ألمانيا حيث يذهب إلى أن السماح باسترجاع البيانات التي تم تخزينها بالخارج يُعد انتهاكا لحقوق السيادة لدولة أخرى وخرقاً للقوانين الثنائية والوطنية المتعلقة بإمكانية التعاون في مجال العدالة القضائية[٢].

ويجب الإشارة إلى أن الوسط الافتراضي للشبكة العنكبوتية لا يرتبط بنطاق إقليم دولة ما، فمكان التفتيش هو المكان الذي يوجد فيه الحاسوب المراد تفتيشه، فإن اختصاص الدولة بالتحقيق في جريمة ما وأن كان يخولها تطبيق قانون إجراءاتها بشأن هذا التحقيق بصرف النظر عن مكان وقوع الجريمة مادامت خاضعة لقانون العقوبات الخاص بها، إلا أن ذلك لا يعني أن تباشر الدولة هذه الإجراءات خارج إقليمها، إذ يتعذر على الدولة مباشرة اختصاصها بالتحقيق خارج إقليمها، لأن ذلك

---

(١) خالد عياد الحلبي، المرجع السابق، ص٢٤٢ – ٢٤٣.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق،ص٣٨٢.

من مظاهر سيادتها فلا يسمح لها بممارسته على إقليم دولة أخرى[١]، ولذا فمن المتعذر قانوناً مباشرة الدولة المختصة بالتحقيق لأي إجراء خارج إقليمها بشأن الجريمة رغم انعقاد اختصاصها بالتحقيق فيها، ولذا تبدو مشكلة الحصول على دليل بشأن بعض الجرائم إذا كان الدليل المراد الحصول عليه يوجد في جهاز موجود في دولة أخرى في إطار الإشكالية المعروضة، إذ لن تتمكن سلطات التحقيق من الحصول عليه، ولذا تبدو اتفاقيات الإنابة القضائية هي السبيل لتحصيل هذا الدليل، بحيث تفوض الدولة الأخرى في جمع هذا الدليل وإرساله لدولة التحقيق[٢].

ولذلك كانت هناك حاجة ملحة لعمل اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات، كما يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة، ويتعين عندئذ أن تسمح السلطة الأخيرة بإجراءات التفتيش والضبط، ويتعين كذلك السماح لهذا السلطة بإجراء تسجيلات للتعاملات الجارية وتحديد مصدرها، ولذلك يتعين تطوير اتفاقيات التعاون الدولي القائمة[٣].

ونصت اتفاقية بودابست الصادرة في ٢٠٠١/١٠/٢٢م، على هذا النظام في المادة (٢٥) بقولها: "أن تتفق الأطراف على أوسع نطاق للتعاون بهدف إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وجمع الأدلة في الشكل الإلكتروني لهذه الجرائم".

---

(١) هناك من يرى في الفقه الألماني أن استرجاع المعلومات والبيانات التي تم تخزينها في الخارج يعتبر انتهاكاً لسيادة الدولة الأخرى. انظر:

Mohrenschl ager (Manfred):computer crimes and other crimes against information technology in GermanyR.I.P, 1993, p.351.

مشار إليه لدى: د. محمد طارق الخن، المرجع السابق، ص١٠٧.

(٢) خالد عياد الحلبي، المرجع السابق، ص٢٤٣ – ٢٤٤.

(٣) د. مدحت رمضان، المرجع السابق، ص٨٢ – ٨٣.

ومن الأمثلة على دور التعاون الدولي ما حدث في ألمانيا، حيث أسفر البحث في إحدى جرائم الغش المعلوماتي عن وجود طرفية حاسوب في ألمانيا متصلة بشبكة اتصالات في سويسرا، حيث كان يتم تخزين بيانات المشروعات فيها، وعندما رغبت سلطات التحقيق الألمانية الحصول على هذه البيانات لم يتحقق لها ذلك إلا من خلال طلب المساعدة المتبادلة [١].

وفي اليابان، قامت مجموعة من المخربين بمهاجمة العديد من المواقع الخاصة في الحكومة اليابانية، واستخدموا في ذلك حواسيب موجودة في الصين والولايات المتحدة الأمريكية. وقد طلبت الشرطة اليابانية المساعدة من بكين وواشنطن من أجل تسليم المعلومات والبيانات المسجلة على هذه الحواسيب في كلتا الدولتين، حتى تتمكن من التوصل إلى هؤلاء المجرمين[٢].

**- الاتجاه الثاني: الاتجاه المؤيد لتفتيش الحاسوب أو المُخدّم الموجود في مكان آخر خارج الدولة:**

يذهب هذا الاتجاه إلى أنه إذا كانت فكرة السيادة الدولية ترتبط بالمفهوم التقليدي للإقليم، فإنه ليس هناك ما يمنع من تطبيق هذا الحكم في شأن تفتيش طرف لنظام معلوماتي من خلال الولوج من نهاية طرفية في دولة أخرى، فذلك لا ينتهك سيادة الدولة، فالنظام المعلوماتي لا يعرف الحدود[٣]، والوحدة التي يتميز بها، هي التي

---

(١) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص٣٨٣.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص٣٨٣.

(٣) يُنظر للنظام المعلوماتي على أنه فضاء افتراضي قد يرتبط بأكثر من جهاز ضمن منظومة واحدة، فيعد كل جهاز متضمناً لنهاية طرفية للنظام المعلوماتي، وللتوضيح نضرب المثال التالي: فإذا كانت هناك منظومة لمجموعة فروع لمصرف واحد مرتبط بعدة أجهزة، فإن كل جهاز بفرع من هذه الفروع سوف يمثل نهاية طرفية للنظام المعلوماتي المتمثل في المنطقة. أ. طارق محمد الجملي، المرجع السابق، ص٦٣.

تعطي للجهة القائمة بالتفتيش سلطة الولوج وتتبع المعلومات ولو امتد نشاطها لطرف نظام معلوماتي في دولة أخرى، ولا يحد من سلطتها هذه – حسب هذا الاتجاه – إلا وجود نظام شفرة للدخول للمعلومات، فذلك يخرج هذا الجزء من نطاق الوحدة المعنوية، وهو ما تفقد معه تلك الجهة صلاحياتها في ذلك الجزء[١].

وفي هذا الاتجاه صدرت عن المجلس الأوروبي توجيهات تجيز تفتيش الحاسوب إلى الشبكة المتصل بها، ولو كانت تلك الشبكة تقع خارج إقليم الدولة، فتنص التوصية رقم (١٣) في ١٩٩٥/٩/١١م، المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات على أنه: "لسلطة التحقيق عند تنفيذ تفتيش المعلومات لضوابط معينة أن تقوم بمد مجال تفتيش حاسوب معين يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة مادامت مرتبطة بشبكة واحدة وأن تضبط البيانات المتواجدة فيها، مادام أنه من الضروري التدخل الفوري للقيام بذلك"[٢].

كما أن المادة (٣٢) من **الاتفاقية الأوربية لجرائم الإنترنت لعام ٢٠٠١م،** فقد سمحت بتفتيش حاسوب موجود في دولة أخرى في حالتين:

الحالة الأولى: إذا تعلق التفتيش ببيانات متاحة للجمهور.

الحالة الثانية: إذا رضي صاحب البيانات بالتفتيش[٣].

كما سمحت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة في القاهرة، بتاريخ ٢٠١٠/١٢/٢١م، في المادة (٢٦) منها على إمكانية تفتيش المعلومات المخزنة، وأكدت على ضرورة تبني مجموعة من الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها، هذا إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية

---

(١) أ. طارق محمد الجملي، المرجع السابق، ص٦٤.

(٢) د. نزيهة مكاري، المرجع السابق، ص١٢٩.

(٣) انظر المادة (٣٢) من الاتفاقية الأوربية.

أخرى أو جزء منها في إقليمها، وكانت هذه المعلومات قابلة للوصول قانوناً أو متوافرة في التقنية الأولى، فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى[١].

هذا وتسمح التشريعات المقارنة بتفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة فتجيز المادة (١٧) الفقرة (٢) من قانون الأمن الداخلي الفرنسي لرجال الضابطة العدلية أن يقوموا بتفتيش الأنظمة المتصلة ولو تواجدت في خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية[٢].

كما أن المادة (١٢٥) من مشروع قانون الحاسوب **في هولندا**، سمحت بتفتيش نظم الحاسوب المرتبطة بحاسوب المتهم، حتى ولو كانت موجودة في دولة أخرى، بشرط أن يكون هذا التدخل مؤقتاً، وأن تكون المعلومات والبيانات لازمة لإظهار الحقيقة[٣].

كما نصت المادة (٢٥/أ) من قانون الحاسوب الهولندي الحالي على الاعتداد بالدليل المتحصل عليه في إقليم دولة أخرى إذا تم ذلك تنفيذاً لاتفاقيات التعاون الأمني والقضائي، وأحياناً تكون تلك الدولة مختصة هي الأخرى بالتحقيق في هذه الجريمة، ولذا فإن لم ترغب في مباشرة التحقيق بشأنها قد تتطوع بتزويد دولة التحقيق بالبيانات التي تم ضبطها وفقاً لما يعرف بنظام تبادل المعلومات أو المساعدات"[٤].

---

(١) عبد العزيز خنفوسي، المرجع السابق، ص١٤٨ – ١٤٩.

(٢) د. نزيهة مكاري، المرجع السابق، ص١٢٩.

(3) Durham (colo):The emerging structures of criminal information law: tracing the contours of a new pardign general report for the A.I.D.P. 1993, p.115.

مشار إليه لدى: د. عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق،ص٣٨٢.

(٤) خالد عياد الحلبي، المرجع السابق، ص٢٤٤.

أيضاً نص المشرع البحريني بموجب المواد (١٦ – ١٥) من قانون جرائم تقنية المعلومات البحريني رقم (٦) لعام ٢٠١٤م، للنيابة حق الدخول إلى حواسيب كل من له علاقة بالجريمة حتى لو كان موجوداً في بلد أجنبي.

**ونحن نرى أنه لاشي يمنع من جواز تفتيش الحاسوب أو المُخدّم الموجود في مكان آخر خارج الدولة فيما إذا لم يكن النظام المعلوماتي محمي بنظام شفرة للدخول للمعلومات، حيث أن النظام المعلوماتي لا يعرف الحدود والوحدة التي يتميز بها، هي التي تعطي للجهة القائمة بالتفتيش سلطة الولوج وتتبع المعلومات ولو امتد نشاطها لطرف نظام معلوماتي في دولة أخرى وذلك لا ينتهك سيادة الدولة، أما في حال وجود نظام شفرة للدخول للمعلومات، فنرى أنه لا يجوز تفتيش هذا النظام المعلوماتي لتلك الدولة، ولذلك نرى أن السبيل لحل تلك المشكلة هو تعزيز التعاون الدولي وذلك من خلال تعزيز دور الإنابة المتبادلة بين الدولة المحققة والدولة التي يراد التفتيش فيها.**

**وقد حسم المشرع السوري** هذا الخلاف بالفقرة (ج) من المادة (٢٦) من قانون مكافحة الجريمة المعلوماتية، التي أجازت تفتيش الأجهزة والبرمجيات الحاسوبية **المتصلة بأجهزة المشتبه فيه،** أيّاً كان مكان وجودها، ضمن حدود الواقعة المسندة إلى المشتبه فيه. أي سواء أكانت هذه الأجهزة موجودة داخل سورية أم خارجها، بشرط أن يكون التفتيش في حدود ضرورات كشف الواقعة الجرمية.

**ونجد أن المشرع السوري قد أصاب في هذا التوجه عندما ربط إجازة تفتيش الأجهزة والبرمجيات الحاسوبية المتصلة بأجهزة المشتبه فيه، أيّاً كان مكان وجودها، سواء أكانت هذه الأجهزة موجودة داخل سورية أم خارجها، بحدود ضرورات كشف الواقعة الجرمية ولم يتركها دون أي قيد، لكن موقف المشرع السوري هذا برأينا هو صحيح فيما إذا كان النظام المعلوماتي غير محمي بنظام شفرة، أما في حالة كون هذا النظام محمي بنظام شفرة فلا يجوز تفتيشه لأن ذلك ينتهك سيادة الدولة الأخرى، ونقترح عليه بعقد اتفاقيات الإنابة المتبادلة مع الدولة المراد التفتيش فيها.**

**جـ-آلية تنفيذ التفتيش الإلكتروني:**

إن المشرع السوري في قانون أصول المحاكمات الجزائية السوري لم يتحدث أو ينص على إجراءات تفتيش الحاسوب وغيرها من الأجهزة التقنية والنظام المعلوماتي لأنه صدر عام ١٩٥٠ أي قبل اكتشاف الإنترنت.

وبشكل عام يجب على أعضاء الضابطة العدلية في الأحوال التي يجيز لها القانون إجراء التفتيش أو سلطات التحقيق أن يراعوا الإجراءات الآتية عند قيامهم بتفتيش نظم الحاسبات الآلية:

-تأمين حماية مسرح الجريمة، وهذا يتضمن القوة الكهربائية، وأجهزة خدمة شبكة الإنترنت، وحلقات الاتصالات الإلكترونية الهاتفية.

-على القائم بالتفتيش أن يحتاط إلى أن المشتبه به قد يتوافر لديه قدرة على الدخول عن بُعد إلى النظام من خلال جهاز الاتصال الوسيط (LAN-bassed) أو (PC-based) أو الإنترنت[١].

- أن يتم التفتيش بأسلوب آلي إلكتروني من قبل الأجهزة القائمة بالتفتيش وبصورة سريعة، وذلك مع مراعاة إبعاد المشتبه فيهم والعاملين على أجهزة الحاسوب عن المكان[٢].
- أن يتم عمل نسخة احتياطية من الأقراص الصلبة أو الأسطوانات المرنة قبل استخدامها في البحث والتحقيق، مع استخدام أمر (Disk comp) للتأكد من دقة النسخ.
- القيام بنزع الجهاز المستهدف (الماكينة CPU) للتأكد من عدم وجود أقراص صلبة إضافية.
- نسخ محتوى الاسطوانات والأقراص وتحليلها للكشف عن:

---

(١) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٥٨.

(٢) خالد عياد الحلبي، المرجع السابق، ص١٥٤.

- الملفات الممسوحة الممكن استعادتها من سلة المهملات، وذلك باستعادتها عن طريق فتح سلة المهملات ثم تحديد وعمل (Select All) (تحديد كلي)، ثم الضغط على قائمة ملف (File) واختيار (Restore) (استرجاع) فتعود الملفات إلى الأماكن التي كانت توجد بها قبل الحذف.

ومع ذلك توجد ملفات لا يمكن العثور عليها في حالتين: الحالة الأولى: إلغاء الملفات بالضغط على مفتاح (Shift+Delete) في نفس الوقت. والحالة الثانية: الضغط على (Empty Recycle Bin) من قائمة (File) وذلك بعد الدخول إلى (Recycle Bin).

- الملفات الخفية باستخدام برنامج (Dos) يتم عن طريق الأمر (DIR/H). وفي حالة استخدام برنامج (WINDOWS 95) يتم الدخول إلى ( Windows Explorer)، ثم يتم اختيار قائمة (View)، ثم (Option)، ثم يتم الدخول إلى (Show all Fills)، ثم يتم الضغط على الأمر (OK).

- إجراء بحث نصي على الكلمات المهمة المتعلقة بالقضية، وذلك بإتباع الخطوات الآتية:

- فتح قائمة (START) ويتم اختيار (FIND) ثم اختيار ( FILES OR FOLDER) فيظهر بعد ذلك صندوق حواري (DIALOG BOX)، فنختار (Advanced).

- وأمام التعبير (CONTAINING TEXT) نكتب الكلمة المطلوب البحث عنها، ثم نضغط على الأمر (Find Now)، فتظهر في أسفل الشاشة الملفات التي تتضمن الكلمات المطلوب البحث عنها.

- تحديد كافة المحتويات القرص الصلب من خلال برنامج الـDOS باستخدام الأمر (DIR/S/P).

وفي حالة استخدام برنامج الـ Windows يتم الدخول إلى برنامج ( Windows explorer)، فتظهر شاشة نشاهد في بدايتها في أعلى اليسار لفظ

(Desktop) وتظهر أسفلها كل محتويات الكومبيوتر من الأماكن التخزينية لكل الأقراص الصلبة وقرص الليزر (CD. Rom).

- يتم إجراء فحص البرامج وجرد البرامج التطبيقية، وعلى وجه الخصوص البرامج الحسابية التي من المحتمل استخدامها في عملية اختلاس.
- حفظ المعدات المحرزة وتجنب درجات الحرارة العالية أو الأتربة أو أي مجال مغناطيسي(١).

ويلاحظ أن أغلب التشريعات لم تحدد مدة معينة لتنفيذ إجراء التفتيش، بينما نلاحظ أن المشرع الإنكليزي حدده خلال شهر واحد من تاريخ إصدار الإذن(٢).

وهناك من يرى(٣) أن تنفيذ إجراء التفتيش في نطاق الحاسوب والإنترنت ربما يحتاج إلى مدة أطول من المدة التي يحتاجها التفتيش التقليدي، بسبب الاتصال عن بُعد أو حتى من خارج البلاد فيحتاج الأمر إلى اتصالات قضائية وتنسيق مع الجهاز القضائي الأجنبي لتفتيش وضبط النظم أو البرامج المجرمة عبر شبكة الإنترنت مثلاً.

**ونحن نرى بعدم تحديد مدة لتنفيذ التفتيش الواقع على نظم الحاسوب والإنترنت، فمن جهة أولى، هذا النوع من التفتيش يختلف في محله عن التفتيش التقليدي، حيث يقع هذا التفتيش على مكونات الحاسوب المادية والمعنوية ولاسيما إذا ما كان هنالك كم هائل من البيانات التي يتطلب تفتيشها وقت طويل، ومن جهة ثانية، يستلزم هذا التفتيش بعض الإجراءات المعقدة فيما إذا كانت العناصر المكونة للجريمة موجودة في بلد آخر الأمر**

---

(١) د. جميل عبد الباقي الصغير، المرجع السابق، ص١٢١ – ١٢٢.

(٢) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٦٠ .

(٣) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٦٠.

**الذي يقتضي الحصول على إذن من هذه الدولة بالتفتيش أو إعطائها إنابة قضائية وهذا كله يتطلب وقت طويل جداً.**

## ثانياً: ضمانات مشروعية التفتيش الإلكتروني للحصول على الدليل الإلكتروني:

إن إجراء التفتيش سواء في الجرائم العادية أو في الجرائم الإلكترونية، يمس حقوق الناس وحرياتهم، لذلك وجب أن تتم هذه الإجراءات بصورة صحيحة وقانونية[١]، لأن التفتيش ينطوي بكونه إجراء من إجراءات التحقيق الابتدائي على مساس بحرية الأشخاص أو انتهاك لحرمة منازلهم يقوم به القاضي حين تتوافر لديه الأدلة على وقوع الجريمة ونسبتها إلى شخص معين، فهو يمس حق المشتبه به في السرية، وهو من حقوق الحرية الشخصية التي يتعين كفالتها[٢]، وبالتالي يجب مراعاة الضمانات القانونية عند ممارسة التفتيش للحصول على الدليل الإلكتروني صوناً للحريات الفردية من التعسف والانحراف في استخدم السلطة[٣].

وتضمنت معظم التشريعات ضمانات معينة يجب إتباعها عند التعرض للحريات الشخصية بإجراء من الإجراءات الماسة بالحرية كالتفتيش وسندرس هذه الضمانات على النحو التالي:

### أ- وقوع جريمة معينة:

يجب أن يكون هناك جريمة وقعت بالفعل، حيث أنه من القواعد الإجرائية المهمة، أن التحقيق الابتدائي لا يباشر فيه إلا بعد وقوع جريمة عادية أو إلكترونية[٤]، أما الجرائم التي يمكن أن تقع مستقبلاً ولو قامت الدلائل الجدية على أنها ستقع

---

(١) خالد عياد الحلبي، المرجع السابق، ص١٤٨.

(٢) د. بارعة القدسي، المرجع السابق، ص١٨٥.

(٣) د. نزيهة مكاري، المرجع السابق، ص١٣٣.

(٤) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٦٢.

بالفعل، فلا تخول التفتيش، ويشترط في موضوع الجريمة أن تكون من نوع الجناية أو الجنحة دون المخالفات التي لا يجوز التفتيش فيها نظراً لعدم خطورتها فلا تبرر انتهاك حرمة مساكن الناس[١]. والعبرة بوصف التهمة هي بما يجري التحقيق بشأنه وليس بالنهاية[٢].

**ونرى أن هذه الضمانة تسهم في عدم خرق حرمة المساكن والحريات الخاصة بشكل عشوائي فيما لو تم هذا التفتيش بمجرد الإبلاغ بأن هنالك جريمة سوف تقع.**

وبالتالي يشترط لصحة التفتيش كإجراء من إجراءات التحقيق أن يهدف إلى جمع أدلة حول جريمة قد وقعت بالفعل، ولذا فإنه فيما يتعلق بصحة التفتيش الوسط الافتراضي أو الحاسوب يشترط أن يكون الفعل المراد الحصول على دليل بشأنه يشكل جريمة، فإذا كان التفتيش يتعلق بجرائم الحاسوب بالمفهوم الضيق، فإنه قد لا يوجد نص في قانون دولة ما يؤكد على تجريم هذا النمط من السلوك، وهو ما يجعل التفتيش غير مشروع لتخلف أحد شروطه لانتفاء صفة الجريمة عن الفعل وفقاً لمبدأ الشرعية الجزائية الموضوعية، وهنالك اتجاه يقدم حلاً لهذه الإشكالية مستندين في ذلك إلى أن الدليل الإلكتروني لا يقتصر مجال العمل به كدليل إثبات على جرائم الحاسوب فهو يصلح لإثبات كافة الجرائم التي ترتكب بواسطة الحاسوب والانترنت ويرى أنه إن خلا تشريع دولة ما من النص على

---

(١) د. بارعة القدسي، المرجع السابق، ص١٨٧. وقد ساير المشرع السوري ذلك في قانون أصول المحاكمات الجزائية السوري وكذلك المصري والقطري فلم يجيزوا تفتيش المنازل إلا في الجنايات والجنح أما قانون الإجراءات الجنائية الإيطالي والعراقي إجازوا إجرء التفتيش بالنسبة لجميع الجرائم سواء أكانت جنايات أو جنح أو مخالفات وهو محل نظر برأينا لأن جرائم المخالفات من الجرائم البسيطة وهي غير جسيمة لتبرر إجازة التفتيش فيها الذي هو من الإجراءات الخطيرة الماسة بحرية الأشخاص وحرمة منازلهم والذي لا يتناسب مع بساطة تلك الجرائم.

(٢) د. أحمد فتحي سرور، الوسيط في الإجراءات الجنائية، المرجع السابق، ص٣٥٩.

تجريم أنماط السلوك التي تمس بنظام المعلومات، فإن ذلك لا يمنع من قيام وصف الجريمة للفعل المراد جمع الدليل بشأنه في حالات كثيرة كاستعمال الحاسوب في التزوير أو استعمال شبكة الانترنت في إرسال ذم وقدح وتشهير أو تهديد، إذ أن وصف الجريمة يثبت لهذه الأفعال وفقاً للتكييف التقليدي المقرر وفق قانون العقوبات فالحاسوب في هذه الحالة وسيلة لارتكاب الجريمة ولا يغير من وصفها كجريمة تقليدية إن جاز التعبير(١).

ومن أجل ضمان حفظ أسرار المدعى عليه غير المتعلقة بالجريمة من الاطلاع عليها يجب اتباع القائم بالتفتيش التعليمات التالية:

- على القائم بالتفتيش أن يلتزم واجب الحيطة والحذر أثناء التفتيش فلا يطلع إلا على الأشياء أو الأماكن التي يحتمل أن يجد فيها بيانات أو برامج أو أشياء أو أدلة أو براهين لها علاقة بالجريمة.
- على المحقق ألا يسترسل في الاطلاع عما ظهر أمامه صدفة.
- أن يحاول المحقق – ما وسعه الجهد– عدم إطلاع غيره على محتويات الحاسوب محل التفتيش(٢).

وقد أخذ **القانون العربي النموذجي الموحد** لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات في المادة (٢٦) بضمانة حفظ أسرار المدعى عليه غير المتعلقة بالجريمة من الاطلاع عليها عندما نص فيها على أنه: " في حالة التفتيش والضبط في نطاق الجرائم الإلكترونية، يجب النص على ضمانات لحماية سرية البيانات الأخرى المخزنة وعدم المساس بحقوق الغير المتعلقة بالبرامج والبيانات المخزنة".

---

(١) خالد عياد الحلبي، المرجع السابق، ص٢٤٥ – ٢٤٦.

(٢) معمر علي إبراهيم محمد، المرجع السابق، ص١٧٠.

**ب- أن يتم التفتيش بناء على أدلة كافية بنسبة الجريمة إلى شخص معين:**

مجرد الإخبار عن جريمة، أو تقديم شكوى من المجني عليه لا يكفي لإجراء التفتيش[١]، بل يشترط لجواز إصدار أمر بتفتيش نظم الحاسوب والإنترنت أن يكون هناك اتهام موجه ضد شخص فاعل أو متدخل، وليكفي أن توجه التهمة إلى شخص، بل يجب أن يكون الاتهام جدياً بحيث قامت عليه من الدلائل ما يكفي لانتهاك حق الخصوصية لديه وتفتيش حاسوبه الشخصي وبرامجه الخاصة[٢]، لأن الأصل حتى يكون التفتيش عن الأدلة صحيحاً لا بد من توافر أمارات أو دلائل كافية على نسبة الجريمة إلى شخص معين، أي أن يكون مظنوناً فيه بأنه فاعل الجريمة أو شريك أو متدخل فيها أو حائز أشياء تتعلق بالجرم، أي أن تتوافر لدى قاضي التحقيق دلائل كافية إما على اتهام شخص معين بارتكاب الجريمة أو بحيازته أشياء تتعلق بالجريمة[٣].

وفيما يتعلق بالتفتيش عن الدليل الإلكتروني، لابد أن تتوافر لدى المحقق أسباب كافية على أنه يوجد في مكان أو لدى الشخص المطلوب تفتيشه أدوات استخدمت في الجريمة الإلكترونية أو أشياء متحصلة منها أو مستندات إلكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المشتبه به أو غيره[٤].

ولا يقدح في جدية التحريات أن يكون ما أسفر عن التفتيش غير ما انصبت عليه، لأن الأعمال الإجرائية محكومة من جهة الصحة والبطلان بمقدماتها لا بنتائجها[٥].

---

(١) آمال عبد الرّحمن يوسف حسن، المرجع السابق، ص١٣١.

(٢) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٧٠.

(٣) د. بارعة القدسي، المرجع السابق، ص١٨٧.

(٤) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص ٣٨٨.

(٥) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٧٠-٧١.

وهناك من يذهب[١] إلى إمكانية وقوع تفتيش نظم الحاسوب والإنترنت على شخص غير المشتبه به بناءً على وجود قرائن قوية تنبئ بحيازته الأشياء أو أدلة تتعلق بالجريمة الإلكترونية، أو أنه يخفي بيانات أو برامج استخدمت في ارتكاب الجريمة أو يخفي المجرم المعلوماتي نفسه.

**ونحن نرى بجواز أن يقع التفتيش في إطار تفتيش نظم الحاسوب والإنترنت على غير المتهم لكن بشرط أن يكون إجراء التفتيش قد تم بناء على أدلة قوية ولا يكفي أن تشير الدلائل إلى أن في حوزته أشياء تظهر الكشف عن الحقيقة.**

وقد نص المشرع السوري على هذه الضمانة في الفقرة (١) من المادة (٨٩) من قانون أصول المحاكمات الجزائية التي جاء فيها: "١ – لا يجوز دخول المنازل وتفتيشها إلا إذا كان الشخص الذي يراد دخول منزله وتفتيشه مشتبهاً فيه بأنه فاعل جرم أو شريك أو متدخل فيه أو حائز أشياء تتعلق بالجرم أو مخف شخصاً مدعى عليه".

**ونرى أن هذه المادة السابقة تطبق أيضاً على التفتيش الواقع على نظم الحاسوب والإنترنت للحصول على الدليل الإلكتروني.**

وقد نص على هذه الضمانة المشرع الأردني في المادة (١٢ الفقرة أ) من قانون جرائم أنظمة المعلومات الأردني لسنة ٢٠١٠م، عندما اشترط من توافر دلائل في الأمكنة على استخدامها لارتكاب أي من تلك الجرائم الإلكترونية لجواز تفتيشها.

وأخيراً المحقق هو الذي يقدر بأن الأدلة التي بين يديه أو المعلومات التي تبلغها كافية للتحرك لإجراء التفتيش أو هي غير كافية، وهو بذلك خاضع لإشراف

---

(١) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٧٢.

المحكمة التي تخضع لها سلطة التحقيق، ولا رقابة لمحكمة النقض على الأدلة التي استند إليها المحقق لإجراء التحقيق[١].

**جـ- إجراء التفتيش من قبل أشخاص مختصين مؤهلين:**

إن تفتيش نظم الحاسوب والإنترنت إجراء خطير لما فيه من مساس بحق الخصوصية، لذلك لا يجوز القيام به إلا من قبل من خوله القانون بذلك[٢].

وبما أن التفتيش هو أحد إجراءات التحقيق الابتدائي، لذلك لا يمكن مباشرته بحسب الأصل سوى من سلطة التحقيق، فلا يجوز للنيابة العامة أو لموظفي الضابطة العدلية إجراؤه إلا في الأحوال الاستثنائية أي إذا كان الجرم مشهوداً أو بناءً على إنابة من سلطة التحقيق[٣].

وقد أعطى المشرع السوري حق إجراء هذا العمل التحقيقي بحسب الأصل لقاضي التحقيق سواء كان الجرم مشهوداً أم غير مشهود، وسواء كان جناية أم جنحة وفي جميع الأمكنة، فله أن يفتش المشتبه به أو غيره[٤]. كما له أن ينيب عن في ذلك أحد قضاة الصلح في منطقته أو قاضي تحقيق آخر في الأمكنة التابعة للقاضي المستناب أو أحد موظفي الضابطة العدلية[٥]، أما النيابة العامة والضابطة العدلية فيجوز لهما استثناءً في حال كانت الجريمة المشهودة جناية تفتيش المدعى عليه ومنزله ومكان وقوع الجريمة، أما إذا كانت الجريمة المشهودة

---

(١) آمال عبد الرّحمن يوسف حسن، المرجع السابق، ص١٣١.

(٢) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٥٤.

(٣) د. بارعة القدسي، المرجع السابق، ص١٨٧ – ١٨٨.

(٤) المادة (٩٤) الفقرة /١/ من قانون أصول المحاكمات الجزائية السوري.

(٥) المادة (١٠١) من قانون أصول المحاكمات الجزائية السوري.

جنحة فليس لهما سوى تفتيش المقبوض عليه[١]. أما المشرع الأردني فقد أعطى حق إجراء تفتيش نظم الحاسوب والإنترنت لموظفي الضابطة العدلية[٢].

**إما بالنسبة لإجراء التفتيش من قبل أشخاص مؤهلين فيبرر ذلك أن** هنالك إجراءات تفتيش في الجرائم الإلكترونية تحتاج إلى تقنيات خاصة تختلف عن حالات التفتيش التقليدية، كما أن تفتيش نظم المعلومات ليست سهلة وتتطلب دراية ومعرفة بملفات الحاسوب ومجال إخفاء المعلومات فيها لأنه يسهل إتلافها جزئياً أو كلياً، وأيضاً يصعب تحديد مكان الدليل أهو مخزن داخل النظام أم على دعامة خارجية، وقد تكون الملفات مشفرة لا يظهر محتواها إلا بفك التشفير[٣].

ويضاف إلى ذلك أنَّ كل المعطيات ليس لها تجسيد دائم على أية دعامة، بمعنى أنها لا توجد مسجلة على أسطوانة صلبة أو مرنة ولا على أية دعامة مادية منقولة أيًا كانت، فقد توجد هذه المعطيات في الذاكرة الحية للحاسوب، ويتم محوها في حالة عدم حفظها أو تسجيلها على أية أسطوانة، وحتى لو كانت المعطيات قد تم تخزينها على دعامة مادية إلا أنّه قد يكون من الصعب الدخول إليها بسبب وجود نظام معلوماتي للحماية[٤].

وبالتالي لا يكفي إجراء التفتيش من قبل أشخاص مختصين بل لا بد أن يكونوا مؤهلين حيث إن نقص خبرة جهات التحقيق بتقنيات الحاسوب ومعالجة البيانات يؤدي إلى إخفاقها في كشف جرائم الحاسوب وضبط مرتكبيها، بل قد يؤدي نقص الخبرة إلى تدمير الدليل عن طريق محو الأسطوانة أو الشريط الممغنط عن خطأ أو إهمال[٥].

---

(١) المواد (٢٩) و (٣٣) و (٤٦) من قانون أصول المحاكمات الجزائية السوري.

(٢) بموجب المادة (١٢ الفقرة أ) من قانون جرائم أنظمة المعلومات الأردني لسنة ٢٠١٠م.

(٣) خالد عياد الحلبي، المرجع السابق، ص١٥٠.

(٤) د. علي حسن الطوالبه، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، المرجع السابق.

(٥) د. جميل عبد الباقي الصغير، المرجع السابق، ص١٢٢.

واتجه الفقه في الولايات المتحدة الأمريكية إلى أن قيام القاضي بإصدار أمر التفتيش يفترض أن يكون ملماً ببعض الجوانب الفنية بالكومبيوتر واستخداماته وذلك حتى لا يكون قراره مشوباً بالبطلان وحتى لا تكون القرارات القضائية وسيلة للتسلط والاستبداد في يد البعض(١).

لذلك يقترح البعض(٢) إجراء تحقيقات هذه الطائفة من الجرائم باستخدام "أسلوب فريق التحقيق"، والذي يتألف من متخصصين في مجالات الحاسوب والمعالجة الآلية للبيانات.

**د-صدور إذن مسبق بالتفتيش:**

بما أن التفتيش يُعد إجراء من إجراءات التحقيق وليس من إجراءات التحري، لذا فيتطلب أوامر قضائية لمباشرته(٣)، فلابد من صدور إذن مسبق بالتفتيش حتى يدل على جدية التحقيق، وبناء عليه لا يجوز التدخل بالإطلاع على البريد الإلكتروني دون إذن صاحبه مالم يصدر إذن قضائي بذلك، وتطبيقاً لذلك قضي في كندا ببطلان الدليل المستمد من البريد الإلكتروني لأحد الأشخاص دون موافقة من هذا الأخير(٤).

ومن التشريعات التي نصت على هذه الضمانة المشرع الأردني عندما اشترط حصول موظفي الضابطة العدلية حصولهم على إذن من المدعي العام المختص، أو من المحكمة المختصة لتفتيش أي مكان تشير الدلائل في استخدامها لارتكاب جرائم إلكترونية(٥).

---

(١) د. مدحت رمضان، المرجع السابق، ص٧٢ – ٧٣.

(٢) د. جميل عبد الباقي الصغير، المرجع السابق، ص١٢٢.

(٣) خالد عياد الحلبي، المرجع السابق، ص١٤٩.

(4) David.G; Masse www. Mase.org/preuve courrie/.thm.p.II.

د. نزيهة مكاري، المرجع السابق، ص١٣٠.

(٥) نص المشرع الأردني في المادة (١٢ الفقرة أ) من قانون جرائم أنظمة المعلومات الأردني لسنة ٢٠١٠م، على أنه: "مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة

وعند إصدار إذن التفتيش لابد من تحديد محل ذلك الإجراء تحديداً دقيقاً وكذا الغرض منه، وأن يتأكد من أنه مما يجوز تفتيشه، وإلا كان هذا الإجراء باطلاً، فمقر الهيئات الدبلوماسية مثلاً لا يجوز تفتيشها(١). كما يجب مراعاة مكان وجود الحاسوب أثناء مباشرة التفتيش فقد يكون في مكان عام أو خاص، كما أن لصفة المكان أهمية خاصة في مجال التفتيش، حيث أنه إذا كان متواجداً في مكان خاص كمسكن المتهم أو أحد ملحقاته، فإنه يأخذ حكمه، فلا يجوز تفتيشه إلا في الحالات والضمانات التي يجوز فيها تفتيش المسكن، وهي الحصول على الإذن بالتفتيش من حائزه(٢)، ويجب التمييز داخل ذلك المكان بين ما إذا كانت مكونات الحاسب منعزلة عن غيرها من الحواسيب الأخرى أم أنها متصلة بحاسوب أو بنهاية طرفية في مكان آخر كمسكن الغير مثلاً، ففي هذه الحالة يتعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش تلك الأماكن، وفي حال كانت المكونات المادية للحاسوب متواجدة في أماكن عامة كمحل بيع البرامج، فإن إجراءات التفتيش تخضع للقواعد المقررة الخاصة بتفتيش تلك الأماكن، وذات الشيء يقال إذا كانت المكونات المادية في حوزة شخص سواء أكان مبرمجاً أو عامل صيانة أو موظفاً في شركة تنتج برامج الحاسوب، إذ تطبق حينئذ أحكام تفتيش الشخص وبذات الضمانات(٣).

---

حقوق المشتكي عليه الشخصية حيث يجوز لموظفي الضابطة العدلية بعد الحصول على إذن من المدعي العام المختص، أو من المحكمة المختصة ...".

(١) عبد العزيز خنفوسي، المرجع السابق، ص١٤٧.

(٢) لا بد من الإشارة إلى أنه بعد الحصول على إذن بتفتيش المسكن فإنه لا يحتاج الحصول على إذن آخر بتفتيش جهاز الحاسوب الموجود فيه، لأن إذن التفتيش الخاص بالمسكن يمتد إلى الأشخاص والاشياء الموجودة في هذا المسكن. معمر علي إبراهيم محمد، المرجع السابق، ص ١٤٩.

(٣) عبد العزيز خنفوسي، المرجع السابق، ص١٤٨.

وكذلك لابد من تحديد عنوان شخص المتهم واسمه وصفته، وتحديد وسائل التفتيش والجهاز الذي سيقوم به، والأشياء التي يتم البحث عنها[١]، كما لو تضمن الإذن تحديد القطع الصلبة المكون منها الحاسوب، وكما لو صدر الإذن بتفتيش ذاكرة الحاسوب والأدوات الأخرى لتخزين البيانات[٢].

ولكن مع ذلك ونظراً لسهولة تدمير المعلومات الموجودة على أجهزة الكومبيوتر بما قد يضر بحسن سير العدالة فقد جرى العمل على إصدار أوامر التفتيش دون إخطار مسبق (No - Knock warrants) في الدعاوى الجزائية المتعلقة بالحاسوب وذلك على الرغم من المخاطر التي قد تترتب على استخدام مثل هذه الأوامر[٣].

حيث إن تنفيذ إذن التفتيش يثير بعض المشكلات في مجال الجرائم الإلكترونية ففي القانون الأمريكي ثمة مبدأ يجب أن يلتزم به رجال الضابطة العدلية، ألا وهو ضرورة الإعلان عن وجودهم والإفصاح عن السلطات المخولة لهم (أو ما يُعرف بقاعدة الاستئذان والإعلان). بيد أن هذه القاعدة العامة يمكن التحلل منها وعدم الالتزام بها على حد تعبير المحكمة الفيدرالية الأمريكية العليا متى كان عضو الضابطة العدلية قد توافر لديه شك مبرر في أن إعمال هذه القاعدة أو التقيد بها سيكون غير مجدٍ أو من شأنه إعاقة فعالية التحقيق، أو من المتوقع أن تنجم عنه خطورة ما، وهذا الاستثناء على قاعدة الاستئذان ينسحب بوجه خاص وفي كثير من الأحيان على تنفيذ إذن التفتيش في الجرائم الإلكترونية ما يسمح لرجال الضابطة مباشرة ذلك دون استئذان تحسباً لما يمكن أن يقوم به الجناة (الهاكرز) من تلاعب بالدليل ومحاولة العبث به متى تولد لديهم الشعور بأن أمرهم سينكشف.

---

(١) خالد عياد الحلبي، المرجع السابق، ص١٧٦ – ١٧٧.

(٢) عبد العزيز خنفوسي، المرجع السابق، ص١٤٧.

(٣) د. مدحت رمضان، المرجع السابق، ص٧٥.

ذلك أن المتهمين والمشتبه فيهم يلجؤون في الغالب إلى تقنية المفاتيح الساخنة أو أسلوب تسخين الأسلاك Hot Wire من أجل إتلاف الدليل وتدميره قبل تمكن رجال الضابطة من الوصول إليه. ولهذا، فإن التمسك بالقاعدة سالفة الذكر ربما يحرم رجال الضابطة من فرصة كشف الدليل.

وبناءً عليه، فإن أمر تقدير المخاطر الناجمة عن التمسك بهذه القاعدة في القانون الأمريكي متروك لرجال الضابطة القائمين بتنفيذ إذن التفتيش. فإذا توافر لديهم ما يبرر الخروج على هذه القاعدة يمكنهم عندئذٍ التماس الإذن من قاضي التحقيق بالسماح لهم بتنفيذ التفتيش أو الضبط دون حاجة للاستئذان أو الإعلان المسبق [١].

**ونرى بحق ضرورة معالجة هذه المشكلة في التشريعات كافة والتشريع السوري خاصة وذلك بوضع نص خاص يقضي بتوسيع سلطات الجهة المعنية بإجراء التفتيش، ولو استلزم الأمر ولوج النظام المعلوماتي دون الحصول على إذن عند الضرورة، إذا كان من شأن انتظار صدور الإذن أن يفوت فرصة الحصول على الدليل الإلكتروني.**

**هـ- تسبيب التفتيش:**

يُعد تسبيب التفتيش من الضمانات الشكلية للتفتيش، حيث يجب أن يتضمن أمر التفتيش الأسباب التي أدت إلى إجراء هذا التفتيش، فلابد أن تستند مذكرة التفتيش إلى سبب موجب ومعقول لإجراء التفتيش ومبرر للاشتباه، وقد يتطلب القانون لاستصدارها من الجهات القضائية تقديم الدليل المعقول على توافر السبب،

---

(١) د. عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي "المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية، الطبعة الأولى، ٢٠٠٤ . ٢٠٠٥ م، ص٢٠٥-٢٠٦-٢٠٨-٢١٠-٢١٥.

ووصف محدد للمكان محل التفتيش وللأشخاص محل التفتيش، ونطاقه ومدى امتداده لشخص غير المشتبه به، إذا اشتبه بتوافر الأدلة الجرمية لديه[١].

ونرى أن التسبيب يكون ضماناً لتوافر العناصر الواقعية التي يتوافر بها سبب التفتيش، بالمعنى الدقيق، وحتى يكون ذلك التسبيب تحت رقابة هيئة الحكم، وكذلك حتى يتمكن الدفاع من مراقبة ما إذا كان إذن التفتيش صدر وفق الشروط القانونية، وبالتالي علة التسبيب هو بيان غاية التفتيش والتأكد من مشروعيته، وبالتالي بسط الرقابة على إجراء التفتيش من حيث صحته أو بطلانه.

وقد نص على تسبيب التفتيش قانون أصول المحاكمات الجزائية الأردني في المادة (٨٣) منه.

**و- توخي الوصول إلى الحقيقة:**

بما أن التفتيش به مساس للحرية الفردية، أو لحرمة المسكن، فيجب أن يكون هناك فائدة ترجى من ورائه وإلا كان تحكمياً[٢].

فإجراءات التفتيش في مكان للحصول على دليل لاتُجرى ولا يؤذن بها إلا بعد التحري من أجل الوصول إلى احتمال وجود فائدة مرجوة من التفتيش[٣].

فالهدف الذي تسعى إليه أجهزة العدالة من وراء جميع إجراءات التحقيق وإجراءات جمع الأدلة يجب أن يكون دائماً وأبداً هو كشف الحقيقة، وهذا ليس من أجل البحث في خصوصيات المشتبه به أو الانتقام للمجني عليه.

فالغرض من التفتيش هو حيازة شيء مفيد للتحقيق، فمجرد الاتهام بالجريمة لا يبرر التفتيش مالم يكن هناك فائدة ومؤداها ضبط أدلة تفيد التحقيق[٤].

---

(١) خالد عياد الحلبي، المرجع السابق، ص١٥٠-١٥٥.

(٢) آمال عبد الرّحمن يوسف حسن، المرجع السابق، ص١٣٢.

(٣) معمر علي إبراهيم محمد، المرجع السابق، ص٣٦-٣٧.

(٤) د. أحمد فتحي سرور، الوسيط في الإجراءات الجنائية، المرجع السابق، ص٣٦٠.

**ي- الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش:**

من أهم الضمانات الشكلية مما يتطلبه القانون في الجرائم حضور شخص أو أشخاص أثناء التفتيش، وتأتي ضرورة حضور المشتبه به أو الشهود عند تفتيش نظم الحاسوب والإنترنت بسبب قابلية هذه النظم للتغيير والتبديل والإتلاف، وبالتالي إمكانية الطعن بسلامة إجراء التفتيش وبطلانه، ومن جهة أخرى إضراراً بمصلحة المشتبه به وحرمانه من حق الدفاع عن نفسه، وإضافة أي برنامج أو بيانات أو محوها أو إتلافها من قبل سلطة التحقيق من شأنها إثبات التهمة على المشتبه به وإقامة الدليل عليه(١).

وقد جاء في توصية المجلس الأوربي رقم ر (٩٥) ١٣ في ١٩٩٥/٩/١١م أنه يتعين إخطار الشخص القائم على الأجهزة بأن النظام كان محلاً للتفتيش مع بيان المعلومات التي تم ضبطها(٢).

كما أن المشرع الفرنسي أوجب في حال تعذر حضور المشتبه به أو غير المشتبه به والذي يجري تفتيش مسكنه، حضور شاهدين لإجراء التفتيش الذي تجريه سلطة التحقيق أو تأذن به، وفي التفتيش الذي يجريه عضو الضابطة العدلية في حالة الجرم المشهود(٣)، وهذا الشرط يحقق ضمانة أكثر للمشتبه به (٤).

---

(١) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٥١..

(٢) د. مدحت رمضان، المرجع السابق، ص٨٠.

(٣) حيث نصت المادة (٩٦) من قانون الإجراءات الجنائية الفرنسي والتي تم تعديلها بموجب القانون رقم ٢٠١٦-٧٣١ المؤرخ في ٣ يونيو ٢٠١٦م، على: " إذا تم البحث في مكان آخر غير عائد للشخص المشتبه به، فإن هذا الشخص مدعو للحضور، وإذا تغيب هذا الشخص أو رفض الحضور، يتم البحث بحضور اثنين من أقربائه أو خلفائه الموجودين في المبنى، وفي حالة عدم وجود هؤلاء، فبحضور شاهدين".

موقع التشريعات الفرنسية:

https://www.legifrance.gouv.fr. تاريخ الدخول في ١/٣/ ٢٠١٨م.

(٤) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٦٠.

كما أجاز القانون الإنكليزي للمتهم أن يطلب حضور شاهد عند تفتيش منزله وما على القائم بالتفتيش إلا الاستجابة لمطلبه، مالم يكن هذا الطلب فيه إعاقة وتأخير للتحقيق(١).

وفي التشريع الجزائري إذا كانت المعاينة لا تتطلب حضور المتهم، فإن التفتيش لا يمكن إجراؤه إلا بحضوره أو بحضور من ينوب عنه أو بحضور شاهدين من غير التابعين للسلطة القضائية وهذا ما تؤكده المواد (٤٥ – ٨٢ – ٨٣) من قانون الإجراءات الجزائية الجزائري(٢).

وفي التشريع اللبناني والسوري فعلى القاضي أن يعين للمشتبه به وكيلاً عنه لإجراء التفتيش أمامه في الجنايات، أما في الجنح فيمكن إجراء التفتيش دون أحد(٣).

وكذلك إذا تم التفتيش لمنزل غير المشتبه به، فإن صاحبه يدعى للحضور بنفسه أو بواسطة غيره كلما كان ذلك ممكناً(٤).

أما في مصر، فقد جرى القضاء على اعتبار هذا الحضور ليس شرطاً جوهرياً(٥).

بينما ذهب التشريع الأمريكي إلى أنه يجوز تخويل دخول المكان خلسة دون إبلاغ الشخص الذي ستكون ممتلكاته محلاً للتفتيش المزمع مباشرته من قِبل المحكمة ذاتها. كما يخولها القانون منح الإذن بتأخير أو تأجيل الإعلام بالتفتيش كلما توافر سبب يبرر أن إخطار المالك يحتمل أن يكون له أثر سلبي، مثل العبث

---

(١) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٥١.

(٢) د. نزيهة مكاري، المرجع السابق، ص١٣٣.

(٣) المواد (٩٣–٩٤) من قانون أصول المحاكمات الجزائية اللبناني، والمواد (٩١–٩٢) من قانون أصول المحاكمات الجزائية السوري.

(٤) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص٣٦١.

(٥) نقض جنائي جلسة ١٩٧٧/٦/٥م، مجموعة الأحكام، س٢٨، رقم ١٤٥، ص٦٩١.

بالدليل أو تعريض حياة الأفراد أو سلامتهم للخطر أو للإفلات من الاتهام أو تهديد أحد الشهود أو الإضرار بسير التحقيق أو تأخير المحاكمة.

وهذا الاستثناء تبرره الضرورة الإجرائية، ومضمونه تغليب مصلحة التحقيق والوصول إلى الدليل على مصلحة الأفراد الذين يتقرر تفتيش ممتلكاتهم، وهذه التضحية قد تكون مستساغة ومقبولة بشرط عدم التوسع في هذا الاستثناء من أجل التعدي على الحرية الفردية وأن يكون تفسير الضرورات التي ألجأت عضو الضابطة إلى ذلك خاضعاً لمراقبة القضاء تفادياً لأي شطط أو تعسف من جانب رجال الضابطة العدلية[١].

**ونحن نرى أن في حضور المشتبه به أو صاحب المحل أو المسكن أو من ينوب عنهما أو الشهود إجراء التفتيش فيه ضمانة أكيدة لنتائج التفتيش الواقعة على نظم الحاسوب والإنترنت، لأنه يتيح للمشتبه به فرص مواجهة الدليل المستمد منه، وذلك في سبيل تحقيق التوازن المنشود بين مصلحة المشتبه به ومصلحة العدالة، ويمكن وضع استثناء على هذه الضمانة في حالة الخشية من العبث بالدليل أو للإفلات من الاتهام أو تهديد أحد الشهود أو الإضرار بسير التحقيق أو تأخير المحاكمة.**

**ء- تحديد الميعاد الزمني لتنفيذ التفتيش:**

حظرت بعض التشريعات الإجرائية تفتيش المسكن ليلاً في أحوال معينة[٢]، حيث اعتبرت هذا الحظر ضماناً للأفراد في مواجهة سلطة الدولة، واختلفت بعض التشريعات في وقت تنفيذ التفتيش في ساعات الليل[٣].

---

(١) د. عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي "المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية، المرجع السابق، ص٢٠٥-٢٠٦-٢٠٨-٢١٠-٢١٥.

(٢) انظر: المادة (٨٥) كويتي)، والمادة (٩٥) تونسي)، والمادة (٥٩) من قانون الإجراءات الجنائية الفرنسي.

(٣) لقد حدد القانون الجزائري وقت التفتيش من ٥ صباحاً إلى ٨ مساءً تطبيقاً لأحكام المادة (٤٧) من قانون الإجراءات الجزائية الجزائري.

ويلاحظ أن بعض التشريعات الأخرى لم تقيد تفتيش المسكن بوقت معين، لذلك يجوز التفتيش في أي ساعة من ساعات النهار أو الليل، والأمر متروك لتقدير القائم بالتفتيش، فله أن يختار الوقت الملائم لتنفيذ التفتيش ضمن المدة المحددة بالإذن[١].

أما في نطاق تفتيش نظم الحاسوب والإنترنت، فيذهب بعض الفقه[٢] إلى عدم تحديد وقت معين لتنفيذ التفتيش وتركه لسلطة المحقق التقديرية، ذلك لأن الوقت الذي تكثر فيه جرائم الإنترنت هو ليلاً ولعدة أسباب منها سهولة الاتصال وفي بعض الأحيان مجانية الاتصال بعد منتصف الليل، ولسهولة الدخول إلى المواقع المراد التلاعب بها أو اختراقها في الليل بسبب قلة المستخدمين في مثل هذا الوقت في الدوائر والمؤسسات والبنوك العامة والخاصة.

**ونحن نؤيد عدم تحديد وقت معين لتنفيذ التفتيش في إطار تفتيش نظم الحاسوب والإنترنت فقط، وذلك لأجل الحصول على الدليل الإلكتروني قبل التلاعب فيه أو إتلافه من قبل المجرمين.**

**ز- السماح بالطعن بالتفتيش والضبط:**

نصت على ذلك توصية المجلس الأوربي رقم ر (٩٥) ١٣ في ٩/١١/ ١٩٩٥م التي سمحت باتخاذ إجراءات الطعن العادية في قرارات الضبط والتفتيش[٣].

---

(١) حيث لم يورد المشرع السوري نصاً يوجب فيه إجراء التفتيش في وقت معين، لذلك يجوز إجراؤه في أي وقت من ساعات النهار أو الليل.

(٢) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٦١.

(٣) د. مدحت رمضان، المرجع السابق، ص٨٠.

**ن- وجوب أن يكون التفتيش خاصاً:**

نص التشريع الأمريكي على وجوب أن لا يكون الأمر بالتفتيش عاماً، حيث يفترض عند إصدار أمر التفتيش أن يكون الهدف منه محدداً تحديداً دقيقاً وأن يتم وصف الأشياء المطلوب ضبطها بصورة تفصيلية بحيث لا يترك أي شيء للسلطة التقديرية لرجل الضابطة الذي سيقوم بتنفيذ الأمر، ولا يختلف الأمر في فرنسا عن الموقف في الولايات المتحدة الأمريكية، حيث أنه لا يجوز أن يكون أمر التفتيش عاماً[١].

وهناك من يرى[٢] – ونحن نؤيده – أنه يترتب على التفتيش البطلان فيما لو كان أمر التفتيش قد صدر عاماً.

**وهكذا نجد أنه بالرغم من أن كل من المعاينة والتفتيش من إجراءات التحقيق، والهدف منهما جمع الأدلة التي تثبت وقوع الجريمة ونسبتها إلى المتهم، إلا أن المعاينة بطبيعتها لا تشكل مساساً بأسرار وحقوق الأفراد وحرمتهم، سواء تعلقت بالأشخاص أو الأشياء أو الأماكن بالقدر الذي يمثله التفتيش الذي هو إجراء يمس بمستودع أسرار المتهم وحرمته سواء انصب على شخصه، أو مسكنه أو أمتعته لذلك يتوجب إحاطة التفتيش بضمانات قانونية بشكل أكبر من المعاينة لضمان مشروعية الحصول على الدليل الإلكتروني.**

---

(١) د. مدحت رمضان، المرجع السابق، ص٧٣.

(٢) د. مدحت رمضان، المرجع السابق، ص٧٢.

## الفرع الرابع

## الضبط الإلكتروني

إن بحث الضبط كإجراء من إجراءات الحصول على الدليل الإلكتروني يقتضي أولاً، بيان مفهوم ضبط الدليل الإلكتروني، وثانياً، ضمانات مشروعية ضبط الدليل الإلكتروني.

**أولاً: مفهوم ضبط الدليل الإلكتروني:**

إن بحث مفهوم ضبط الدليل الإلكتروني يقتضي منا تعريفه وبيان محله ثم بيان مدى قابلية ضبط المكونات المادية والمعنوية، وأخيراً بيان آلية ضبط الدليل الإلكتروني.

**أ-تعريف الضبط:**

يقصد بالضبط في قانون أصول المحاكمات الجزائية بأنه: "وضع اليد على شيء يتصل بجريمة وقعت، ويفيد في كشف الحقيقة عنها، وعن مرتكبيها، وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو من إجراءات التحقيق"(١).

فالضبط هو الوسيلة القانونية التي تضع بواسطتها السلطة المختصة يدها على جميع الأشياء التي وقعت عليها الجريمة أو نتجت عنها أو استعملت باقترافها، كالأسلحة والأشياء المسروقة، والثياب الملوثة بالدم، والأوراق... وغير ذلك(٢).

والضبط هو الأثر المباشر للتفتيش، فالعلاقة وثيقة بين التفتيش والضبط، فإذا بطلت إجراءات التفتيش بطل الضبط، إلا أنه قد يتم الضبط من غير تفتيش، وذلك عندما يقدم المشتبه به باختياره الأشياء المتعلقة بالجريمة(١).

---

(١) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص ٣٩٤.

(٢) د. محمد طارق الخن، المرجع السابق، ص١٠٩.

أما الضبط في البيئة المعلوماتية فيقصد به: "وضع اليد على الدعائم المادية المخزنة فيها البيانات الإلكترونية التي تتصل بالجريمة الإلكترونية"[٢].

**ب- محل الضبط:**

إن الضبط بطبيعته وبحسب تنظيمه القانوني وغايته لا يرد سوى على الأشياء، أما الأشخاص فليسوا محلاً للضبط بالمعنى الدقيق، لكنهم محلاً للقبض حال حضورهم أو الإحضار في حال غيابهم، وإذا كانت بعض القوانين تتحدث عن ضبط الأشخاص وإحضارهم فإنه يعني القبض عليهم وإحضارهم، والقبض نظام قانوني يختلف تماماً عن ضبط الأشياء[٣].

ومن ناحية أخرى فإن القانون لا يفرق في مجال الضبط بين المنقول والعقار، ذلك أن كليهما يمكن ضبطه كذلك، ويستوي أن يكون الشيء المضبوط مملوكاً للمشتبه به أو لغيره[٤].

وضبط الأدلة الإلكترونية أو ما يتعلق بجرائم الحاسوب والإنترنت يتصل بضبط المكونات المادية لأنظمة الحاسوب، وضبط المكونات المعنوية والبرمجيات، وضبط المعطيات التي تتناقل أو يجري تبادلها في نطاق شبكة المعلومات التي تربط الحاسبات معاً وما يتصل بها[٥].

إذاً فيما يتعلق بالضبط الإلكتروني للحصول على الدليل الإلكتروني فإننا نميز بين ضبط المكونات المادية، وضبط المكونات المعنوية، وكذلك نعرض مدى قابلية البريد الإلكتروني للضبط.

---

(١) د. محمد طارق الخن، المرجع السابق، ص١٠٩.

(٢) عبد العزيز خنفوسي، المرجع السابق، ص١٥٠.

(٣) خالد عياد الحلبي، المرجع السابق، ص١٧٠.

(٤) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص ٣٩٤.

(٥) خالد عياد الحلبي، المرجع السابق، ص١٦٩.

**١- مدى قابلية المكونات المادية للضبط:**

غني عن البيان أن المكونات المادية لا تثير مشكلة من حيث إمكانية ضبطها لأنها أشياء مادية[١]، فلقد ذكرنا أن أجهزة الحاسوب ومخرجاتها، والمعدات التي تستعملها شبكة الإنترنت، والأقراص المدمجة، والدعامات الأخرى المخزنة عليها البيانات والمعلومات، تصلح لتفتيشها وضبطها، لأنها أشياء مادية تحتوي على برامج وبيانات ومعلومات مخزنة عليها.

والأشياء التي يمكن ضبطها من الحاسوب أو الأشياء المرتبطة به تنحصر فيما يلي:

- جهاز الحاسوب، المكون من الشاشة ولوحة المفاتيح والسماعات والفأرة وغيرها من المعدات.
- قرص التخزين الثابت وأقراص الليزر والأقراص المرنة.
- الأشرطة الممغنطة.
- الأوراق التي تمت طباعتها والمحفوظة في الملفات.
- لوحة الأم ولوحة الدوائر والطابعة[٢].
- الأجهزة والوحدات الملحقة بالحاسوب لاستخدام شبكة الإنترنت، كجهاز المودم، كجهاز المودم (Modem)، وأجهزة اختراق الاتصالات وتحليل الشفرات وكلمات المرور[٣].

وقد أخذ القانون الجزائي الألماني بذلك، وجعل الضبط يقع على الأشياء المادية المحسوسة وذلك في المادة (٩٤) منه، وأيضاً قانون الإجراءات اليوناني، والقانون الجزائي الكندي حيث أجازوا ضبط الأشياء ذات الطبيعة المادية[٤].

---

(١) أ. طارق محمد الجملي، المرجع السابق، ص٥٩.

(٢) خالد عياد الحلبي، المرجع السابق، ص١٧٢ - ١٧٣.

(٣) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٤٠.

(٤) خالد عياد الحلبي، المرجع السابق، ص١٧٥.

وضبط الأجهزة الإلكترونية كما يُعتقد ليس دليلاً على الإثبات وإنما هي خطوة نحو الإثبات أو تمهيداً للدخول إلى الإثبات أو النفي، فالجرائم الإلكترونية ليست مثل الجرائم التقليدية فحيازة المخدرات تشكل جريمة لذات الحائز أما حيازة الأجهزة ليست جريمة(١).

**ونحن نرى أن ضبط المكونات المادية للحاسوب والممثلة بمعدات الحاسوب والإنترنت وكابلات الشاشة وشاشة العرض ومفاتيح تشغيله...إلخ، يمكن أن يطبق بصددها ذات القواعد التقليدية للضبط دون أدنى صعوبة.**

**٢- مدى قابلية المكونات المعنوية للضبط:**

نظراً لكون الضبط محله في مجال الجرائم الإلكترونية، البيانات المعالجة إلكترونياً، فقد ثار التساؤل: **هل يصلح هذا النوع من البيانات لأن يكون محلاً للضبط الذي يعني كما رأينا وضع اليد على شيء مادي ملموس؟**

انقسم الفقه إلى اتجاهين:

**الاتجاه الأول: الاتجاه الرافض:**

يرى هذا الاتجاه أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم المادي لا ينطبق على بيانات الحاسوب غير المحسوسة أو المحسوسة(٢).

وقد أيد هذا الاتجاه جانب من الفقه الفرنسي مثل (Gassin) حيث يرى(٣) أن النبضات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة وبالتالي لا تعد شيئاً مادياً بالمعنى المصطلح ولذلك لا يمكن ضبطها.

---

(١) معمر علي إبراهيم محمد، المرجع السابق، ص٣٧.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٧٩.

(٣) Gassin R, le droit et l'informatique, Dalloz, Paris , France, 1982, pp. 38.

ويقترح هذا الاتجاه، إزاء النقص التشريعي ضرورة أن يضاف إلى الغاية التقليدية للتفتيش إمكانية البحث وضبط المواد المعالجة عن طريق الحاسوب أو بيانات الحاسوب، وبذلك تصبح الغاية من التفتيش بعد هذا التطور التقني الحديث هي البحث عن الأدلة المادية أو أية مادة معالجة بواسطة الحاسوب[١].

وبالتالي يذهب هذا الاتجاه إلى أنه بما أن بيانات الحاسوب لا تصلح لأن تكون محلاً للضبط، لانتفاء الكيان المادي عنها، فلا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس، عن طريق التصوير الفوتوغرافي، أو بنقلها على دعامة مادية أو غيرها من الوسائط المادية، ويستند هذا الاتجاه إلى أن النصوص التشريعية المتعلقة بالضبط يكون محل تطبيقها الأشياء المادية الملموسة[٢].

وقد أخذ بهذا الاتجاه القانون الألماني في المادة (١٦١) من قانون الإجراءات الألماني، عندما نص على أن البيانات المعالجة إلكترونياً لا يمكن ضبطها مجردة إلا إذا تم تحويلها إلى كيان مادي مطبوعة على ورق، أو عن طريق التصوير الفوتوغرافي[٣].

وكذلك ذهب القانون الروماني إلى أن الضبط ينصب على الدعامة المادية المدون عليها بيانات الحاسوب، كالأشرطة المغناطيسية أو الأقراص، وليس على الكيان غير المادي[٤].

**ونرى أنه لابد من تطوير النصوص القانونية المتعلقة بالضبط، لتشمل إمكانية ضبط معطيات الحاسوب والبيانات المعالجة إلكترونياً.**

---

(١) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص٣٧٩-٣٨٠.

(٢) خالد عياد الحلبي، المرجع السابق، ص١٧١.

(٣) خالد عياد الحلبي، المرجع السابق، ص١٧٥.

(٤) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٤٦.

وهذا ما ذهب إليه المشرع البلجيكي، وذلك بمقتضى قانون ٢٨ /١١/٢٠٠٠م، المعدل لقانون التحقيق الجنائي الذي إضاف المادة (٣٩مكرر) والتي سمحت بضبط الأدلة الإلكترونية مثل: نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية(١).

**الاتجاه الثاني: الاتجاه المؤيد:**

يرى هذا الاتجاه أن البيانات المعالجة إلكترونياً ما هي إلا ذبذبات إلكترونية أو موجات كهرومغناطيسية تقبل التسجيل والحفظ والتخزين على وسائط مادية، وبالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره(٢).

وبالتالي فهذا الاتجاه ينفي الطابع المعنوي لهذه البيانات، ويؤكد أنها شيء مادي يمكن تلمسه في المحيط الخارجي، وأنها كيان مادي لا يمكن إنكاره، وذلك استناداً إلى حكم صدر من محكمة جنح – بروكسل– في بلجيكا، أكد على أن هذه البيانات أشياء مادية محسوسة وبالتالي يمكن خضوعها لقواعد التفتيش التقليدية ومن ثم إمكانية ضبطها(٣).

وهكذا ينصب الضبط على الأشياء المادية وغير المادية، كما هو الحال في مراقبة المحادثات الهاتفية وتسجيل المحادثات الخاصة، وعلى ما هو مخزن في أجهزة الحاسوب، أو مخزن على الأقراص أو على الدعامات الأخرى(٤).

ومن التشريعات التي أيدت ضبط المكونات المعنوية والتي يجري تبادلها في نطاق شبكة المعلومات الإنترنت، قانون الإجراءات الجنائية اليوناني وذلك في

---

(١) عبد الناصر محمد محمود فرغلي، د. محمد عبيد سيف سعيد المسماري، المرجع السابق، ص١٥.

(٢) خالد عياد الحلبي، المرجع السابق، ص١٧١.

(٣) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٨٥.

(٤) خالد عياد الحلبي، المرجع السابق، ص١٧٠.

المادة (٢٥١) التي خولت سلطات التحقيق إمكانية القيام بأي شي ضروري لجمع وحماية الدليل الجزائي، ويفسر الفقه الجزائي عبارة – أي شيء– بأنها تمتد لتشمل ضبط البيانات المخزنة أو تلك التي تمت معالجتها إلكترونياً، لذلك فإن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسوب لا تشكل أية مشكلة في اليونان، إذ بإمكان المحقق أن يعطي أمراً للخبير الخاص بالحاسوب، والذي يقوم بجمع البيانات وتكون مقبولة كدليل في إجراءات المحاكمة الجزائية.

كذلك فإن المادة (٤٨٧) من القانون الكندي تمنح سلطة إصدار إذن الضبط – لأي شيء– طالما توافرت أسس معقولة للاعتقاد بأن الجريمة التي وقعت أو يشتبه في وقوعها أو أن هناك نية في ارتكاب الجريمة بواسطته أو سوف ينتج دليلاً على وقوع الجريمة وهكذا فإن هذا النص يفسر بطريقة جلية على أنه يسمح بضبط بيانات الحاسب الآلي غير المحسوسة[١].

كما أن المشرع الأردني قد أجاز ضبط المكونات المعنوية بشكل صريح وواضح. في قانون جرائم أنظمة المعلومات الأردني لسنة ٢٠١٠م، وذلك في الفقرة (ب) من المادة (١٢) منه[٢].

وقد أجاز القانون السوري ضبط كل ما يعدّ من آثار الجريمة، وسائر الأشياء والأوراق التي تساعد على إظهار الحقيقة، سواء أكانت تؤيد التهمة أم تنفيها. وقد أوجب القانون عرض الأشياء المضبوطة على المدعى عليه أو على

---

(١) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٧٩.

(٢) حيث نصت الفقرة (ب) من المادة (١٢) على انه: ".... يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج والأنظمة والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون، والأموال المتحصلة منها والتحفظ على المعلومات، والبيانات المتعلقة بارتكاب أي منها".

من ينوب عنه للمصادقة والتوقيع عليها، فإذا امتنع، صرّح القائم بالضبط بذلك في المحضر[١].

أما بالنسبة إلى **إجراءات ضبط المكونات المعنوية للحاسوب والإنترنت**، فإن البيانات والمعلومات لا يمكن ضبطها بشكل منفصل عن أجهزة وأدوات التخزين، فالحاسوب والأجهزة الملحقة به، هي بمثابة الأوعية المادية التي تحتوي هذه المعلومات والبيانات، وهي تشبه الحقيبة التي تُحفظ فيها الأوراق. وقد أجاز المشرع السوري في الفقرة (هـ) من المادة (٢٦) من قانون مكافحة الجريمة المعلوماتية للضابطة العدلية الحصول على **نسخة** من البيانات والمعلومات والبرمجيات الحاسوبية التي تم تفتيشها؛ **ويمكن للضابطة العدلية في حالات الضرورة ضبط الأجهزة** والبرمجيات الحاسوبية المستخدمة أو جزء من مكوّناتها.

ومن هذا النص نستنتج أن المشرع السوري قد أحسن فعلاً عندما أجاز ضبط المكونات المعنوية بنص صريح وواضح.

**٣- مدى قابلية البريد الإلكتروني للضبط:**

في الواقع تُخضع أغلب التشريعات هذا البريد للنص القانوني الوارد في قانون أصول المحاكمات الجزائية الخاص بضبط الخطابات والرسائل والجرائد والمطبوعات والطرود، وجميع البرقيات لدى مكاتب البريد، وبالتالي فإن التشريعات مازالت تخضع البريد الإلكتروني إجرائياً للقواعد الخاصة بالبريد العادي، لكن بالنظر لطبيعة البريد الإلكتروني فأصبح من الملح أن تتطور هذه القواعد وأن تتحدث عن ضبط البريد الإلكتروني، ومراقبته ووضع قواعد إجرائية خاصة به لكي يصبح من السهل الوصول لهذا الدليل وحفظه قبل أن يتم محوه بسرعة، تفوق الإجراءات الخاصة بالبريد العادي، والتعامل معه كدليل معنوي قائم بذاته، ومنفصل عن إمكانية إفراغه في مستندات ورقية تقليدية[٢].

---

(١) المواد (٣٢)، (٣٤)، (٩٧) من قانون أصول المحاكمات الجزائية السوري.

(٢) أمجد خليل حمودة، المرجع السابق، ص١٢٢.

**ونحن نرى بضرورة تطوير قواعد الضبط لتتلاءم مع طبيعة البريد الإلكتروني وتخصيص إجراءات تتصف بالمرونة والسرعة تفوق الإجراءات الخاصة بالبريد العادي لضبط هذا البريد وذلك نظراً لسهولة التخلص من الأدلة الإلكترونية الموجودة فيه.**

**جـ- آلية ضبط الدليل الإلكتروني:**

يرى الفقه المقارن أن على رجل الضابطة العدلية عندما يصل إلى مسرح الجريمة، أن يتبع في ضبط المعلومات الإلكترونية الإجراءات التالية[١]:

١- تأمين مسرح الجريمة الإلكترونية من العبث، إذ يجب عزل الحواسيب عن الشبكة، لتجنب إجراء أي تغيير على الأدلة الإلكترونية من قبل الغير. فلا بد من إجراء عملية الفصل الضرورية بين الحاسوب وبين كل شخص ليس له علاقة بالقائمين على الدعوى الجزائية [٢]، وذلك خشية قيام المشتبه به أو من له علاقة أو مصلحة ما بتدمير الأدلة بإزالتها من الحاسوب والمشرع المقارن يدرك مدى أهمية ضبط وتحريز الأدلة الإلكترونية.

٢- كما يجب رفع البصمات عن الأجهزة لمقارنتها فيما بعد ببصمة المشتبه به.

٣- حجز أو مصادرة الحاسوب أو القرص الصلب، وجميع الحاويات المادية والذواكر، كالسواقات والأقراص الممغنطة. فقد قام المشرع الأمريكي في المرشد الفيدرالي بإجازة مصادرة القطع الصلبة (في الحاسوب ومكوناته المادية) إلا أن هذا الإجراء قد لا يكون هناك إمكانية في اتخاذه كما لو كان الضبط يتم عن بُعد في حالة اتخاذ إجراءات جزائية عن بُعد، ولذلك اتجه المشرع المقارن إلى الاعتراف بوجود أساليب أخرى تصلح لكي يتم الضبط بمقتضاها مثل النسخ (copy) في حالة عدم وجود إمكانية لضبط القطع الصلبة فيتم مثلاً نسخ المواد

---

(١) د. محمد طارق الخن، المرجع السابق، ص١٠٩.

(٢) د. مأمون سلامة، شرح قانون الإجراءات الجنائية، د.ط، دار الفكر العربي، الإسكندرية، مصر، بلا تاريخ، ص٣٥٨ .

التي تحتاج إلى فك شفرتها لكي يتم التعرف على محتوياتها، وبالتالي يكون أسلوب النسخ صالح تماماً أن ينتج عنه دليل إلكتروني مقبول أمام القضاء وإلى جوار النسخ يوجد أيضاً أسلوب تجميد التعامل مع الحاسوب أو أحد القطعات المكونة له والتي تم استخدامها في ارتكاب الجريمة، والتي تحتوي على ما يفيد الأدلة على ارتكابها، ومثل هذا الإجراء يصلح أن يتخذ في مواجهة الحاسبات الخادمة التي تحتوي على مواقع القرصنة، وكذلك يصلح أسلوب التجميد إذا كان القرص الصلب يحتوي على ملفات مشفرة وتحتاج بالتالي إلى فك شفرتها لكي يمكن التعرف على محتوياتها الإجرامية أو يكون الدخول إلى الحاسوب يحتاج إلى كلمة مرور (password) فالتجميد هنا يساعد خبراء المعمل الجنائي على القيام بعملهم دون خوف من ضياع الدليل[١].

٤- وضع ملصقات على الأشياء المضبوطة، وتوثيقها وتغليفها، وتحضيرها لنقلها بالحالة التي كانت عليها إلى مكان الاختبار والفحص.

٥- تحرير محضر بعد إجراء عملية الفحص، يتضمن ذكر جميع الإجراءات السابقة، والنتائج التي تم التوصل إليها بنتيجة الفحص.

كما وضعت المنظمة الدولية لدليل الحاسوب[٢]عدة معايير لضبط الدليل الإلكتروني وقد تمت المصادقة على هذه المعايير خلال المؤتمر الدولي للبحث

---

(١) د. عمر محمد بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي (المرشد الفيدرالي الأمريكي لتفتيش وضبط نظام الحاسب الآلي وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية)،المرجع السابق، ص٢١٩.

(٢) تأسست المنظمة الدولية لدليل الحاسوب (International Organization on computer Evidence) في عام ١٩٩٥، وتتكون من الجهات الحكومية المسؤولة عن تطبيق القانون، أو من الهيئات الحكومية التي تزاول التحقيق في مجال الحاسوب. وتهدف هذه المنظمة إلى تزويد الجهات الدولية القانونية بكيفية تبادل المعلومات بتحقيقات جرائم الحاسوب والمسائل ذات الصلة بالمعلوماتية الشرعية. كما تقوم بتنظيم عملية الاتصال بين أعضائها، وتقدم التوصيات اللازمة في هذا المجال، وتقيم المؤتمرات المتعلقة بنشاطاتها.

المعلوماتي والجريمة التقنية، المنعقد في تشرين الأول عام ١٩٩٩ (IHCFC)[١]، وهذه المعايير هي:

- عدم تغير الدليل أثناء ضبطه.
- أن تتم عملية الضبط من قبل شخص مؤهلٍ في المعلوماتية الشرعية.
- جميع النشاطات المتعلقة بالضبط والوصول والتخزين ونقل الدليل الإلكتروني، يجب أن تكون موثقة ومحفوظة بغرض التدقيق.
- أن يكون الشخص الذي بحوزته الدليل الرقمي مسؤولاً عن جميع الإجراءات المتعلقة بهذا الدليل.
- أن تكون الجهات المسؤولة عن ضبط وتخزين ونقل الدليل الإلكتروني والوصول إليه مسؤولة عن تطبيق هذه المبادئ[٢].

**ونرى أنه لابد من أن يكون ضبط الدليل الإلكتروني متناسب مع ماهيته، بحيث ينصبّ الضبط على جميع الأجهزة والأدوات التي تمّ تخزين المعلومات فيها، لأن ضبط المعلومات والبيانات لا يمكن أن يتم بمعزل عن وسائط التخزين.**

**ثانياً: ضمانات مشروعية ضبط الدليل الإلكتروني:**

يمثل الضبط أحياناً اعتداء على حقوق الغير، أو على حرمة حياته الخاصة، فيجب اتخاذ الضمانات اللازمة لحماية هذه الحقوق والحريات[٣]، ومن أهم تلك الضمانات:

**أ- أن يكون الدليل الإلكتروني متعلق بالجريمة المراد ضبطها:**

من أهم الضمانات القانونية التي يجب توافرها في الضبط ليكون مشروعاً هي أن تكون البيانات المراد ضبطها متعلقة بالجريمة، فالأجهزة قد تحوي

---

(١) وهو اختصار لـ International Hi - tech crime and Forensics conference.

(٢) د. محمد طارق الخن، المرجع السابق، ص١٢١.

(٣) خالد عياد الحلبي، المرجع السابق، ص١٧٢.

بيانات شخصية أو بيانات لا تتعلق بالجريمة فيكون الضبط غير مشروع كما قد تحتوي الأجهزة على ملفات تتعلق بالمراسلات الخاصة ببعض العاملين مع الغير بالبريد الإلكتروني فيكون ضبطها والاطلاع عليها متعارضاً مع النصوص التي تحمي حرمة الحياة الخاصة والمراسلات الشخصية[١].

**ونحن نشدد على مراعاة تعلق هذه البيانات والمعلومات المراد ضبطها بالجريمة حفاظاً على مبدأ مشروعيتها.**

**ب- إن تقوم بضبط الدليل الإلكتروني سلطة مختصة:**

وقد حدد المشرع السوري في الفقرة (هـ) من المادة (٢٦) من قانون مكافحة الجريمة المعلوماتية هذه السلطة ومنحها للضابطة العدلية، وكذلك فعل المشرع الأردني عندما حدد السلطة المختصة بضبط الدليل الإلكتروني بالضابطة العدلية وذلك في قانون جرائم أنظمة المعلومات الأردني لسنة ٢٠١٠م، في الفقرة (ب) من المادة (١٢)منه[٢].

**جـ- الحصول على إذن مسبق لضبط الدليل الإلكتروني:**

لا بد من صدور إذن بالضبط يمنح صلاحية لدخول نظام الحاسوب وضبط ما يحتويه من بيانات ومعلومات[٣].

وقد نص على هذه الضمانة المادة (٤٨٧) من القانون الجزائي الكندي عندما منحت سلطة إصدار إذن لضبط أي شيء تتوافر أسس معقولة للاعتقاد بأن الجريمة ارتكبت أو يشتبه في ارتكابها[١].

---

(١) د. مدحت رمضان، المرجع السابق، ص٧٢.

(٢) حيث نصت الفقرة (ب) من المادة (١٢) على انه: ".... يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج والأنظمة والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون، والأموال المتحصلة منها والتحفظ على المعلومات، والبيانات المتعلقة بارتكاب أي منها".

(٣) خالد عياد الحلبي، المرجع السابق، ص١٧٧.

ونظراً لأن الجريمة الإلكترونية تتم في بيئة غير تقليدية، فهي تقع خارج إطار الواقع المادي الملموس، وأركانها تقوم في بيئة الحاسوب والإنترنت، وهذا الأمر يجعل إمكانية محو وطمس الدليل بسهولة، ومن ثم يكون من الصعب ملاحقة المجرم أو كشف شخصيته، لذلك يرى جانب من الفقه ضرورة تدخل المشرع بإضافة حالة ارتكاب الجريمة الإلكترونية كظرف استثناء يسمح لرجال السلطة العامة بالقيام بضبط الأدلة عند وقوع الجريمة، وبدون إذن مسبق من النيابة العامة، وهذا حماية للأدلة من المحو والتعديل من قبل الفاعل[٢].

**ونرى بضرورة الاستغناء عن طلب الإذن لضبط الأدلة الإلكترونية في الجرائم الإلكترونية استثناءاً وذلك خشية محو وطمس الدليل بسهولة، ومن ثم يكون من الصعب ملاحقة المجرم أو كشف شخصيته.**

**وأخيراً درسنا في هذا المبحث، الحصول على الدليل الإلكتروني في الإجراءات التقليدية، فتناولنا في المطلب الأول منه صعوبات الحصول على الدليل الإلكتروني في الإجراءات التقليدية، وتبين لنا أن هذه الصعوبات منها ما يتعلق بالجريمة الإلكترونية ومنها ما يتعلق بالدليل الإلكتروني ومنها ما يتعلق بأسباب متعددة لعل من أهمها نقص خبرة أجهزة العدالة وصعوبات فنية، كما درسنا في المطلب الثاني مشروعية الحصول على الدليل الإلكتروني في الإجراءات التقليدية، فدرسنا الخبرة الإلكترونية وضمانات مشروعيتها، وأيضاً المعاينة وذلك بتعريفها ومحل إجراءها وآلية المعاينة وضمانات مشروعيتها، وكذلك درسنا إجراءات التفتيش والضبط وعرضنا لمشروعية خضوع المكونات المادية والمعنوية لإجراء التفتيش والضبط وآلية التفتيش والضبط للحصول على الدليل الإلكتروني، وأخيراً عرضنا ضمانات مشروعية التفتيش والضبط في الحصول على دليل إلكتروني مشروع، ونظراً لأن هذه الإجراءات التقليدية لاتعد**

---

(١) خالد عياد الحلبي، المرجع السابق، ص١٧٦.

(٢) عائشة بن قارة مصطفى، المرجع السابق، ص٤٨.

**كافية بشكل فعال للحصول على الدليل الإلكتروني، مما أدى إلى ظهور إجراءات حديثة، حيث إن التطور المستمر الذي يتصف به الدليل الإلكتروني أدى إلى تطور وسائل الحصول عليه، وسنعرض هذه الإجراءات الحديثة في المبحث الثاني.**

# المبحث الثاني
# مشروعية الحصول على الدليل الإلكتروني في الإجراءات الحديثة

إن التطور المذهل للجريمة والمجرم، وأمام تفاقم حجم الأضرار الناجمة عنهما فإن كافة وسائل البحث والتحقيق التقليدية تقف عاجزة عن كشفهما ولتفادي تغلب وسائل ارتكاب الجريمة على وسائل الكشف عنها ومكافحتها، لا بد من الاعتماد على الأساليب العلمية والتقنية الحديثة، فالميزة التي يجب أن تطبع الأبحاث والتحقيقات الجنائية المعاصرة هي الاتجاه والسير نحو الاستفادة من معطيات العلم الحديث في اكتشاف الجريمة وإثباتها بالوسائل الفنية بتقديم الدليل العلمي المادي في إطار احترام الشرعية الإجرائية(١).

فالسبب الذي يدعو لضرورة إنشاء إجراءات حديثة للحصول على الدليل الإلكتروني يتمثل في الأسباب التالية: أولهما: إن إجراءات التحقيق التي تهدف إلى جمع الأدلة كثيرة، ومن هذه الإجراءات الانتقال والمعاينة وسماع الشهود، وندب الخبراء، والتفتيش والاستجواب والمواجهة، وإجراءات جمع الأدلة هذه لم ترد في القانون على سبيل الحصر، ولذا يجوز للمحقق أن يباشر أي إجراء آخر يرى فيه فائدة للإثبات طالما انه لا يترتب على اتخاذه تقييد لحريات الإفراد أو مساس بحرمة مساكنهم(٢).

وثانيهما: عجز الإجراءات التقليدية عن الوصول إلى الدليل الذي يكفي لإثبات هذا النوع الجديد من الجرائم(٣)، كما أن الإجراءات التقليدية التي يتم إتباعها

---

(١) بهلول مليكة، المرجع السابق، ص٤.

(٢) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٩٧ – ٩٨. و. أ. م. جاسم خريبط خلف، المرجع السابق، ص٧.

(٣) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٥٨.

بغرض الحصول على الدليل الإلكتروني تواجه صعوبات كثيرة[١] تحيط بهذه الإجراءات في سبيل استخلاص الدليل الإلكتروني[٢]، فعلى سبيل المثال أن وسائل المعاينة وطرقها التقليدية لا تفلح غالباً في إثبات دليل الجريمة الإلكترونية التي تنفرد بطبيعة خاصة بها[٣]، وثالثهما: إن ثورة الاتصالات عن بُعد في تأثيرها على طبيعة الجرائم التي ترتكب كنتيجة لاستخدام تقنيتها العلمية ستزيد من تعقيد الدليل الجزائي، وطرق الوصول إليه، بحيث أن ذلك قد يؤثر على الطرق التقليدية للحصول عليه، وهذا الأمر يتطلب أن يلحق التطور طرق الحصول على الدليل بالنسبة لهذه الجرائم المستجدة لكي يمكن عن طريقها الوصول إليه[٤]. ورابعهما: أن التطور المستمر الذي يتصف به الدليل الإلكتروني أدى إلى تطور وسائل الحصول عليه والتي يجب مراعاتها قانونياً حتى يكون في الإمكان الاعتماد عليه

---

(١) «من المسائل التي أثيرت بمناسبة تعذر الحصول على الدليل في الجريمة الإلكترونية بطرق تقليدية نظراً لخصوصية هذا النوع من الجرائم، هو مدى سريان الحماية المعول بها للاطلاع غير المصرح به على الأوراق المختومة أو المغلقة، لتمتد إلى نظام المعالجة الآلية للبيانات والمحمي فنياً ضد الاختراق، حيث يجب عدم المساس بمبدأ المشروعية، وإن السبب في حظر الاطلاع على الأوراق المغلقة ، والمغلقة والمختومة هو رغبة صاحبها في عدم اطلاع الغير عليها، بدليل انه اتخذ سبل الحماية الممكنة ضد محاولة الاطلاع غير المصرح بها، بدليل إغلاق هذه الأوراق أو تغليفها بأي طريقة وذات العلة تتوافر في البيانات المعالجة ألياً، حيث لا يمكن بدون الحصول على مفتاح الشفرة أو الكود أو كلمة المرور الدخول إلى نظام هذه البيانات، وبذلك يكون صاحب ذلك النظام قد رفض مسبقاً عمليات الاطلاع غير المصرح به ما لم يكن الراغب في الاطلاع مصرحاً له عن طريق أعطائه مفتاح المرور إلى هذه البيانات وذلك لا يتوافر في حالة عضو الضبط القضائي القائم بالتفتيش موضوع الحديث، إن هذا التوجه يهدف أولا وأخيرا إلى إيجاد مظلة حماية قانونية لنظام البيانات المعالجة ألياً والتي لا يصرح للغير بالاطلاع عليها» أنظر: أ.م. جاسم خريبط خلف، المرجع السابق، ص١٧.

(٢) هلال آمنة، المرجع السابق، ٥٧.

(٣) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٩٤.

(٤) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٥٨.

كدليل إثبات في مختلف القضايا[١]، فذكرنا أن الدليل الإلكتروني ليس على صورة واحدة وإنما له خصوصية التنوع، ونظراً إلى ما تتمتع به طبيعته من ضرورة توافقه مع الواقعة الجرمية، وهذا يعني أنه ليس هناك وسيلة واحدة للحصول عليه وفي كل الأحوال يظل الدليل المستمد منها إلكترونياً[٢].

وهذا يعني أن الطرق العلمية والفنية للحصول على الدليل الإلكتروني قد أصبحت هي المناسبة لإثبات هذا النوع من الجرائم[٣].

وعلى ضوء ذلك يمكن القول بأن الدليل المتحصل من الوسائل الالكترونية يستمد طبيعته من ذات العمليات الالكترونية التي نتج منها في حالة الاعتداء عليها بالأفعال غير المشروعة، ولذلك فهو يتخذ أيضا طبيعة إلكترونية بحيث تصعب على المحقق القيام بها إلا بأتباع إجراءات معينه ذو طبيعة فنية، وليس أدل على ذلك من أن التلاعب في المستندات الالكترونية لا يمكن كشفه بالطرق التقليدية وإنما قد يحتاج ذلك إلى أدلة الكترونية قد تتحصل من الوسائل الالكترونية ذاتها أو باستخدام التقنية العلمية المتقدمة التي يتعين إتباعها للوصول إليه[٤].

كذلك فإن ظهور الحاسبات الآلية واستخدامها على مجال واسع سواء على المستوى الفردي أو على المستوى الحكومي، وما صاحب ذلك من تطور تقني بأساليب الاستنساخ الملونة عن طريق الناسخات والطابعات الملونة، فقد ترتب عليه أفوال دور المستندات الورقية والاتجاه نحو تصاعد لدور المستندات الإلكترونية كالأشرطة الممغنطة وأسطوانات الفيديو والدعامات المثبتة والميكروفيلم، وهذه الدعامات الجديدة لا تتكيف مع قواعد الإثبات التقليدية التي

---

(١) هلال آمنة، المرجع السابق، ص٢١.

(٢) سهى إبراهيم داود عريقات، المرجع السابق، ص١٧.

(٣) د. محمد أحمد المنشاوي، المرجع السابق، ص٥١٥.

(٤) أ. م. جاسم خريبط خلف، المرجع السابق، ص٧ – ٨.

تتصب على المستندات الورقية، ومن ثم فإن إثباتها يثير العديد من المشكلات حول مدى اعتبارها محررات يمكن أن يقع عليها التزوير أو التزييف[١].

ومما يؤكد ذلك أن الجرائم التي تقع على بطاقات الائتمان تتميز بطبيعة خاصة الأمر الذي يتطلب إتباع طرق في البحث والاستقصاء تكون مختلفة عن المتبعة في إثبات الجرائم التقليدية[٢].

وقد ورد جزء من هذه الإجراءات في الاتفاقية المتعلقة بالجريمة الإلكترونية (اتفاقية بودابست) المنعقدة في ٢٠٠١/١١/٢٣م، حيث خصصت هذه الاتفاقية الباب الثاني (القانون الإجرائي) وحددت المادة (١٦) ومايليها لهذه الإجراءات (الإجراءات الحديثة في الحصول على الدليل الإلكتروني)، وأخذت بها قوانين بعض الدول كالقانون الفرنسي والأمريكي.

ومن المعروف إن البيانات في البيئة التكنولوجية ليست دائماً ساكنة، بحيث يمكن أن تكون متحركة عبر شبكة من الشبكات، ولهذا لابد من أن يكون الإجراء متماشياً مع طبيعة هذه البيانات[٣].

وتبعاً لما تقدم سنقسم دراستنا للإجراءات الحديثة للحصول على الدليل الإلكتروني إلى الإجراءات المتعلقة بالبيانات الساكنة من جهة، والإجراءات المتعلقة بالبيانات المتحركة من جهة أخرى، وذلك في المطلبين التاليين:

**المطلب الأول: مشروعية الحصول على الدليل الإلكتروني في الإجراءات المتعلقة بالبيانات الساكنة.**

---

(١) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٥٣.

(٢) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٥٢.

(٣) تجدر الإشارة إلى أن الإجراءات الخاصة بكل من البيانات الساكنة والمتحركة مستقاة من اتفاقية بودابست، وهي أولى المعاهدات الدولية التي تكافح الجرائم الإلكترونية. هلال آمنة، المرجع السابق، ص٥٧.

**المطلب الثاني: مشروعية الحصول على الدليل الإلكتروني في الإجراءات المتعلقة بالبيانات المتحركة.**

# المطلب الأول
# مشروعية الحصول على الدليل الإلكتروني
# في الإجراءات المتعلقة بالبيانات الساكنة

هناك من يرى[١] أن الإجراءات المتعلقة بالبيانات الساكنة لها أهمية في استخراج الدليل الإلكتروني خاصة وأنها تكون تحت إشراف مختصين في الحاسوب وملحقاته وشبكاته، على الرغم من أن فيها اعتداء على الحياة الشخصية للأفراد بسبب الاطلاع على بياناتهم الخاصة إلا أنه يمكن التغاضي عن هذا الاعتداء في سبيل كشف الحقيقة في الجريمة الواقعة والحصول على الدليل الإلكتروني وهو الهدف المنشود، ونسبة الجريمة الإلكترونية لأشخاص معينين، وعلى الرغم من الخلاف حول السلطة التي لها حق في الاطلاع على البيانات، وكذلك الخلاف فيما يتعلق بإلزام مزود الخدمات بإعطاء المعلومات، إلا أن الهدف يبقى هو إيجاد الدليل الإلكتروني.

وتتمثل هذه الإجراءات في التحفظ المعجل على البيانات المخزنة، وفي الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك، وسنبحثهما في الفرعيين التاليين:

**الفرع الأول: التحفظ المعجل على البيانات المخزنة.**

**الفرع الثاني: الأمر بتقديم بيانات معلوماتية عن المشترك.**

---

(١) هلال آمنة، المرجع السابق، ص٦٢.

## الفرع الأول

## التحفظ المعجل على البيانات المخزنة

إن دراسة إجراء التحفظ المعجل على البيانات المخزنة، يقتضي أولاً بيان مفهوم التحفظ المعجل على البيانات المخزنة، وثانياً بيان مشروعية التحفظ المعجل على البيانات المخزنة.

### أولاً: مفهوم التحفظ المعجل على البيانات المخزنة:

إن التعرض لمفهوم هذا الإجراء، يقتضي منا تحديد المقصود بمزودي الخدمات بما أنهم هم من يحوزون هذه البيانات، وكذلك تعريف التحفظ المعجل على البيانات المخزنة.

**أ – تعريف مزودي الخدمات:**

يُعرف مزود الخدمات بأنه: " الشخص الذي يقدم خدماته إلى الجمهور بوجه عام في مجال الاتصالات الإلكترونية التي لا تقتصر في أدائها على طائفة معينة من المتعاملين معه بمقتضى عقد من العقود"(١).

كما عرف المشرع القطري في المادة الأولى من القانون رقم (١٤) لسنة ٢٠١٤م، الخاص بمكافحة الجرائم الإلكترونية، مزودي الخدمة بأنه: " أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة تخزين المعلومات".

وأيضاً عرف القانون الفلسطيني رقم (١٦) لسنة ٢٠١٧م، بشأن الجرائم الإلكترونية مزودي الخدمة بأنه هو: " أي شخص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال عن طريق تكنولوجيا المعلومات، أو أي شخص آخر يقوم

---

(١) عائشة بن قارة مصطفى، المرجع السابق، ص١٥٦،

بمعالجة أو تخزين أو استضافة بيانات الحاسوب نيابة عن أية خدمة إلكترونية أو مستخدمي هذه الخدمة".

ويميز قانون حماية الحياة الخاصة في مجال الاتصالات الإلكترونية في الولايات المتحدة الأمريكية (ECPA) بين نوعين من مزودي الخدمات، حيث يتمثل النوع الأول في مزودو خدمة الاتصالات الإلكترونية والذي يقصد به كل من يقدم خدمة إلى مستخدمي الشبكة والتي تتمثل في تسهيل إرسال واستقبال الاتصالات السلكية والإلكترونية، أما النوع الثاني فهم مزودو خدمة معالجة المعلومات عن بُعد الذي يعرف حسب ما جاء في القسم (2) (c)2703S.C U S 18) من قانون خصوصية الاتصالات الإلكترونية الأمريكية بأنه: "كل من يقدم للجمهور خدمة معالجة البيانات عن بُعد بوسيلة من وسائل الاتصالات الإلكترونية"(١).

ومنه فإن أرسل شخص لشخص آخر رسالة عن طريق البريد الإلكتروني فإنها تمر بالضرورة بمزود خدمة الاتصالات الإلكترونية، وقبل أن يتلقاها المرسل إليه تبقى مخزنة لدى مزود الخدمات، لأنها عندما تصل للمرسل إليه فإنه قد يقوم بمسحها(٢).

**ب – تعريف التحفظ المعجل على البيانات المخزنة:**

يقصد بهذا الإجراء: "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"(٣).

ويبرر هذا الإجراء أن البيانات في البيئة الإلكترونية قابلة للمحو أو التغيير أو العبث بها بسرعة، وقد يكون الدافع هو طمس كل ما يؤدي إلى كشف شخصية فاعل الجريمة، فمثلاً قد يعلم أعضاء الضابطة العدلية بوجود صور دعارة للأطفال

---

(١) عائشة بن قارة مصطفى، المرجع السابق، ص١٥٦،

(٢) هلال آمنه، المرجع السابق، ص٥٨.

(٣) عائشة بن قارة مصطفى، المرجع السابق، ص١٥٩.

في اليوم الأول فيقومون باتخاذ إجراءات الحصول على إذن تفتيش في اليوم التالي، وفي اليوم الثالث يحصلون على الإذن ثم يصل إلى علمهم أن المزود قام بشطب السجلات كالمعتاد في اليوم الثالث المذكور. فالتحفظ من خلال هذا المثال يتضح أنه إجراء أولي أو تمهيدي الهدف منه هو محاولة الاحتفاظ بالبيانات قبل فقدانها(١).

كما أن البيانات المذكورة في الأمر تتضمن أيضاً بيانات المرور المتعلقة بالاتصالات السابقة وهذا بغرض تحديد خط سير الاتصال أي مكان ومصدر وصول هذه الاتصالات، والتي تُعد من الأمور الجوهرية للتعرف على هوية الأشخاص الفاعلين، وقد عرفت المادة الأولى الفقرة (د) من اتفاقية بودابست هذا النوع من البيانات وقالت بأنها صنف من بيانات الحاسوب التي تشكل محلاً لنظام قانوني محدد، حيث يتم استخراج هذه البيانات من الحواسيب عبر تسلسل حركة الاتصالات لتحديد مسلك الاتصالات من مصدرها إلى الجهة المقصودة، وبذلك تشمل مجموعة من البيانات تتمثل في: مصدر الاتصال ووجهته المقصودة، خط السير ووقت أو زمن الاتصال وفقاً لتوقيت غرينتش، حجم الاتصال ومدته ونوع الخدمة المعطاة مثل نقل الملفات أو بريد إلكتروني أو مراسلات فورية، وغالباً ما يحوز مزود الخدمة بمفرده على بيانات المرور ما يكفي للتحديد بدقة مصدر أو نهاية الاتصال، بل إن كل واحد منهم يكون لديه بعض أجزاء اللغز، ويتعين أن توضع هذه الأجزاء تحت الاختبار بقصد تحديد مصدرها والجهة المرسلة إليها(٢).

**ثانياً: مشروعية التحفظ المعجل على البيانات المخزنة:**

إن بحث مشروعية التحفظ المعجل على البيانات المخزنة، يقتضي بيان الأساس القانوني لمشروعيته، وضمانات هذا الإجراء، لذلك لابد لنا أن نبحث في:

---

(١) هلال آمنة، المرجع السابق، ص٥٩.

(٢) عائشة بن قارة مصطفى، المرجع السابق، ص١٥٩ – ١٦١.

**أ – الأساس القانوني لمشروعية التحفظ المعجل على البيانات المخزنة:**

في ظل تزايد الجريمة الإلكترونية أنه يجب توجيه مزودي الخدمات بأن يحتفظوا بكل هذه المعلومات التي تتعلق بالاتصالات الإلكترونية وإرسال نسخ منها بشكل دوري إلى الجهات المختصة ووضعها في قسم خاص يطلق عليه اسم الأرشيف الإلكتروني.

ونجد الأساس القانوني لمشروعية هذا الإجراء في اتفاقية بودابست حيث جاء في المادة (١٦) منها على أنه: "لابد على كل طرف في هذه الاتفاقية، أن يسمح لسلطاته المختصة أن تأمر مزود الخدمة أن يقوم بالتحفظ العاجل على البيانات المعلوماتية المخزنة بواسطة نظام معلوماتي، وهذا عندما تكون هناك أسباب كافية عن تعرض هذه البيانات للفقد أو التغيير، وهذا خلال ٩٠ يوم كحد أقصى، وهذه المدة قابلة للتمديد".

وقد حددت المذكرة التفسيرية لاتفاقية بودابست الأسباب التي تعود إلى اتخاذ مثل هذا الإجراء وذلك للمبررات التالية:

١ – قابلية البيانات المعلوماتية للتلاشي، حيث تكون محلاً للمحو أو التغيير سواء كان ذلك بدافع إجرامي من أجل طمس معالم الجريمة وكل ما يدل على صفة المجرم، أو بدافع غير إجرامي وهذا في إطار الحذف الروتيني للبيانات التي لم تعد هناك حاجة إليها[١].

٢ – في غالب الأحيان يتم اقتراف الجرائم الإلكترونية عن طريق نقل الاتصالات عبر نظم الحاسوب، ويمكن أن تحتوي هذه الاتصالات على أمور غير مشروعة، مثل مواد إباحية للأطفال أو فيروسات الحاسوب، أو الدليل على ارتكاب جرائم أخرى مثل الاتجار بالمخدرات فتحديد مصدر إرسال هذه الاتصالات يمكن أن تساعد في تحديد هوية مرتكبي الجريمة.

---

(١) هلال آمنة، المرجع السابق، ص٥٩.

٣ – تـأمين الـدليل الإلكترونـي مـن الضـياع، حيـث يـتم نسـخ الاتصـالات ذات المحتوى غير المشروع أو الدليل على نشاط جزائي من قبل مزودي الخدمات، مثل المراسلة الإلكترونية التي تم إرسالها أو استقبالها، ومن ثم يمكن الكشف عن دليل جزائي للجرائم المرتكبة[١].

وقد نص المشرع الأمريكي على هذا الإجراء في القسم (f) (18 U S.C2703) من قانون خصوصية الاتصالات الإلكترونية الأمريكي (ECPA).

أما المشرع الفرنسي فرأى أن هذا الإجراء يُعد اعتداء على حق الخصوصية، واحتراماً منه لحرمة الحياة الخاصة ألزم مزودي الخدمة بمحو البيانات التي تتعلق بالاتصالات الإلكترونية بين مستخدمي هذه الشبكة، وعاقب بالغرامة من يتقاعس عن محو هذه البيانات[٢].

إلا أن القـانون الفرنسـي بـالأمن القـومي والصـادر فـي ٢٠٠١/١١/١٥م، أقـر بمشروعية هذا الإجراء وذلك في حالين: الأول يتعلق بمتطلبات المحاسبة المالية بين مزودي الخدمات والمشتركين في خدماتهم، حيث يقدم مزودو الخدمات لبعض هؤلاء المشتركين بعض الخدمات مدفوعة الأجر، أما الثاني فهو يتعلق باعتبارات التعاون مع القضاء التي تبرر الاحتفاظ بتلك البيانات لمدة لا تزيد عن السنة.

وهذا الاستثناء يؤكد ما ذهب إليه التوجه الأوربي رقم (٥٨) لسنة ٢٠٠٢م، والذي قرر بدوره أنه من حق الدول الأعضاء اتخاذ التدابير اللازمة لحماية الأمن العام والدفاع القومي وأمن الدولة والتدقيق في الجرائم بما يتضمنه ذلك من استثناءات على الحق في الخصوصية، ومن بين هذه الاستثناءات ضرورة التحفظ المعجل على البيانات المعلوماتية المخزنة حفاظاً عليها من التلف والتغيير.

---

(١) هلال آمنة، المرجع السابق، ص٦٠.

(٢) تنص الفقرة الأولى من المادة (٢٣) من قانون البريد والاتصالات الفرنسي على أنه: " يجب على مقدمي خدمة الاتصالات محو وإخفاء أية بيانات تتعلق بالاتصال من اللحظة التي ينتهي بها الاتصال".

وتجدر الإشارة إلى أنه توجد بعض الاستثناءات على التزام مزودي الخدمات بالتعاون مع سلطات التحقيق، حيث يستبعد القانون الفرنسي البيانات التي تحوزها جهات معينة من القاعدة السابقة والتي تفرض واجب التعاون مع رجال العدالة بوجه عام، مثل ما جاء في نص المادة (٣١) في الفقرة الثانية من القانون رقم (٧٨/١٧) الصاد في يناير ١٩٧٨م، الخاص بالمعلوماتية والحريات في فرنسا، حيث تنص هذه المادة على عدم جواز مراقبة المعلومات التي تجمعها الكنائس أو أي تجمعات دينية أو فلسفية أو سياسية، أو نقابية والتي تتعلق بأعضائها أو المتراسلين معها، كما يستثنى أيضاً من هذه القاعدة أنواع معينة من المعلومات نصت عليها المادة (١٨) من قانون الأمن الداخلي الذي عدل قانون الإجراءات الجزائية الفرنسي وأدخل المادة (١/٦٠) الخاصة بالمعلومات التي تكتسي طابع سر المهنة، حيث تنص هذه المادة على أنه: "باستثناء المعلومات التي تُعد من أسرار المهنة التي أوردها القانون، والمتواجدة في الأنظمة المعلوماتية أو أي أجهزة للمعالجة الآلية....."[١].

كما نص على هذا الإجراء قانون مكافحة الجرائم الإلكترونية المصري لسنة ٢٠١٦م، حيث نص في المادة (٢٧) منه بالتحفظ على أدلة الإثبات، وهي متعلقة بمزودي الخدمة الإلكترونية، بإلزامهم بحفظ وتخزين بيانات خط سير الحركة، ووسائل البيانات وذلك لمدة مائة وثمانين يوماً.

وبالتالي نص المشرع المصري على التحفظ على الأدلة وربطه بمدة زمنية معينة محددة وهي ستة أشهر.

كما أن المشرع البحريني نص على هذا الإجراء في قانون تقنية المعلومات البحريني رقم (٦) لعام ٢٠١٤م، حيث جاء في المادة (١/١٢) منه على أن: "للنيابة العامة الحق بأمر أي شخص سواء مزود الخدمة أم غيره بحفظ الأدلة لمدة ٩٠ يوماً قابلة للتجديد، وكذلك الحفاظ على سرية الأدلة وعدم الإفشاء بها".

---

(١) هلال آمنة، المرجع السابق، ص٥٨ – ٥٩.

وأيضاً نص المشرع القطري في المادة (٢١) الفقرة (٤) من القانون رقم (١٤) لسنة ٢٠١٤ م، الخاص بمكافحة الجرائم الإلكترونية، على أنه: " يلتزم مزود الخدمة، وفقاً للإجراءات القانونية المقررة، بالآتي:

٤- الاحتفاظ المؤقت والعاجل ببيانات تقنية المعلومات أو بيانات المرور أو معلومات المحتوى لمدة تسعين يوماً قابلة للتجديد، بناءً على طلب الجهة المختصة أو جهات التحقيق والمحاكمة".

أما المشرع السوري فقد نص في المادة (٨) من قانون مكافحة الجريمة المعلوماتية وتنظيم التواصل عبر الشبكة السوري رقم (١٧) لعام ٢٠١٢م، على أنه: " أ- يعاقب مقدم الخدمات على الشبكة الذي يهمل تنفيذ التزامه بحفظ نسخة من المحتوى لديه وحفظ بيانات الحركة التي تسمح بالتحقق من هوية الأشخاص الذين يسهمون في وضع محتوى على الشبكة بالغرامة من مئة ألف إلى خمسمائة ألف ليرة سورية.

ب-إذا كان الإهمال المشار إليه في الفقرة /أ/ من هذه المادة مقصوداً وأدى إلى عرقلة التحقيق في جريمة أو الشروع فيها أو إلى عدم التمكن من وقف وقوعها تكون العقوبة الحبس من ثلاثة أشهر إلى سنتين والغرامة من مئتي ألف إلى مليون ليرة سورية".

ونستخلص من هذه المادة أن المشرع السوري نص على مشروعية هذا الإجراء وإجازته وذلك بجعله التزاماً عاقب على الإخلال به بعقوبات جزائية.

**لكن نلاحظ أن المشرع السوري في الفقرة (ب) من المادة (٨) السابقة نص على فيما إذا كان الإهمال المشار إليه في الفقرة /أ/ من هذه المادة مقصوداً ونحن بدورنا ننتقد المشرع السوري بالإشارة إلى الإهمال المقصود فهو لم يوفق بهذه العبارة والسبب في ذلك أن الإهمال هو صورة من صور الخطأ ولا يوجد أهمال مقصود.**

أما بالنسبة لبعض الدول، فمن الملاحظ أن التحفظ على البيانات يُعد بالنسبة لها، سلطة قانونية جديدة، فهو إجراء تحقيقي مستحدث في سبيل مكافحة

الجريمة الإلكترونية، كما أنه متماشياً مع البيئة الإلكترونية التي تكون فيها البيانات قابلة للمحو والفقد[١].

**ب – ضمانات مشروعية التحفظ المعجل على البيانات المخزنة:**

يُعد من أهم ضمانات مشروعية التحفظ المعجل على البيانات المخزنة، ما يلي:

**١ – تقييد التحفظ المعجل على البيانات المخزنة بمدة معينة:**

يجب أن يتم تقييد التحفظ المعجل على البيانات المخزنة بفترة معقولة تمكن من الرجوع لمرتكب الجريمة إذا كان هناك عنوان إنترنت[٢].

حيث قيدت اتفاقية بودابست التحفظ المعجل بمدة ٩٠ يوم كحد أقصى، وهذه المدة قابلة للتمديد.

وهي نفس المدة التي أخذ بها المشرع البحريني في قانون تقنية المعلومات البحريني رقم (٦) لعام ٢٠١٤م. في المادة (١/١٢)، وكذلك المشرع القطري في المادة (٢١) الفقرة (٤) من القانون رقم (١٤) لسنة ٢٠١٤ الخاص بمكافحة الجرائم الإلكترونية.

كما تضع بعض التشريعات المقارنة كالقانون الفرنسي التزاماً على مزودي الخدمات بإزالة البيانات التي يتم تخزينها تلقائياً، ويتعلق الأمر بالاتصالات الإلكترونية بين مستعملي شبكة الإنترنت والتي تتعلق بهوية المتصلين وساعة الاتصال بل إن القانون الفرنسي للأمن القومي والصادر في ٢٠٠١/١١/١٥م، أورد عقوبات في حالة عدم قيام مزود الخدمات بمسح تلك البيانات، وهذا احتراماً لحرمة الحياة الخاصة، المادة (L39 - 3) من قانون الأمن القومي. وحتى في حالة كان التحفظ المعجل لاعتبارات التعاون مع القضاء التي تبرر الاحتفاظ بتلك البيانات فقد قيدها مدة لا تزيد عن السنة[٣].

---

(١) هلال آمنة، المرجع السابق، ص٥٨.

(٢) معمر علي إبراهيم محمد، المرجع السابق، ص ٨٤.

(٣) هلال آمنة، المرجع السابق، ص٥٨ – ٥٩.

كما أن المشرع المصري قيد التحفظ على الأدلة وربطه بمدة زمنية معينة محددة وهي ستة أشهر.

وقد أغفل المشرع السوري النص على هذه الضمانة، **ونرى أن تقييد التحفظ المعجل على البيانات المخزنة بمدة معينة يعد من أهم ضمانات مشروعية إجراءه، ونقترح على المشرع السوري الأخذ بهذه الضمانة لما فيها من حماية أكبر لحق خصوصية الفرد.**

**٢ – صدور إذن من الجهة القضائية المختصة:**

لابد من صدور إذن من الجهة القضائية المختصة للاطلاع على هذه البيانات وذلك احتراماً لحق الخصوصية.

وقد نص على هذه الضمانة المشرع القطري في المادة (٢١) الفقرة (٤) من القانون رقم (١٤) لسنة ٢٠١٤ الخاص بمكافحة الجرائم الإلكترونية، عندما نص على أن الاحتفاظ المؤقت والعاجل ببيانات تقنية المعلومات أو بيانات المرور أو معلومات المحتوى، يجب أن يكون بناءً على طلب الجهة المختصة أو جهات التحقيق والمحاكمة.

**ونرى أن في هذه الضمانة فائدة كبيرة لما يحققه من صدور إذن من الجهة القضائية المختصة في عدم الاطلاع على هذه البيانات إلا إذا كان هنالك مبرر له وعدم انتهاك الحق في الخصوصية لأسباب غير جدية.**

**٣– الحفاظ على سرية الأدلة وعدم الإفشاء بها أو الانتفاع منها:**

احتراماً لحق الخصوصية يجب أن تبقى المعلومات المخزنة على الأقراص طي الكتمان حتى تظهر الحاجة إلى استخراج بعض المعلومات منها وذلك بعد صدور إذن خاص من الجهات المختصة.

حيث نص المشرع البحريني على هذه الضمانة في قانون تقنية المعلومات البحريني رقم (٦) لعام ٢٠١٤م، وذلك في المادة (١/١٢) منه، حين فرض التزاماً على الأشخاص أو مزودي الخدمة الذين تكلفهم النيابة العامة بالوصول للأدلة والتحفظ عليها بعدم إفشاء أي سر يتعلق بدليل من أدلة الدعوى أو حتى أخبار المتهم، وأيضاً أي محاولة من قبلهم للانتفاع من هذه الأدلة[١].

## الفرع الثاني

## الأمر بتقديم بيانات معلوماتية عن المشترك

إن دراسة إجراء الأمر بتقديم بيانات معلوماتية عن المشترك، يقتضي أولاً، تعريف هذا الإجراء، وثانياً، بيان مشروعية الأمر بتقديم بيانات معلوماتية عن المشترك.

**أولاً: تعريف الأمر بتقديم بيانات معلوماتية عن المشترك:**

المقصود بهذا الأمر هو: "تمكين السلطة المختصة من إلزام مزودي الخدمة بتقديم بيانات موجودة بحوزتهم أو تحت سيطرتهم تتعلق بالمستخدم".

وقد حددت اتفاقية بودابست المقصود بهذه البيانات بقولها أنها تتعلق بنوع خدمة الاتصال التي اشترك فيها الشخص والوسائل الفنية لتحقيقها، العنوان البريدي أو الجغرافي ورقم هاتف ودخول المشترك للحصول على تلك الخدمة والفواتير التي ترسل إليه، وأي معلومات تتعلق بطريقة الدفع، وأي معلومات أخرى تتعلق بأداء الخدمة أو الاتفاق بين المشترك ومزود الخدمة[٢].

ويمتد الأمر الذي يمكن للسلطة المكلفة بالتحقيق إصداره ليشمل نوعين من البيانات المتعلقة بالمستخدم:

---

(١) أمجد خليل حمودة، المرجع السابق، ص١٣١.

(٢) هلال آمنة، المرجع السابق، ص٦١.

**أ-البيانات المتعلقة بالمرور[١]:**

وهي التي تكون في الغالب في حيازة مزود الخدمة فقط، والمقصود بهذا النوع من البيانات تلك التي تعالج الاتصالات التي تمر من خلال نظام معلوماتي، فتحدد الاتصال ومقصده وسيره وتاريخه ووقته، ويتضمن هذا النوع من البيانات (بيانات المرور المتعلقة باتصالات سابقة)، حيث إنه من خلال هذه البيانات يمكن تحديد خط سير الاتصال فيتيح إمكانية تحديد هوية من ساهم في ارتكاب الجريمة محل التحقيق.

**ب- البيانات المتعلقة بمحتوى الاتصال:**

المقصود بها مضمون المعلومات المنقولة عن طريق الاتصال الإلكتروني.

وليس هناك اختلاف جوهري بين هذين النوعين من البيانات من ناحية المضمون، وإنما يتمثل الاختلاف بينهما في درجة تعلق كل منهما بحماية الحق في الخصوصية.

**ثانياً: مشروعية الأمر بتقديم بيانات معلوماتية عن المشترك:**

إن دراسة مشروعية الأمر بتقديم بيانات معلوماتية عن المشترك، يقتضي بيان الأساس القانوني له، وكذلك بيان ضمانات مشروعية إجراءه.

**أ-الأساس القانوني لمشروعية الأمر بتقديم بيانات معلوماتية عن المشترك:**

الأصل أن البيانات الشخصية التي تخص مستخدمي الشبكات تدخل في إطار الحق في الخصوصية الذي تحميه الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية الصادر في ١٩٥٠/١١/٤م، وبالتالي لا يجوز لمزود الخدمات أو غيره إفشاء ما لديهم من معلومات إلى الغير.

---

(١) حددت المادة (١) فقرة (د) من اتفاقية بودابست لعام ٢٠٠١م، بيانات المرور على أنها: " أي بيانات كومبيوتر متعلقة باتصال عن طريق منظومة كومبيوتر، والتي تنشأ من منظومة كومبيوتر تشكل جزءاً من سلسلة الاتصالات، توضح مصدر الاتصال، والوجهة المرسلة إليها، والطريق الذي تسلكه، ووقته وتاريخه، وحجمه، ومدة وقوع الخدمة المذكورة ".

لكـن جـاء فـي توصـية المجلـس الأوربـي رقـم ر (٩٥) ١٣ فـي ٩/١١/ ١٩٩٥م أنـه مـع احتـرام الحصـانات والامتيـازات المقـررة قانونـاً تجيـز القـوانين الإجرائيـة توجيـه أوامـر لمـن يحـوز أشـياء تفيـد فـي الكشـف عـن الحقيقـة بتسـليمها، ولـذلك يتعـين تعـديل القـوانين الإجرائيـة بإصـدار مثـل هـذه الأوامـر لمـن يحـوز معلومات (برامج – قواعد – بيانات) تتعلق بأجهزة الحاسوب بتسليمها للكشف عن الحقيقة.

كما يتعين ومع احترام الحصانات والضمانات المقررة قانوناً إعطاء سلطات التحقيق سلطة توجيه أوامر لمن يكون لديه معلومات خاصة للدخول على نظام من أنظمة المعلومات أو للدخول على ما يحويه من معلومات باتخاذ اللازم للسماح لرجال التحقيق بالاطلاع عليها. وأن تخول سلطات التحقيق بإصدار أوامر لأي شخص آخر لديه معلومات عن طريقة التشغيل والمحافظة على المعلومات [١].

كما أن بعض التشريعات المقارنة تسمح لأعضاء الضابطة العدلية أن يأمروا الأشخاص بتسليم ما تحت أيديهم من موضوعات والتي يُطلب تقديمها كدليل، ومن بينها البيانات المتعلقة بالشخص المشترك في الجريمة، والتي يحوزها مزودو الخدمات، وهذا الأخير يلزمه القانون الفرنسي رقم (٧١٩) لسنة ٢٠٠٠م، المعدل للقانون (١٠٦٧) لسنة ١٩٨٦م، الخاص بحرية الاتصالات، حيث تنص المادة (٩/٤٣) من هذا القانون على أنه: "يتعين على مزودي خدمات الدخول المحافظة على بيانات مستعملي خدماتهم وذلك تمهيداً لطلب السلطات منهم تلك البيانات التي قد تفيد كدليل في جريمة معينة وقعت بالفعل"[٢].

أما فيما يتعلق بالقانون الأمريكي فإنه في قانون خصوصية الاتصالات الإلكترونية (ECPA) أجاز لأعضاء الضابطة العدلية، وهذا في إطار ما يقومون

---

(١) د. مدحت رمضان، المرجع السابق، ص٨١ – ٨٢.

(٢) هلال آمنة، المرجع السابق، ص٦٠.

بـه مـن جمـع المعلومـات الاطـلاع علـى البيانـات الموجـودة فـي حـوزة مـزودي الخدمات، والتي تخص مستخدمي شبكة الإنترنت وذلك من خلال توجيه تكليف إلى مزود الخدمات بتقديم تلك المعلومات، وهذه المعلومات تتمثل في ثلاث أنواع: حيث يتمثل النوع الأول في المعلومات الشخصية الخاصة بالمشترك مثل اسمه ورقم هاتفه وعنوانه، والنوع الثاني هو المعلومات الشخصية الخاصة بالمتعامل مع المشترك، أي كل من يتصل به، أو يدخل معه في صفقة مثلاً، وبالنسبة للنوع لثالث فهو المعلومات المتعلقة بمحتوى البيانات، كمضمون المحادثات ومضمون الملفات(١).

وهناك قوانين لا تجيز إصدار مثل هذا الأمر لأعضاء الضابطة العدلية وإنما تجيزه لسلطة التحقيق، مثل القانون المصري، حيث جاء في نص المادة (٩٩) من قانون الإجراءات الجنائية المصري على أنه: "لقاضي التحقيق أن يأمر الحائز لشيء يرى ضبطه أو الاطلاع عليه بتقديمه، ويسري حكم المادة (٢٤٧) على من يخالف ذلك الأمر.....".

ولا تختلف سلطة النيابة العامة في ذلك عن سلطة التحقيق، كما أن للمحكمة أن تصدر مثل هذا الأمر وفقاً للقانون المصري، وتنص المادة (٢٩١) من القانون نفسه على: "للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازماً لظهور الحقيقة"(٢).

أما فيما يتعلق باتفاقية بودابست فقد نصت في المادة (١٨) منها على أنه: "يجوز تمكين السلطات المختصة من إلزام مقدمي الخدمات إعطاء البيانات المتعلقة بالمشترك، سواء كانت في حيازته المادية أو تحت سيطرته، ويشترط في

---

(١) د.عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي (المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية)، المرجع السابق، ص٢٧١ .

(٢) هلال آمنة، المرجع السابق، ص٦١.

هذه البيانات أن تكون مخزنة، وبالتالي فإنه لا يدخل فيها أي معلومات متعلقة بحركة ومحتوى البيانات ذات العلاقة باتصالات مستقبلية".

وأيضاً نص المشرع القطري في المادة (٢١) الفقرة (١) و (٣) من القانون رقم (١٤) لسنة ٢٠١٤ الخاص بمكافحة الجرائم الإلكترونية، على أنه: "يلتزم مزود الخدمة، وفقاً للإجراءات القانونية المقررة، بالآتي:

١-تزويد الجهة المختصة، أو جهات التحقيق والمحاكمة، بجميع البيانات والمعلومات اللازمة التي تساعد في كشف الحقيقة، بناءً على أمر من النيابة العامة.

٣-الاحتفاظ بمعلومات المشترك لمدة سنة".

وفي القانون السوري فقد نصت المادة (١١) من قانون مكافحة الجريمة المعلوماتية وتنظيم التواصل عبر الشبكة السوري رقم (١٧) لعام ٢٠١٢م، تحت عنوان الامتناع عن إجابة أمر السلطة القضائية على ما يلي: " يعاقب مقدم الخدمات على الشبكة الذي يمتنع عن إجابة أمر السلطة القضائية بسحب أي جزء من المحتوى المخزن لديه من التداول أو بمنع الوصول إليه بالعقوبة المنصوص عليها على جرائم الامتناع عن تنفيذ قرار السلطة القضائية".

ومن هذا النص نستنتج أن المشرع السوري قد إجاز هذا الإجراء واعترف بمشروعيته وعاقب على عدم تنفيذ الأمر من قبل مقدم الخدمات بعقوبات جزائية.

**ب- ضمانات مشروعية الأمر بتقديم بيانات معلوماتية عن المشترك:**

يُعد من أهم ضمانات مشروعية الأمر بتقديم بيانات معلوماتية عن المشترك، الآتي:

**١- أن يتخذ هذا الإجراء في الجرائم الجسيمة:**

من ناحية الجرائم التي يجوز من أجل مكافحتها اتخاذ هذا الإجراء فإنه يجب حصرها في أشد الجرائم جسامة.

ونرى أنه يجب قصر هذا الإجراء على الجنايات والجنح فقط دون المخالفات نظراً لبساطتها والتي لا تبرر انتهاك خصوصية الأفراد.

**٢- تحديد السلطة المختصة للقيام بهذا الإجراء:**

أكدت اتفاقية بودابست في المادة (١٨) منها على ضرورة تحديد السلطة المختصة بإصدار أمر تقديم البيانات، حيث يسمح لرجال السلطة العامة بإصدار مثل هذا الأمر إذا تعلق الأمر ببيانات المشترك المعلنة للجمهور، في حين أن هناك دول تشترط أن يكون هذا الأمر صادراً فقط من السلطات القضائية كالتشريع السوري في المادة (١١) من قانون مكافحة الجريمة المعلوماتية وتنظيم التواصل عبر الشبكة السوري رقم (١٧) لعام ٢٠١٢م، ولاسيما عند الحصول على نوع معين من البيانات المتعلقة بالحق في الخصوصية مثل رقم بطاقة الائتمان، أو حساب بنكي للمشترك.

**ونحن نرى أنه يجب التمييز بين البيانات المتعلقة بالمرور والبيانات المتعلقة بمحتوى الاتصال، فالبيانات المتعلقة بمحتوى الاتصال أكثر أهمية بالنسبة للحق بالخصوصية من البيانات المتعلقة بالمرور، الأمر الذي يستدعي إحاطتها بضمانات أكبر، فلا يكفي أن تناط هذه السلطة بأعضاء الضابطة العدلية، وإنما يجب أن توكل للسلطة القضائية.**

**وفي نهاية بحث الحصول على الدليل الإلكتروني في الإجراءات المتعلقة بالبيانات الساكنة، نرى أنه لا يجوز إنكار دور الإجراءات المتعلقة بالبيانات الساكنة في الحصول على الدليل الإلكتروني، لكن بالمقابل يجب إحاطة هذه الإجراءات بضمانات معينة تكفل مشروعية الدليل الإلكتروني وأهم هذه الضمانات، وقوع جريمة معينة وأن تكون هذه الجريمة من نوع الجناية والجنحة فقط دون المخالفات، والاشتباه بالمدعى عليه أنه مرتكب الجريمة، وإعطاء هذه السلطة لسلطة التحقيق فقط دون غيرها لخطورة هذا الإجراء.**

# المطلب الثاني
# مشروعية الحصول على الدليل الإلكتروني في الإجراءات المتعلقة بالبيانات المتحركة

يقصد بالإجراءات المتعلقة بالبيانات المتحركة المراقبة الإلكترونية، ويمكن تعريف المراقبة الإلكترونية بأنها: "ذلك العمل الذي يقوم به المراقب، باستخدام التقنية الإلكترونية، لجمع المعلومات عن المشتبه به، سواء أكان شخصاً أم مكاناً أم شيئاً، وذلك لتحقيق غرض أمني"(١).

وإن المراقبة الإلكترونية تتم من خلال التنصت أو مراقبة المكالمات الهاتفية أو المراقبة الإلكترونية على شبكات الإنترنت(٢)، وإن دراسة إجراء التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية للحصول على الدليل يقتضي بيان ماهية التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية، وثانياً مشروعية التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية كإجراء للحصول على الدليل الإلكتروني، وذلك في الفرعين التاليين:

**الفرع الأول: ماهية التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية.**

**الفرع الثاني: مشروعية التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية.**

---

(١) د. محمد طارق الخن، المرجع السابق، ص١٠٠.

(٢) ومع ذلك يعتبر البعض عملية المراقبة أو التنصت على المكالمات الهاتفية نوعاً من التسجيل تتم بطريقة غير مباشرة عبر الأسلاك الهاتفية، كما يعتبر التسجيل والمراقبة وسيلتين متلازمتين تستخدمان في مجال كشف الجريمة. انظر: كوثر أحمد خالند، المرجع السابق، ص٢١٩.

## الفرع الأول

## ماهية التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية

لابد لنا من دراسة أولاً، ماهية التنصت أو الاعتراض على المكالمات الهاتفية، وثانياً، ماهية التنصت أو الاعتراض على المكالمات الإلكترونية.

**أولاً: ماهية التنصت أو الاعتراض على المكالمات الهاتفية:**

إن التنصت السري يعني أن المحادثات الصادرة من هاتف معين أو إليه أو أي عنوان هاتفي آخر، ينصت إليه بشكل سري أو يلتقط باستخدام وسائل تقنية مساعدة من أجل الحصول على محتويات تلك المكالمات موضوع المراقبة(١).

ويتم التنصت عادة باستخدام ميكروفونات مخفية عندما تكون الشرطة بحاجة إلى استخدام هذه الوسائل – ضمن الحدود القانونية – للكشف عن بعض الجرائم خاصة المنظمة منها، كجرائم المخدرات والجرائم المنظمة ضد أمن الدولة، ومن أجهزة التنصت الاعتيادية المعتمدة من قبل الشرطة في العالم ميكروفونات صغيرة الحجم مرتبطة بسلك رفيع متصل بمسجل صغير الحجم أيضاً، بحيث تستخدمها الشرطة وتتكلم مع المشتبه به ويسجل صوته مثلاً دون أن تكشف الشرطة عن هويتها لغرض إلقاء القبض على ذلك الشخص واستخدام المكالمة المسجلة في الإثبات(٢).

ومن الجدير بالذكر أن التنصت على المكالمات الهاتفية وتسجيلها قد لا يتطلب اتصالاً فعلياً بالخط الهاتفي المراد مراقبته، لأنه يكون هناك مجال كهربائي كافٍ حول الخط يسهل عملية التقاط المحادثات، كما قد لا يتطلب الدخول إلى المسكن أو المكان المراقب لغرض وضع بعض أجهزة المراقبة والتسجيل، إذ من الممكن وضع أجهزة دقيقة معدة لهذا الغرض تثبت خارج جدران المكان المراقب،

---

(١) كوثر أحمد خالند، المرجع السابق، ص٢٢٠.

(2) Frank J. Donner; The age of Surveillance, Washington, DC, 1981, P.110 - 112.

كما أن هناك من الأجهزة ما يمكن دسها في ملابس الشخص المراقب دون علمه[١].

وتختلف مراقبة المكالمات الهاتفية عن التسجيل الصوتي، في أن الأولى تتم دائماً خلسة وبصورة سرية ودون علم الأشخاص المراد مراقبتهم، كما تتميز المراقبة بخاصية أخرى وهي أن تسجيل المكالمات الهاتفية من خلال عملية المراقبة أو التنصت لا يقتصر على أحاديث الشخص المتهم فحسب، بل يتعدى ذلك إلى الطرف الآخر الذي يبادله الحديث أيضاً[٢].

ويؤخذ على استراق السمع أو التنصت على المحادثات الهاتفية، أنه لا يوجد ما يؤكد صدور الحديث عن الشخص المراقب، ولا سيما إذا كانت الأصوات تتشابه، كما أنه من السهل أن يستعمل الغير هاتف المشتبه به في غيبته مثلاً، ويزعم بأنه المشتبه به، وعليه يجب الحذر في قبول الدليل الذي يتم الحصول عليه عن طريق مراقبة المحادثات الهاتفية لما يشوبه من شكوك، إلا إذا أقر المشتبه به بصحة محتوى المراقبة أو التسجيل[٣].

وتتبنى التشريعات الجزائية معيارين لتحديد خصوصية المكالمة الهاتفية وتسجيل المحادثات الشخصية، وهما: معيار طبيعة المكان ومعيار طبيعة الكلام بحيث تمد التشريعات التي تأخذ بالمعيار الأول حمايتها للأحاديث التي تتم في الأماكن الخاصة فقط، دون الاعتبار لطبيعة المكالمات الهاتفية أو الأحاديث الشخصية، ومنها ما توفر الحماية معتمدة على طبيعة الحديث من حيث عدها من قبيل الخصوصية أو العلانية دون الاهتمام بالمكان الذي يجري فيه ذلك الحديث[٤].

---

(١) كوثر أحمد خالند، المرجع السابق، ص٢٢٠.
(٢) كوثر أحمد خالند، المرجع السابق، ص٢٢٠ – ٢٢١.
(٣) كوثر أحمد خالند، المرجع السابق، ص٢٢١.
(٤) كوثر أحمد خالند، المرجع السابق، ص٢٣٦ – ٢٣٧.

وينتقد البعض[١] موقف التشريعات التي تأخذ بمعيار خصوصية المكان، **ونحن نؤيد هذا الانتقاد لأن معيار طبيعة المكان من حيث كونه مكاناً خاصاً يصح الاستناد إليه في حالة حرمة المساكن والمحلات الخاصة، في حين حرمة المحادثات ينبغي أن تصان سواءً أكانت في مكان خاص أم عام، وأن المحادثات الهاتفية هي بطبيعتها سرية، ولها خصوصية بصرف النظر عن المكان الذي يجري فيه الحديث الهاتفي.**

**ثانياً: ماهية التنصت أو الاعتراض على المكالمات الإلكترونية:**

إن بحث ماهية التنصت أو الاعتراض على المكالمات الإلكترونية، يقتضي تعريف هذا الإجراء ومحله وكذلك الآلية المتبعة لإجرائه.

**أ- تعريف التنصت أو الاعتراض على المكالمات الإلكترونية[٢]:**

التنصت أو الاعتراض على المكالمات الإلكترونية والذي يطلق عليه أيضاً بالاعتراض الإلكتروني هو إجراء يتعلق بالبيانات المتحركة وإجراءاتها ويُعرَّف بأنه: "اعتراض الاتصالات الإلكترونية الخاصة، والمقصود بهذا الإجراء مراقبة الاتصالات الإلكترونية أثناء بثها، أي في الزمن الفعلي لنقلها بين الأطراف"[٣].

حيث أن من أهم خصائص الإنترنت أنه يسهل مراقبته، فالمعلومات تنتقل من خلال أجهزة الحاسوب التي تتصل ببعضها البعض عن طريق الخادم ضمن شبكة الإنترنت، وبالتالي فإن كل جهاز أو موقع يسهل متابعته ومراقبته من أي جهاز مرتبط بالإنترنت[٤].

---

(١) د. عوض محمد، الوجيز في قانون الإجراءات الجنائية، ج١، د.ط، دار المطبوعات الجامعية، الإسكندرية، مصر، بلا تاريخ ، ص٣١١.

(٢) يسمى الاعتراض الإلكتروني أيضاً بـ "التقصي الإلكتروني" أو "اعتراض المراسلات".

(٣) هلال آمنة، المرجع السابق، ص٦٢.

(٤) خالد عياد الحلبي، المرجع السابق، ص٥٣.

**ب- محل التنصت أو الاعتراض على المكالمات الإلكترونية:**

ميزت اتفاقية بودابست بين نوعين من البيانات المعلوماتية محل التنصت أو الاعتراض على المكالمات الإلكترونية وهما: البيانات المتعلقة بالمرور والبيانات المتعلقة بمحتوى الاتصال [١]، لذلك لابد لنا من دراسة هذين النوعين من البيانات.

**النوع الأول: البيانات المتعلقة بالمرور:**

عرفت المادة الأولى من اتفاقية بودابست البيانات المتعلقة بالمرور بأنها: "كل البيانات التي تعالج الاتصالات التي تمر عن طريق نظام معلوماتي، والتي يتم إنتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصراً في سلسلة الاتصال، مع تعيين المعلومات الخاصة بأصل الاتصال، مقصد الاتصال أو الجهة التي تقصد من الاتصال، خط السير، الساعة والتاريخ، حجم وفترة الاتصال، نوع الخدمة".

**النوع الثاني: البيانات المتعلقة بمحتوى الاتصال:**

إن الاتفاقية لم تورد تعريفاً لها، ولكنها تشير إلى المحتوى الإخباري للاتصال، يعني مضمون الاتصال أو الرسالة أو المعلومات المنقولة عن طريق الاتصال، فيما عدا البيانات المتعلقة بالمرور.

وهناك من يلاحظ أن هناك تقارباً في المعنى بين كلا النوعين، إلا أنهما مختلفان تماماً من حيث درجة المساس بالحق في الخصوصية، حيث يكون ذلك أكثر أهمية بالنسبة لمراقبة محتوى الاتصال أو المراسلة، ومن ثم تفرض ضمانات أكبر عند 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.

---

(١) وقد أكدت اتفاقية بودابست هذا التمييز حيث أدرجت كل إجراء على حدا تحت عنوان خاص فخصت تجميع حركة البيانات بعنوان" التجميع في الزمن لبيانات المرور" في المادة (٢٠) أما تجميع محتوى البيانات فجاء تحت عنوان "اعتراض محتوى البيانات" في المادة (٢١).

وعلى العكس تضع بعض الدول مفهوماً موحداً لكل من تجميع حركة البيانات ومراقبة محتوى البيانات الإلكترونية، ومن ثم تسري عليهما نفس الضمانات الخاصة عند اتخاذ أحد الإجراءات، دون الأخذ في الحسبان الحساسية التي تحيط بموضوع مراقبة محتوى البيانات، ويرجع ذلك إلى عدم وجود تمييز في القانون الذي لا يوجد فيه اختلافات حول المصلحة في الخصوصية أو لتشابه إجراءات التجميع التقني، ومن هذه الدول فرنسا(١).

وفي إطار تحديد محل المراقبة الإلكترونية ثارت مشكلة تحديد طبيعة البريد الإلكتروني غير المفتوح والمنتظر في صندوق خطابات مقدم خدمات الإنترنت **فهل يجب اعتبارها اتصالات إلكترونية مخزنة أم اتصالات إلكترونية متحركة وبالتالي تطبق عليها الإجراءات المتعلقة بالبيانات المتحركة والمتمثلة في اعتراض الاتصالات الإلكترونية، ومن ثم لا يتم الحصول عليها إلا عن طريق سلطة الاعتراض؟** وحسم المشرع الأمريكي هذا الأمر، وعد الاتصالات الإلكترونية المخزنة من قبيل البيانات الساكنة، وبالتالي تطبق عليها كل الإجراءات التي تتناسب مع هذا النوع من البيانات من تفتيش والأمر بالتحفظ العاجل بدليل أنه قام بتعديل القسم (2703) من قانون خصوصية الاتصالات الإلكترونية (ECPA)، ليشمل حماية الاتصالات الإلكترونية المخزنة من البريد الإلكتروني والرسائل الصوتية غير المفتوحة والمخزنة لدى مزود الخدمة(٢).

وقد تم تأكيد هذه القاعدة في العديد من التطبيقات مثل ( United States v.Smith) حيث قرر القضاء الأمريكي بأنه لا يمكن مراقبة الاتصالات السلكية وهي في حالة التخزين الإلكتروني(٣).

---

(١) عائشة بن قارة مصطفى، المرجع السابق، ص١٦٥ – ١٦٧.

(٢) هلال آمنة، المرجع السابق، ص٦٢.

(٣) عائشة بن قارة مصطفى، المرجع السابق، ص١٦٥ – ١٦٧.

وحدد الأمر الفرنسي الدوري الصادر في ١٩٨٨/٢/١٧ المراسلات الخاصة بأنها تلك الموجهة لشخص أو أكثر من الأشخاص الطبيعية أو المعنوية المحددين سلفاً، وأعطى أمثلة على ذلك رسائل العمل داخل مؤسسة أو إدارة أو منشأة مهنية والمراسلة للعاملين فقط. ويُعد من قبيل المراسلات الخاصة تلك الخدمات التي تقوم بنقل المراسلات الخاصة بين الأشخاص كصناديق البريد الإلكترونية أو بين المتعاملين ومقدمي الخدمة والعمليات الخاصة بالمعاملات البنكية والمعاملات الخاصة بإنهاء اتفاقات تجارية أو إنهاء أوراق إدارية، وعادة ما توجد رابطة تعاقدية بين الخدمة والمتعاملين معها ومن مظاهرها توفير الاتصال واستخدام شفرة خاصة للاتصال(١).

**جـ- الآلية المستخدمة في التنصت أو الاعتراض على المكالمات الإلكترونية:**

إن السؤال الذي يطرح نفسه هو: **ما هي التقنية المستخدمة في التنصت أو الاعتراض على المكالمات الإلكترونية؟**

في الحقيقة تعددت التقنيات المستخدمة في مجال التنصت أو الاعتراض على المكالمات الإلكترونية، فهناك برامج مخصصة لفحص الرسائل الإلكترونية الصادرة والواردة، وبرامج تقوم باستعادة الرسائل التي تمّ إلغاؤها أو محوها، وأخرى تقوم بتعقب المواقع الإباحية، وغير ذلك من هذه البرمجيات. وسنتناول فيما يلي أبرز أنواع هذه البرمجيات:

**- تقنية برنامج "كارنيفور" للتنصت على البريد الإلكتروني:**

طورت إدارة تكنولوجيا المعلومات التابعة لمكتب التحقيقات الفيدرالي FBI، برنامج أطلق عليه اسم "كارنيفور"، حيث يقوم هذا البرنامج بتعقب وفحص رسائل البريد الإلكتروني الصادرة والواردة عبر المخدمات المستخدمة من قبل مزودي

(1) HUET PIERRE, Les services multimédia, AFTEL, Le droit du multimédia de la télématique à l'internet ; sous la direction de PIERRE HUET avec le concours de H. MAISL, A. LUCAS, éd. 1996,. pp14.

مشار إليه لدى: د. مدحت رمضان، المرجع السابق، ص٧٦ – ٧٧.

خدمة الإنترنت، فيما إذا كان هناك اشتباه بأن هذه الرسائل تحمل معلومات عن جرائم أو حوادث جرمية. هذا البرنامج يقوم بفحص وتسجيل الرسائل التي تحتوي على كلمات أو معلومات يشتبه في أن لها علاقة بالجرائم، ويتجاهل الرسائل الأخرى(١).

**- برامج استعادة الوثائق الإلكترونية الممحاة:**

في عام ١٩٨٨م، أسس الأمريكي "جون جيسين" شركة تدعى "اكتشاف الأدلة أو القرائن الإلكترونية". وقد اتجهت هذه الشركة لتسهيل عملها في البحث والتحري نحو الوثائق الإلكترونية، باعتبار أن هذه الوثائق تترك وراءها أثراً لا يُمحى، ويمكن استعادتها مهما اجتهد الفاعل في محوها، وذلك على عكس الوثائق الورقية التي تتحول إلى مادة يصعب استرجاع المعلومات منها بعد حرقها أو تمزيقها.

ومن أشهر القضايا الذي اعتمدت على هذا الأسلوب، القضية التي رفعتها وزارة العدل الأمريكية وتسع عشرة ولاية ضد شركة مايكروسوفت، لمحاولتها احتكار أنظمة تصفح الإنترنت. فبعد البحث في نظام البريد الإلكتروني العائد لهذه الشركة، تم اكتشاف رسائل إلكترونية تتعلق بمحاولة الإضرار بالمنافسين التجاريين، التي اعتقد أصحابها أنهم قاموا بمحوها. ومن أشهر الرسائل الممحاة التي استخدمت في هذه القضية، الرسالة التي سأل فيها رئيس مايكروسوفت عدداً من كبار الموظفين في شركته عمّا إذا كان لديهم خطة تتعلق بما يمكن فعله من أجل إلحاق الضرر بالخصوم التجاريين(٢).

---

(١) د.مصطفى محمد موسى، دليل التحري عبر شبكة الإنترنت، الطبعة الأولى، دار الكتب القانونية، القاهرة، مصر، بلا تاريخ، ص١٨٩. د. محمد طارق الخن، المرجع السابق، ص١٠١.

(٢) د. مصطفى محمد موسى، دليل التحري عبر شبكة الإنترنت، المرجع السابق، ص١٩٣ - ١٩٤.

**- برنامج مراقبة البريد الإلكتروني:**

وهو برنامج صمّمه المبرمج الأمريكي "ريتشارد إتوني"، حيث يقوم هذا البرنامج بسبر محتوى البريد الإلكتروني موضوع المراقبة، وقراءة الرسائل التي قام صاحبها بإتلافها، أو تلك التي لم يقم بتخزينها أصلاً، ويمكن تحميل هذا البرنامج على أي جهاز حاسوب بهدف مراقبة بريده الإلكتروني. وقد استخدمت المخابرات الأمريكية هذا البرنامج لكشف مشتبه به من الجنسية الروسية حاول اختراق بعض المواقع على شبكة الإنترنت(١).

ومن الأمثلة الشهيرة للمراقبة الإلكترونية عن طريق مراقبة البريد الإلكتروني، أنه تمّ الكشف عن العلاقة الغرامية بين الرئيس الأمريكي السابق "بيل كلينتون" والآنسة "مونيكا لوينسكي"، عن طريق مراقبة البريد الإلكتروني لهما(٢).

**- برنامج تعقب المواقع الإباحية:**

ويُعرَّف هذا البرنامج باسم "نوبد شرطة الإنترنت" وهو يقوم بالبحث عن الصور الجنسية المخلّة بالأخلاق في أنظمة الحواسيب التي تعمل وفق برنامج تشغيل ويندوز بإصداراته الحديثة، ثم يقوم بتبليغ الهيئات الحكومية عنها، بهدف تطهير شبكة الإنترنت من هذه المواقع والصور(٣).

---

(١) د. مصطفى محمد موسى، المرجع السابق، ص٢١٦. د. محمد طارق الخن، المرجع السابق، ص١٠١ - ١٠٢.

(٢) د. محمد طارق الخن، المرجع السابق، ص١٠٢.

(٣) د. مصطفى محمد موسى ، المرجع السابق ص٢١٧. د. محمد طارق الخن، المرجع السابق، ص١٠٢.

## الفرع الثاني

## مشروعية التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية

لابد من دراسة أولاً، الأساس القانوني لمشروعية التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية، وثانياً، دراسة ضمانات مشروعية التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية.

### أولاً: الأساس القانوني لمشروعية التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية:

سندرس الأساس القانوني لمشروعية التنصت أو الاعتراض على المكالمات الهاتفية، ومن ثم الأساس القانوني لمشروعية التنصت أو الاعتراض على المكالمات الإلكترونية.

### أ- الأساس القانوني لمشروعية التنصت أو الاعتراض على المكالمات الهاتفية:

هناك من يرى[١] أنه لا يجوز استخدام وسيلة إثبات تنافي الأخلاق السليمة كالتنصت على الهاتف، والمذياع السري.

لأن مراقبة المحادثات الهاتفية تتم دون علم الإنسان وتتيح سماع وتسجيل أدق أسرار حياته الخاصة[٢].

إلا أن الرأي السائد هو مشروعية اعتراض المحادثات الهاتفية، لأن الغرض من مشروعية المراقبة هي تحقيق نوع من التوازن بين حق الافراد في الخصوصية والسرية وحق المجتمع في مكافحة الجريمة بوسائل فعالة ليعيش أمناً ومطمئناً[٣].

---

(١) معمر علي إبراهيم محمد، المرجع السابق، ص ٤٤.

(٢) د. علي حسن محمد طوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص ١٥٤.

(٣) د. علي حسن محمد طوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص ١٥٤.

وبالنسبة لموقف التشريعات، فقد إجاز قانون الإجراءات الجنائية الفرنسي مراقبة الاتصالات الخاصة بخصوص تحقيق قضائي على أن تكون الجريمة على درجة جسيمة من الخطورة وتكون كذلك عندما تكون العقوبة المقررة لها الحبس لمدة سنتين أو أكثر (المادة ١٠٠ من قانون الإجراءات الجنائية الفرنسي). ووضع أجهزة المراقبة يتعين أن يكون من قبل أشخاص مؤهلين من العاملين بمرفق الاتصالات العام. ويجب ألا تزيد المراقبة في جميع الأحوال على أربعة أشهر قابلة للتجديد[١].

كما أن القانون الفرنسي الصادر في ١٠ يوليو ١٩٩١م، في شأن الاتصالات يجيز اعتراض الاتصالات البعدية (télématique) [٢]، في حالة المراقبة الإدارية على الاتصالات الخاصة[٣]، فقد حدد المشرع الفرنسي حالاتها على سبيل الحصر بالمادة الثالثة من قانون ١٠ يوليو لعام ١٩٩١ بشأن سرية المراسلات فلا تجوز المراقبة إلا للبحث عن معلومات تتعلق بالأمن القومي والمحافظة على المركز العلمي والاقتصادي لفرنسا ولمكافحة الإرهاب والجريمة المنظمة وإعادة تنظيم الجماعات التي تم حلها بمقتضى قانون عام ١٩٣٦ بشأن جماعات القتال والفرق الخاصة، كما تستهدف التجارة غير المشروعة بالمخدرات، وتجارة السلاح وتزييف العملة والمتاجرة في العنصر البشري. ويقدر رئيس الوزراء حدود المراقبة الأمنية بناء على توصية مكتوبة ومسببة من قبل وزير الدفاع أو وزير الداخلية أو وزير الجمارك، ويقوم هؤلاء جميعاً بمباشرة هذا الاختصاص بأنفسهم ولا يجوز لهم تفويض الغير في مباشرته إلا لأثنين

---

(1) BENSOUSSAN ALAIN: Internet. Aspects juridiques, memento - guide, hermes, 1996, pp.89.

د. مدحت رمضان، المرجع السابق، ص٧٨.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص ٣٨٣.

(٣) يطلق على هذه المراقبة "بالمراقبة الأمنية Interceptions de sécurité".

من معاونيهم، ويتعين إعدام متعلقات التسجيلات والمراقبة بانتهاء الغرض منها، ولقد أنشأ قانون ١٩٩١ لجنة تسمى باللجنة القومية لمراقبة التسجيلات الأمنية (Commission nationale de contrôle des interceptions de sécurité)، وتتكون اللجنة من ثلاثة أعضاء، ويتولى تعيين رئيسها رئيس الجمهورية ويتولى تعيين عضو من النواب من قبل رئيس مجلس النواب ويعين عضو آخر من أعضاء مجلس الشيوخ من قبل رئيس المجلس وتنعقد هذه اللجنة بناء على دعوة من رئيسها، ويجوز لها أن تتصدى من تلقاء نفسها أو بناء على طلب من أصحاب المصلحة للتأكد من أن أعمال المراقبة تتم في إطار القانون، وكل المعلومات التي تصل للجنة تعد سرية، وتقوم كل عام بنشر تقرير عن نشاطها[1].

كما أن المشرع الجزائري إجاز المراقبة المحادثات الهاتفية في التعديل الأخير لقانون الإجراءات الجزائية بالقانون ٢٢/٦ المؤرخ في ٢٠٠٦/١٢/٢٠م، في نص المادة (١٤)، المتممة للباب الثاني من الكتاب الأول من الأمر رقم ١٥٥/٦٦، في الفصل الرابع تحت عنوان "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور"، في المواد من (٦٥ مكرر ٥ إلى ٦٥مكرر ١٠).

وفي التشريع السوري نصت المادة (٩٦) من قانون أصول المحاكمات الجزائية السوري على إعطاء الحق لقاضي التحقيق بمراقبة المحادثات الهاتفية متى كان لذلك فائدة في ظهور الحقيقة.

وإذا أخذنا عبارة (الفائدة من ظهور الحقيقة) بالمعنى الواسع، أي بالمعنى الذي يفيد المصلحة العامة، فالمصلحة العامة تقتضي بالسماح بمراقبة المحادثات الهاتفية لاسيما في الجرائم الإلكترونية ومنها جرائم الاتصالات التي تتميز

---

(1) BENSOUSSAN ALAIN:op, cit, .p.89.

د. مدحت رمضان، المرجع السابق، ص٧٨ – ٧٩.

بصعوبة إثباتها وطبيعتها الخاصة والتي تختلف عن الجرائم التقليدية، لأن هذه المراقبة تحقق فائدتين:

الفائدة الأولى: تتمثل في المساعدة في كشف الجريمة.
الفائدة الثانية: هي تشكيل حماية وقائية مسبقة في هذا النوع من الجرائم.

**ب- الأساس القانوني لمشروعية التنصت أو الاعتراض على المكالمات الإلكترونية:**

إن امتداد الأمر إلى حد التقاط الاتصالات التي تتم عبر الإنترنت، أفقد الإنسان حريته وخصوصيته، ما جعل الفقهاء يقولون بأن أجهزة المراقبة السمعية تعد نكسة للتقدم المذهل للتقنيات الحديثة(١).

حيث إن المشرع يعطي الحماية القانونية لهذا النوع من الاتصالات الإلكترونية عبر الإنترنت، بغية حماية الحياة الخاصة للأشخاص، وهذا عن طريق حماية مستودع أسرارهم، وهذه الأخيرة تُعد عرضة للانتهاك أكثر إذا ما استخدمت في هذا الأمر الوسائل الإلكترونية(٢).

ألا أن هناك من يرى(٣) بما أن الاتصالات عبر شبكة الحاسوب والإنترنت تحتاج إلى خطوط الهاتف، وبالتالي ينتج عن ذلك أن مراقبة المحادثات عبر الإنترنت وشبكات الحاسوب وتسجيلها لا يتعارض مع الرأي الفقهي الذي اعتبر مراقبة المحادثات الهاتفية مشروع.

ويذهب بعض الفقه (٤) إلى أنه من الصحيح أن مراقبة الاتصالات الإلكترونية فيه اعتداء على الحياة الخاصة للأفراد وسرية اتصالاتهم، التي كفلتها

---

(١) هلال آمنة، المرجع السابق، ص٦٥.
(٢) هلال آمنة، المرجع السابق، ص٦٥.
(٣) د. علي حسن محمد طوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٥٩.
(٤) هلال آمنة، المرجع السابق، ص٦٩.

مختلف التشريعات، إلا أن هذا الأمر ضروري في بعض الأحيان في هذه الجرائم المستحدثة التي لا تكفي الإجراءات التقليدية فقط لإثباتها والحصول على الدليل الإلكتروني، وكان لابد من إتباع إجراءات حديثة تتماشى مع طبيعة كل من الدليل الإلكتروني، والجرائم الإلكترونية.

فعلى الرغم إن التنصت من أنه مثير للجدل إلا أنه مسموح به تحت ظروف معينة في جميع الدول تقريباً. فقد أكد المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات في البرازيل ١٩٨٤ على السماح للسلطات العامة باعتراض الاتصالات داخل نظام الحاسوب ذاته(١).

أما الاتفاقية الأوربية حول جرائم الانترنيت لعام ٢٠٠١، فقد سمحت المادتان /٢٠/ و/٢١/ منها بمراقبة حركة البيانات ومحتواها أثناء عملية التراسل.

وفي فرنسا، أجاز القانون الفرنسي الصادر في ١٩٩١/٧/١٠م، اعتراض الاتصالات عن بُعد بما في ذلك شبكات تبادل المعلومات(٢). وحينما أصدر المشرع الفرنسي القانون المؤرخ في ٢٠٠٠/٨/١، الذي عدّل قانون حرية الاتصالات المؤرخ في ١٩٨٦/٩/٣٠م، سمح بمقتضى هذا التعديل لمزودي الخدمات بمراقبة حركة أعضاء الإنترنت(٣).

وفي هولندا، يجوز لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات الحاسوبية(٤)، وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات(٥).

وفي الولايات المتحدة الأمريكية، سبق أن أصدرت قانوناً بعنوان (Communication Decency Acte of 1996 - CDA) وكان القانون يسمح

---

(١) لموسخ محمد، المرجع السابق.

(٢) د. علي حسن محمد طوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص ١٥٤. هلال آمنة، المرجع السابق، ص٦٢.

(٣) د. محمد طارق الخن، المرجع السابق، ص١٠٠.

(٤) د. علي حسن محمد طوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٥٧.

(٥) هلال آمنة، المرجع السابق، ص٦٢.

لسلطات التحقيق بنوع من المراقبة الإلكترونية على شبكات الإنترنت نتيجة زيادة النشاطات غير القانونية أو المحتويات الضارة بالأطفال[١].

كما إجاز قانون خصوصية الاتصالات الإلكترونية ECPA[٢]اعتراض الاتصالات الإلكترونية بما فيها شبكات الحاسوب

وفي اليابان أقرت محكمة مقاطعة (KOFU) سنة ١٩٩١ شرعية التنصت على شبكات الحاسوب للبحث عن الدليل الإلكتروني[٣].

وفي فلسطين إجاز المشرع في قانون الجرائم الإلكترونية رقم (١٦) لعام ٢٠١٧م، لقاضي الصلح أن يأذن للنيابة العامة بمراقبة الاتصالات والمحادثات الإلكترونية وتسجيلها والتعامل معها؛ للبحث عن الدليل المتعلق بالجريمة، وذلك في الفقرة (١) من المادة (٣٥) منه[٤].

وفي سورية فقد سمحت الفقرة (أ) من المادة ٢٦ من قانون مكافحة الجريمة المعلوماتية بالتقصي الإلكتروني أو المراقبة الإلكترونية.

وهكذا نستنتج أن معظم الدول أخذت بالتنصت على المكالمات الإلكترونية وأجازتها بهدف رصد الجرائم المستحدثة والحصول على الدليل الإلكتروني.

ومن الأمثلة الواقعية على التنصت على المكالمات الإلكترونية هي قيام مجرم معلوماتي من الأرجنتين في آب عام ١٩٩٥م، بالدخول إلى شبكة الحاسوب في

---

(١) د. علي حسن محمد طوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٥٧. كوثر أحمد خالند، المرجع السابق، ص٢٥١.

(٢) وهو اختصار ل – The Electronic Communication Privacy Act وقد تمّ تعديله بموجب القانون الوطني الأمريكي Patriot Act 2001، ومتوفر على الموقع: www.wikipedia.org

(٣) هلال آمنة، المرجع السابق، ص٦٢.

(٤) حيث نصت الفقرة (١) من المادة (٣٥) على أنه: "لقاضي الصلح أن يأذن للنيابة العامة بمراقبة الاتصالات والمحادثات الإلكترونية وتسجيلها والتعامل معها؛ للبحث عن الدليل المتعلق بالجريمة وذلك لمدة خمسة عشر يوماً قابلة للتجديد لمرة واحدة، بناءً على توافر دلائل جديدة، وعلى من قام بالتفتيش أو المراقبة أو التسجيل أن ينظم محضراً بذلك يقدمه إلى النيابة العامة".

مركز آمرية الرقابة البحرية للاستطلاع المحيطي في سانيتاغو بكاليفورنيا، بصورة غير مشروعة إلى مالا يقل عن (٣٩٥) موقع عبر العالم وعلى مدى (٨٣٦) مناسبة، وتشمل (١٢) دائرة أمريكية لمواقع البحرية، و لـ(٣٨) مرة منفصلة واستهداف (١٣٨) موقعاً في (٢٣) بلداً بـ (٣٩٥) مناسبة، وقام بتعديل بعض الملفات، لكن غالبية النشاط الإجرامي تركز في تركيب ملفات وقام بتعديل بعض الملفات، لكن غالبية النشاط الإجرامي تركز في تركيب ملفات استكشاف (Sniffer) لإزالة أسماء وكلمات السر الشخصية للمستخدم، وقدرت الخسارة المادية نتيجة ذلك في شبكة ناسا (NASA) وحدها بأكثر من مائة ألف دولار، وتعاونت عدة جهات لمتابعة هذا المجرم، ونتيجة للتحريات التي أجرتها هذه الجهات تم الحصول على أمر قضائي من المحكمة المختصة يسمح لها بالدخول والتنصت على الاتصالات الإلكترونية حيث تم ربط الحاسوب لديها مع جامعة هارفارد، الأمر الذي مكنها من تحديد هوية المجرم بنجاح من بين (١٦٥٠٠) حساب من حسابات المستخدمين، في شبكة الحواسيب التي يصل عددها ما بين (٨٠٠٠) إلى (٩٠٠٠) حاسوب، ومن حوالي (٢٠٠) إلى (٣٠٠) مستخدم للخطوط المباشرة، مما يعني حوالي (٦٠،٠٠٠) رسالة بريد إلكتروني في اليوم الواحد، وتم تحديد هوية المجرم باستخدام عملية التقليص الأوتوماتيكي[١].

**ثانياً: ضمانات مشروعية التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية:**

يشترط في التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية أن يكون مشروع[٢].

---

(١) The Neis, Argentine Computer Inversion Investigation – FBI- Law Enforcement, Bulletin- Oct 1928, Vol 67- Issue 10, pp.9.
د. علي حسن الطوالبه، التعاون القضائي في مجال مكافحة الجرائم الإلكترونية، مركز الإعلام الأمني، جامعة العلوم التطبيقية، البحرين، ص٥.

(٢) د. محمد طارق الخن، المرجع السابق، ص١٠٠.

وبالتالي فإنه إن اقتضت الضرورة بغرض التحقيق مراقبة أو اعتراض هذه الاتصالات وتسجيلها، حينها من الوجوب مراعاة مجموعة من الضمانات في هذا الشأن وهي نفس ضمانات المقررة للمحادثات الهاتفية، مع الأخذ في عين الاعتبار الطبيعة الخاصة لهذه الاتصالات[١]، ومن خلال استقراء موقف التشريعات المختلفة التي نصت على جواز المراقبة الإلكترونية يمكننا أن نستخلص أهم ضمانات مشروعية إجراء المراقبة الإلكترونية، كما يلي:

**أ- إن يكون هنالك جريمة خطيرة ارتكبها المدعى عليه:**

لا بد من أن يكون هنالك جرائم خطيرة ارتكبها المدعى عليه لإمكان مراقبته إلكترونياً.

وأكد المجلس الأوربي في التوصية رقم ر (٩٥) ١٣ في ١٩٩٥/٩/١١م، على أنه يجب مراجعة القوانين الإجرائية بغرض توفير إمكانية المراقبة والتسجيل أثناء نقل المعلومات وبخصوص التحقيقات بشأن بعض الجرائم الخطيرة المتعلقة بسرية وتكامل وتوفير أنظمة المعلومات والاتصالات[٢].

**من هذه التوصية نستنتج أن المجلس الأوربي رهن إجازة المراقبة والتسجيل فقط بخصوص التحقيقات بشأن بعض الجرائم الخطيرة وليس كل الجرائم مما يستوجب تحديد للجرائم التي يجوز فيها المراقبة.**

وقد نص على هذه الضمانة المشرع الهولندي عندما أجاز لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات الحاسوبية، إذا كانت هناك جرائم خطيرة ارتكبها المتهم[٣].

لكن السؤال الذي يطرح نفسه هو: **ما هي الجرائم الخطيرة التي يجوز فيها إجراء المراقبة الإلكترونية؟**

---

(١) هلال آمنة، المرجع السابق، ص٦٧.

(٢) د. مدحت رمضان، المرجع السابق، ص٨١.

(٣) د. محمد طارق الخن، المرجع السابق، ص١٠٠.

حدد المشرع الجزائري في المادة (٦٥ مكرر ٥) [١] الجرائم التي يجوز فيها اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، وذلك على سبيل الحصر، وهي : جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات [٢] أو جرائم تبيض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد.

**ونرى أنه قد أحسن المشرع الجزائري عندما إجاز المراقبة الإلكترونية في جرائم محددة على سبيل الحصر منعاً من التوسع في إجازة المراقبة الإلكترونية التي تعد استثناء من الأصل العام وهو حرمتها.**

وفي المقابل نجد المشرع **المصري** اعتمد على معيار جسامة العقوبة في تحديد الجرائم التي تجوز فيها المراقبة، وهي الجنايات والجنح المعاقب عليها لمدة لا تقل عن ثلاثة أشهر، هذا ويشترط في الجريمة محل المراقبة أن تكون قد وقعت فعلاً، حيث يبنى على ذلك ضرورة صدور الإذن بالمراقبة[٣].

**ونحن نرى أن الجرائم تقسم إلى جنايات وجنح ومخالفات حسب نوع العقوبة المحكوم بها، وتعد الجنايات من أخطر الجرائم تليها الجنح ومن ثم المخالفات التي تعد أبسط أنواع هذه الجرائم، وبالتالي من وجهة نظرنا لا يجوز إجراء المراقبة الإلكترونية إلا في الجنايات والجنح أما المخالفات فلا يمكن أن يبرر إجراء المراقبة الإلكترونية فيها نظراً لبساطتها والتي تمنع انتهاك حرمة**

---

(١) نصت المادة (٦٥ مكرر ٥) على أن: "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبيض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد".

(٢) وهذا لدراية من المشرع الجزائري على عدم كفاية الوسائل التقليدية للحصول على الدليل الإلكتروني، نظراً لما تتمتع به الجريمة الإلكترونية من خصوصية.

(٣) هلال آمنة، المرجع السابق، ص٦٨ – ٦٩.

**الاتصالات الإلكترونية، ولا يكفي ذلك بل لابد من تحديد الجنايات كما فعل المشرع الجزائري والجنح على أن يكون معاقباً عليها بحد أدنى من العقوبة لتجوز فيها المراقبة الإلكترونية.**

**ب- إن يكون هنالك مشتبه به إلكترونياً:**

والمشتبه به الإلكتروني يمكن أن يكون شخصاً، أو موقعاً، أو بريداً إلكترونياً مخالفاً للقانون. وتشمل المراقبة الإلكترونية جميع تحركات المشتبه به عبر الإنترنت، بما في ذلك بريده الإلكتروني(١).

**جـ- فائدة المراقبة في إظهار الحقيقة:**

ترى التشريعات المعاصرة أن القول بوجود فائدة من المراقبة من خلال إظهار الحقيقة، هي السند الشرعي المبرر للاعتراض وهذا على أساس أن هذا الإجراء فيه اعتداء على الحياة الخاصة للأفراد، ولهذا فهو جائز في حالات ضيقة وذلك برجاء ظهور الحقيقة وإلقاء القبض على الفاعلين أما مدى فائدة اعتراض الاتصالات الإلكترونية فهي خاضعة لتقدير إما قاضي التحقيق أو قاضي الحكم، وهذا التقدير بدوره يخضع لرقابة قضاء الموضوع(٢).

ونص على هذه الضمانة التشريع الهولندي عندما ربط مشروعية التنصت على شبكات الحاسوب بحالة إذا كان على قدر عال من الأهمية للكشف عن تلك الحقيقة(٣).

---

(١) د. محمد طارق الخن، المرجع السابق، ص١٠٠.

(٢) هلال آمنة، المرجع السابق، ص٦٨.

(٣) معمر علي إبراهيم محمد، المرجع السابق، ص ٦٩.

**د- صدور إذن بإجراء المراقبة الإلكترونية من السلطة المختصة[١]:**

تعد السلطة القضائية بصفة عامة المختصة في إصدار هذا الإذن، وُيعد هذا الأمر ضمانة ضرورية حتى يكون هذا الأمر مشروعاً، وهذا ما نص عليه القانون **الفرنسي**، فالمشرع أوجب صدور الإذن بالمراقبة من قاضي التحقيق المختص، أو من قاضي الحكم ، وحرمان النيابة العامة من إعطاء هذا الإذن، حتى لا يكون هناك أي تعسف من طرفها، إلا في حالة ما إذا كانت النيابة العامة تتولى التحقيق بنفسها، وهذا في حالة ما إذا رأت ضرورة مراقبة الاتصالات الإلكترونية، وهذا ما نص عليه المشرع **المصري**، كما أنه عند صدور هذا الإذن فإن كلاً من قاضي التحقيق أو النيابة العامة غير ملزمين بتنفيذه بأنفسهما، بل في الإمكان تكليف عضو الضابطة العدلية بهذا الأمر[٢].

وفي المقابل خالف المشرع **الجزائري** ذلك وأجاز للنائب العام المختص أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، وهذا في المادة (٦٥) مكرر ٥ من ق. إ. ج. ج[٣].

---

(١) يجب التمييز بين اعتراض الاتصالات الإلكترونية أثناء البث (On line) أي وقوع الاعتراض أثناء الاتصال بين أطرافه، واعتراض الاتصالات الإلكترونية المخزنة، أو وقوع المراقبة والتفتيش على الاتصالات الإلكترونية الموجودة في صندوق البريد الإلكتروني أو الرسائل الصوتية المخزنة في مزود الخدمة، ففي الحالة الأولى يجب تقييد الأمر بالحصول على إذن من النائب العام، أما في الحالة الثانية تخضع للقواعد العامة للتفتيش.

(٢) عائشة بن قارة مصطفى، المرجع السابق، ص١٧٤ – ١٧٥ .

(٣) حيث نصت المادة (٦٥ مكرر ٥) من قانون الإجراءات الجزائية الجزائري على أن : "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبيض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يلي:

– اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

وفي القانون الليبي يقيد المشرع النيابة العامة في إجراء التنصت بالحصول على إذن من القاضي الجزائي[١].

وهناك من يرى[٢] – ونحن نؤيده – أنه بالنظر لطبيعة الدليل الإلكتروني الصعبة فإنه من الضروري التخفيف من شروط وجوب استئذان النيابة العامة للقاضي الجزائي، حتى تتمكن من الاعتراض بنفسها في جريمة من الجرائم الإلكترونية التي تتولى التحقيق فيها، وهذا كسباً للوقت من جهة، وحفاظاً على الدليل من التلف والزوال والحصول عليه من جهة أخرى.

**كما** أعطى المشرع **الهولندي** لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات، وفي **الولايات المتحدة الأمريكية** يجوز اعتراض الاتصالات الإلكترونية بما فيها شبكات الحاسوب بشرط الحصول على إذن تفتيش صادر من القاضي[٣].

**أما في سورية** فقد سمحت الفقرة أ من المادة ٢٦ من قانون مكافحة الجريمة المعلوماتية بالمراقبة الإلكترونية **بشرط الحصول على إذن من السلطة**

---

– وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص 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 (٤٧) من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن.

تنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص في حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناءاً على إذن من قاضي التحقيق وتحت مراقبته المباشرة" .

(١) أ. طارق محمد الجملي، المرجع السابق، ص٥٦.

(٢) عائشة بن قارة مصطفى، المرجع السابق، ص١٧٤ – ١٧٥ .

(٣) هلال آمنة، المرجع السابق، ص٦٢.

**القضائية المختصة**، ويشمل مفهوم السلطة القضائية النيابة العامة وقضاء التحقيق والمحاكم الجزائية[١].

لكن إذا ذكرنا أن الأصل في مراقبة الاتصالات الإلكترونية هو الحظر، إلا إذا صدر **إذن قضائي** في هذا الشأن، ولكن هناك حالات يكون فيها الاعتراض مشروعاً حتى دون صدور الإذن القضائي، وتتمثل في **سلطة مزود الخدمات في مراقبة الاتصالات الإلكترونية** دون إذن، ويتحقق هذا الأمر إما في نطاق المراقبة المعتادة لمزود الخدمة بغرض متابعة عمل الشبكة، أو بناء على شكوى من المشترك، وسنشرحهما كالتالي:

**الحالة الأولى: المراقبة المعتادة لمزود الخدمة لعمل الشبكة:**

نصت بعض التشريعات صراحة كالقانون الأمريكي على حق مزودي الخدمات في مراقبة الاتصالات الإلكترونية الخاصة بالمشتركين في خدماتهم، وهذا الأمر يعد من العمل اليومي لشبكاتهم، بهدف حماية أنظمتهم من إساءة الاستعمال، أو من إلحاق الضرر بها عن طريق الفيروسات مثلاً، أو الاستيلاء عليها بالسرقة مثلاً.

وقد طبق القضاء هذا الأمر كحكمه بأنه من الجائز لمزودي الخدمات أن يقوموا بهذا النوع من المراقبة لمكافحة الغش، وأيضاً السرقة التي تستهدف الخدمات التي يعطونها، كقيام شخص بتقليد خط هاتف محمول للحصول على الخدمة دون دفع الاشتراك، ما يستدعي بمزود هذه الخدمة أن يتابع الأمر لمعرفة الفاعل.

والمشرع الأمريكي لم يعط هذه السلطة لمزودي الخدمات على إطلاقها، وفرض عدة شروط حتى تصح هذه الرقابة، فأول شرط هو أن يكون مزود الخدمات مجنياً عليه في الجريمة، أما الشرط الثاني فهو أن يقوم بالمراقبة والتبليغ عما يعرفه من جرائم إلى الجهات القضائية، وهذا كنوع من الحماية على حقوقه،

---

(١) د. محمد طارق الخن، المرجع السابق، ص١٠٠.

وليس لقيامه بدور المساعد للضابطة العدلية في التحريات التي يقومون بها، والشرط الثالث هو ألا يطلب رجل الشرطة من مزود الخدمة القيام بتلك المراقبة عوناً له، أي إن المبادرة بالتبليغ يجب أن تأتي من طرف مزود الخدمات، ويتمثل الشرط الرابع في أن لا يشارك رجل الشرطة أو يشرف على مزود الخدمات في قيامه بأعمال المراقبة(١).

**الحالة الثانية: المراقبة بناءاً على شكوى المشترك:**

اختلفت التشريعات المقارنة فيما يخص المراقبة على الاتصالات الإلكترونية، بعد طلب من مالك الجهاز الذي وقع عليه الاعتداء، بعد أن يطلب من رجال الضابطة العدلية وضع جهازه تحت المراقبة، وظهر في خضم هذا الاختلاف موقفين، الأول مؤيد والثاني معارض.

فيما يخص الموقف المعارض أخذ به رأي في كندا، الذي يعد أن مزود الخدمات متساوي في عمله مع رجال السلطة العامة، وبالتالي ليس من حقه أن يقوم بتلك المراقبة، وتلك التسجيلات دون إذن، وهذا على أساس أنه إن قام بهذا الأمر يعد مخالفاً لما جاء في المادة (٢/٢٤) من ميثاق الحريات الكندي.

أما الموقف المؤيد يجسده القانون الأمريكي الذي يسمح لضحايا الهجوم على الحاسوب بتفويض السلطات وهذا من أجل مراقبة الاتصالات السلكية والإلكترونية، أو مراقبة الجهاز محل الاعتداء، وهذا الأمر يلزم أن تتوافر فيه أربعة شروط هي:

الأول: هو أن يسمح المالك لأعضاء الضابطة العدلية بوضع الجهاز الخاص به تحت المراقبة، أما الثاني فهو أن يتم هذا الأمر في إطار تحقيق جنائي قائم، والثالث أن تتوافر دلائل كافية على أن تسجيل الاتصالات الآتية من الجهاز الصادر منه الاعتداء يفيد في كشف الحقيقة، والشرط الرابع هو أن يقتصر أعضاء

---

(١) هلال آمنة، المرجع السابق، ص٦٦ – ٦٧.

الضابطة العدلية على اعتراض الاتصالات الصادرة من وإلى الأجهزة محل التحقيق(١).

**هـ- تسبيب الإذن الصادر بشأن مراقبة الاتصالات الإلكترونية:**

يجوز للقاضي إصدار إذن مراقبة الاتصالات الإلكترونية كما سبق ورأينا، من خلال قيامه بأعمال التحري وما يراه من ضرورة هذه المراقبة، لما لها من أهمية في ظهور الحقيقة في جريمة ما خاصة الجريمة الإلكترونية، وفي المقابل يتحتم تسبيب هذا الإذن، وهذا التسبيب ينتج بصفة عامة من مدى اقتناع القاضي بجدية التحريات التي اتخذها عضو الضابطة العدلية، والسبب في ضرورة تسبيب الإذن القضائي الصادر بشأن مراقبة الاتصالات الإلكترونية، هو كون هذه المراقبة تمس بحريات الأفراد، فهي استثناء على القاعدة العامة والمتمثلة في حرمة الحياة الخاصة للمواطنين وحقهم في سرية مراسلاتهم واتصالاتهم(٢).

**ولم تنص التشريعات التي أخذت بالمراقبة الإلكترونية على ضرورة تسبيب الإذن الصادر بشأن مراقبة الاتصالات الإلكترونية ونرى أن ذلك يعد ثغرة قانونية ينبغي معالجتها بأسرع وقت بالنظر إلى أهمية التسبيب كضمانة مهمة لتبرير هذه المراقبة.**

**و- تحديد الأشخاص المخولين بإجراء التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية:**

**ففي الولايات المتحدة الأمريكية**، أعطى قانون خصوصية الاتصالات الإلكترونية ECPA الحق لعضو الضابطة العدلية في الحصول على المعلومات الأساسية للمشترك (كالاسم والعنوان وغيرها)، أو المعلومات المتعلقة ببريده

---

(١) هلال آمنة، المرجع السابق، ص٦٧.

(٢) هلال آمنة، المرجع السابق، ص٦٨.

الإلكتروني أو بريده الصوتي، بمجرد توجيه أمر من المحكمة إلى مزود خدمة الإنترنت تأمره فيه بالكشف عن محتويات الحساب[١].

بينما أعطى **المشرع الفرنسي** في القانون المؤرخ في ٢٠٠٠/٨/١، الذي عدّل قانون حرية الاتصالات المؤرخ في ١٩٨٦/٩/٣٠، هذا الحق لمزودي الخدمات بمراقبة حركة أعضاء الإنترنت[٢].

**ونرى أن المشرع الفرنسي لم يصب في ذلك عندما أعطى هذا الحق لمزودي الخدمات وكان الأجدر به الاقتداء بموقف المشرع الأمريكي وإعطائه هذا الحق لعضو الضابطة العدلية لأنه هو الأقدر على القيام بالمراقبة الإلكترونية نظراً لخبرته في تقصي الجرائم.**

وأكد **المشرع الجزائري** في أن لقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه، أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة (٦٥) مكرر ٥ أعلاه[٣].

وقد أعطى **المشرع السوري** سلطة القيام بالمراقبة الإلكترونية في الفقرة (أ) من المادة (٢٦) من قانون مكافحة الجريمة المعلوماتية للضابطة العدلية.

وهناك من يرى[٤]– ونحن نؤيده – أن القيام بعملية التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية تتطلب الاستعانة بمختصين في علم الأصوات واللغة وعلى هذا الأساس، يتضمن مخبر الشرطة العلمية في الجزائر فرعاً مختصاً في هذا المجال هو فرع علم التحقيق الجنائي الصوتي.

---

(١) د. محمد طارق الخن، المرجع السابق، ص١٠٠.

(٢) د. محمد طارق الخن، المرجع السابق، ص١٠٠.

(٣) انظر المادة (٦٥) مكرر ٨ ق. إ. ج. ج

(٤) بهلول مليكة المرجع السابق، ص١٧٠.

كما أن البحث والتحقيق في هذا النوع من الجرائم (الإلكترونية)، يتطلب اللجوء إلى المختصين ذوي الخبرات في العلوم البيانية الرقمية، وفي هذا الإطار ظهر للوجود فرع علمي جديد هو علم "الأدلة الجنائية الحاسوبية أو الرقمية"، ويعتبر من العلوم الحديثة والمعاصرة الذي بدأ الاهتمام يزداد بازدياد الاعتماد على الأجهزة الرقمية بمختلف أنواعها، الحاسوب، الهاتف النقال، الكاميرات الرقمية، بطاقات الائتمان وغيرها من الأجهزة التي باستطاعتها تخزين معلومات، ويعرف هذا العلم بأنه أحد فروع علم الأدلة الجنائية الذي يهتم بالتعّرف على الأدلة الرقمية حفظها وتحليلها ثم تقديمها للقضاء(١).

لذلك يرى جانب من الفقه الجنائي أن متطلبات العدالة الجنائية تفرض على الأجهزة الحكومية أن تتحمل كامل مسؤولياتها نحو اكتشاف الجرائم وضبط المجرمين ومحاكمتهم، وهذا يقتضي توفير الإمكانيات التقنية اللازمة للتحقيق في الجرائم الإلكترونية، وبمعنى أخر يتعين استقطاب وجذب الكفاءات المهنية المتخصصة في هذا المجال، للاستعانة بها في تحقيق هذه الجرائم(٢).

**وقد أصاب المشرع الجزائري في ذلك لأن القيام بالتنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية تتطلب أشخاص مؤهلين وذوي خبرة تقنية للقيام بهذه المهمة.**

**ولم تنص باقي التشريعات على تحديد الأشخاص المخولين بإجراء التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية ويعد ذلك ثغرة تشريعية ينبغي معالجتها بأسرع وقت ممكن والنص عليها وتحديد هؤلاء الأشخاص على أن يكونوا من رجال الضابطة العدلية المتخصصة في تقصي الجرائم الإلكترونية التي يتوافر بهم جملة من المؤهلات والخبرات التي تؤهلهم للقيام بهذه المهمة الصعبة.**

---

(١) بهلول مليكة، المرجع السابق، ص١٧٥.

(٢) أ.م. جاسم خريبط خلف، المرجع السابق، ص١٠.

**ي- توفير السرية والاحترام للمعلومات:**

وجاءت هذه الضمانة في توصية المجلس الأوربي رقم ر (٩٥) ١٣ في ٩/١١/ ١٩٩٥م التي أكدت على أنه في حالة جمع المعلومات بطريق المراقبة والتسجيل يتعين توفير السرية والاحترام للمعلومات التي يفرض القانون لها حماية خاصة وبصورة مناسبة(١).

**وبذلك نستنتج على أن المشرعين في مختلف التشريعات أحاطوا هذه المراقبة بمجموعة من الضمانات التي تحد من تعسف السلطات المختصة، كلزوم صدور الإذن حتى يتم اعتراض الاتصالات الإلكترونية، كما أن المشرعين ومنهم المشرع الجزائري ضيقوا من استعمال هذا الاعتراض وقصروه فقط على جرائم معينة، وكذلك عدم إعطاء الإذن باستعماله إلا إذا كان ظهور الحقيقة والقبض على الفاعلين يستدعي هذا الأمر.**

**ونرى أن المراقبة تُعد اعتداء على حرية الحديث الذي هو حق من الحقوق اللصيقة بالشخصية الإنسانية وتدخل في حياته الخاصة، ودون خصوصية الحديث يصبح الفرد متردداً خائفاً من ممارسة حقه والحديث عبر وسائل الاتصال الحديث، وذلك فيه مساس بأهم الحقوق اللصيقة بالإنسان تكمن في أنها تكشف أدق أسرار الأشخاص دون علمهم، وتمتد إلى كشف أسرار كل شخص يتصل بالشخص المراقب. إلا أنه يمكن السماح به في أحوال ضيقة، وأن يكون في نطاق ضيق، لأن إجراء المراقبة الإلكترونية مهم ويقوم بدور فعال للحصول على الدليل الإلكتروني، وذلك لعدم فاعلية الإجراءات التقليدية للحصول على هذا الدليل والتي لا تتناسب مع طبيعته، ولكن لابد من إحاطة هذا الإجراء بضمانات عدة ولا سيما تحديد نوع الحديث المراد التقاطه، والجريمة المتعلقة بها، والجهة المصرح لها بذلك، وتحديد مدة المراقبة، وكل هذه الضمانات تكفل مشروعية الحصول عل الدليل الإلكتروني.**

---

(١) د. مدحت رمضان، المرجع السابق، ص٨١.

**وفي نهاية هذا المبحث نجد أن الإجراءات الحديثة التي تعد في غالبيتها إجراءات فنية، وإن كانت تتميز بالفعالية والسرعة في الحصول على الدليل الإلكتروني وبالتالي الكشف عن الجرائم وإسنادها إلى مرتكبها، إلا أنها قد تتضمن في ذات الوقت اعتداء على الحريات الشخصية، مما يصم الدليل الإلكتروني الناتج عنها بعدم المشروعية، فلا بد من أن تباشر في إطار القانون وضمن ضوابط وضمانات تراعي الحرية الشخصية للمشتبه به.**

**وأخيراً درسنا في هذا المبحث ضمانات مشروعية الحصول على الدليل الإلكتروني في الإجراءات الحديثة، فدرسنا الإجراءات المتبعة في البيانات الساكنة وضماناتها في الحصول على دليل إلكتروني مشروع، ومن ثم تطرقنا للحديث عن الإجراءات المتبعة في البيانات المتحركة وهي المراقبة الإلكترونية فعرضنا مفهومها ومحل هذه المراقبة، كما درسنا مدى جواز إجراء المراقبة الإلكترونية وموقف التشريعات منها. وأخيراً تطرقنا لضمانات المراقبة الإلكترونية التي تكفل مشروعية الدليل الإلكتروني الناتج عنها.**

# خلاصة الباب الأول

في هذا الباب الذي كان بعنوان متطلبات مشروعية الدليل الإلكتروني في الإثبات الجزائي، وقد قسمناه لفصلين، وبحثنا في الفصل الأول مشروعية وجود الدليل الإلكتروني، ودرسنا في المبحث الأول ماهية الدليل الإلكتروني عن طريق البحث في مفهوم هذا الدليل بتعريفه والتعرف على خصائصه وطبيعته ومصادره ومكانته من أدلة الأثبات الجزائي، وكذلك التعرف على أنواعه المختلفة، وفي المبحث الثاني درسنا الموقف من مشروعية الدليل الإلكتروني كأحد أدلة الإثبات الجزائي، فدرسنا موقف أنظمة الإثبات وموقف الاتفاقيات والفقه والقضاء والقانون من هذا الدليل كأحد أدلة الإثبات الجزائية.

وفي الفصل الثاني الذي كان بعنوان مشروعية الحصول على الدليل الإلكتروني، قسمناه لمبحثين، ودرسنا في المبحث الأول الحصول على الدليل الإلكتروني في الإجراءات التقليدية، حيث قمنا بدراسة صعوبات الحصول على الدليل الإلكتروني في الإجراءات التقليدية، ومن ثم قمنا بدراسة مشروعية الحصول على الدليل الإلكتروني في الإجراءات التقليدية من خبرة ومعاينة وتفتيش وضبط، وفي المبحث الثاني درسنا مشروعية الحصول على الدليل الإلكتروني في الإجراءات الحديثة، فقمنا بدراسة مشروعية الحصول على الدليل الإلكتروني في الإجراءات المتعلقة بالبيانات الساكنة وهي التحفظ المعجل على البيانات المخزنة وكذلك الأمر بتقديم بيانات معلوماتية عن المشترك، كما قمنا بدراسة مشروعية الحصول على الدليل الإلكتروني في الإجراءات المتعلقة بالبيانات المتحركة وهي ماتُعرف بالمراقبة الإلكترونية.

# الباب الثاني

## الأحكام المترتبة على مشروعية الدليل الإلكتروني في الإثبات الجزائي

# الباب الثاني
# الأحكام المترتبة على مشروعية الدليل الإلكتروني في الإثبات الجزائي

يترتب على مشروعية الدليل الإلكتروني في الإثبات الجزائي أحكام كثيرة، فتطلب مشروعية الدليل الإلكتروني يحتم علينا دراسة آثار مشروعيته، ولاسيما مؤيدات عدم مشروعية الدليل الإلكتروني إن كان لجهة جزاء عدم المشروعية بالنسبة للدليل الإلكتروني أو لجهة جزاء عدم مشروعية الدليل بالنسبة للأشخاص الذين يحصلون عليه بطرق غير مشروعة، وأيضاً أن دراسة آثار مشروعية الاعتراف بهذا الدليل يتطلب معرفة نطاق الاعتداد به أهو يقتصر على الجرائم الإلكترونية التي هي النطاق الطبيعي للإثبات به أم يمتد كذلك إلى الجرائم التقليدية.

كما أن دراسة الأحكام المترتبة على مشروعية الدليل الإلكتروني في الإثبات الجزائي يتطلب بيان كيفية تقدير هذا الدليل المستحدث لدى القاضي الجزائي كونها آخر المراحل التي يمر بها الدليل الإلكتروني، وذلك في نظم الإثبات المختلفة وكذلك في التشريعات المقارنة.

وبناء على ذلك سنقسم هذا الباب إلى الفصليين التاليين:

**الفصل الأول: آثار مشروعية الدليل الإلكتروني في الإثبات الجزائي.**

**الفصل الثاني: تقدير الدليل الإلكتروني في الإثبات الجزائي.**

# الفصل الأول
# آثار مشروعية الدليل الإلكتروني في الإثبات الجزائي

إن دراسة آثار مشروعية الدليل الإلكتروني في الإثبات الجزائي تقتضي منا بيان مؤيدات عدم مشروعية الدليل الإلكتروني إن كان لجهة جزاء عدم المشروعية بالنسبة للدليل الإلكتروني أو لجهة جزاء عدم مشروعية الدليل بالنسبة للأشخاص الذين يحصلون عليه بطرق غير مشروعة، كما أن دراسة أثار مشروعية الاعتراف بهذا الدليل يتطلب معرفة نطاق الاعتداد به أهو يقتصر على الجرائم الإلكترونية التي هي النطاق الطبيعي للإثبات به أم يمتد كذلك إلى الجرائم التقليدية.

وبناء على ذلك سنقسم هذا الفصل إلى المبحثين التاليين:

**المبحث الأول: مؤيدات عدم مشروعية إجراءات الحصول على الدليل الإلكتروني.**

**المبحث الثاني: نطاق العمل بالدليل الإلكتروني.**

# المبحث الأول
# مؤيدات عدم مشروعية إجراءات الحصول على الدليل الإلكتروني

من المعروف أن قواعد الأصول الجزائية تنظم إجراءات التحقيق الابتدائي والنهائي بغية الوصول إلى دليل لكشف الحقيقة، ومع ذلك فلا تخلو الحياة العملية من احتمال مخالفة تلك القواعد(١).

وبالتالي تخضع إجراءات الحصول على الدليل لرقابة القضاء من ناحية المشروعية، لأنه الحارس الطبيعي للحريات، فكل إجراء من الإجراءات الماسة بحرية الأفراد يجب أن يأمر بها القضاء أو أن يكون الحق للأفراد الاعتراض عليها ضماناً لمشروعيتها(٢).

وبما أن قانون الأصول الجزائية قد بني على قواعد قانونية مقررة لحماية مصالح معتبرة، ولا يتأتى تحقيق هذه الغاية إلا إذا كانت هناك قواعد قانونية أخرى تضمن تطبيقها، هذه القواعد هي التي تحدد المخالفات التي تعتري وتصيب الإجراءات، وتجعلها معرضة لعدم تحقق الغاية التي قصدها المشرع منها مما يجعلها معيبة، وبالتالي يحق أن يطبق عليها أحد الجزاءات الإجرائية التي أهمها البطلان، مع عدم الإخلال بالجزاءات الموضوعية الأخرى والموجهة إلى الشخص القائم والمنفذ للإجراء، كالجزاء الجزائي أو التأديبي أو المدني(٣).

وإن دراسة جزاء عدم مشروعية الدليل الإلكتروني، تقتضي بيان هذا الجزاء بالنسبة للدليل غير المشروع، والأحكام التي تخص هذا الجزاء؟، كما تقتضي دراسة

---

(١) كوثر أحمد خالند، المرجع السابق، ص ٦٠.

(٢) د. عبد الحميد الشواربي، البطلان الجنائي، المرجع السابق، ص١١٣ – ١١٦.

(٣) محمد الطاهر الرحال، بطلان إجراءات التحقيق في قانون الإجراءات الجزائية الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة منتوري، قسنطينة، الجزائر، ٢٠٠٨-٢٠٠٩م، ص١.

جزاء عدم مشروعية الدليل، بيان مسؤولية الأشخاص الذين حصلوا على هذا الدليل بطرق غير مشروعة. وبناء على ذلك سنقسم هذا المبحث إلى المطلبين التاليين:

**المطلب الأول: المؤيدات الإجرائية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني.**

**المطلب الثاني: المؤيدات العقابية والمدنية والتأديبية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني.**

## المطلب الأول

## المؤيدات الإجرائية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني

الدعوى الجزائية هي: "مجموعة الأعمال الإجرائية التي تهدف إلى التحقق من وقوع الجريمة ونسبتها إلى فاعلها"(١).

وهي تشمل جميع الإجراءات التي تباشر منذ أول عمل من أعمال التحقيق حتى صدور حكم بها، وقد اشترط المشرع في كل عمل إجرائي ضرورة توافر شروط معينة لا يصح إلا بها، وهذا يعني إن الإجراء يجب أن يتم بالطريقة التي حددها القانون، ومن قبل السلطة المختصة التي أناط بها هذا القانون اتخاذ الإجراء.

وإذا كان القانون الإجرائي يبيح الاعتداء على حرمة الحياة الخاصة للأفراد، ويسمح بانتهاك السر عن طريق مراقبة المحادثات الهاتفية، وتسجيل المحادثات الخاصة خلسة، فذلك لا يكون إلا بعد الموازنة بين المصلحة العامة للمجتمع وبين الحقوق الفردية، فالإجراءات الجزائية تهدف إلى تنظيم العدالة، ويجب على الأجهزة

---

(١) د. عبد الحميد الشواربي، البطلان الجنائي، المرجع السابق، ص٩.

المختصة أن تعمل وفقاً لقواعد قانونية معينة تحمي حقوق الأفراد وتصونها من التعسف والتحكم وإساءة استعمال السلطة(١).

ولهذا فإن مشروعية الإثبات الجزائي تستلزم عدم قبول أي دليل كان البحث عنه أو الحصول عليه قد تم بطريق غير مشروع، فحرية القاضي الجزائي في الإثبات لا تعني أن يتم البحث عن الدليل أو الحصول عليه بأي وسيلة، وإن انتهكت حقوق الأفراد وضماناتها التي أقرها القانون لهم، بل إن عملية البحث عن الأدلة واستقصائها يجب أن يراعى فيها الضمانات، وأهمها قيم العدالة وأخلاقيتها ومراعاة حقوق الدفاع ومقتضيات الحفاظ على الكرامة الإنسانية، وإن وسيلة القضاء في الرقابة على الإجراءات الجزائية تكون من خلال حرمان الإجراء المعيب من ترتيب الأثر القانوني للإجراء الذي باشره بالمخالفة لما تنص عليه القاعدة الإجرائية، فالضمانات الإجرائية التي يقررها القانون تصبح غير ذات قيمة ما لم يتقرر الجزاء على مخالفتها، ومن هنا تنبع أهمية الجزاء الإجرائي (البطلان) في حماية ضمانات المتهم(٢).

وبناء على ذلك سنقسم هذا المطلب إلى الفرعين التاليين:

**الفرع الأول: بطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني.**

**الفرع الثاني: أحكام بطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني.**

---

(١) د. محمد أمين الخرشة، مشروعية الصوت والصورة في الإثبات الجنائي، دراسة مقارنة، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠١٥م، ص٢١٤.

(٢) د. محمد أمين الخرشة، المرجع السابق، ص ٢١٥.

## الفرع الأول

## بطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني

يُعد البطلان من أهم المواضيع القانونية في مختلف فروع القانون من حيث أصوله وتطبيقاته، والدور الذي يؤديه، ويكتسب البطلان أهمية كبرى باعتباره إجراء يلامس ويلحق إجراءات الدعوى وكيفية سيرها في كافة مراحلها ولا يقتصر على جانب معين(١).

والبطلان جزاء إجرائي لأن قانون الأصول الجزائية هو الذي يقرره كأثر لتخلف شروط إجرائية تطلبها صراحة أو ضمناً، وهو جزاء إجرائي كذلك من حيث محله لأنه ينصب على الإجراء فيحدد نصيبه من القيمة القانونية(٢).

وإن بحث بطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني، يقتضي منا التعرف أولاً على ماهية البطلان، وثانياً من عرض موقف الفقه والتشريع من جزاء عدم مشروعية الإجراءات للحصول على الدليل الإلكتروني.

**أولاً: ماهية البطلان:**

تتطلب تحديد ماهية البطلان من تعريفه، وكذلك من عرض موقف التشريعات من نظرية البطلان، كمايلي:

---

(١) محمد ذيب محمود نمر، أحكام البطلان في الإجراءات والمحاكمات الجزائية، دراسة مقارنة بين القانونين الفلسطيني والأردني، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن،٢٠١٣م، ص١.

(٢) أسامة عبدالله محمد زيد الكيلاني، البطلان في قانون الإجراءات الجزائية الفلسطيني، دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، ٢٠٠٨م، ص١.

**أ-تعريف البطلان:**

البطلان لغةً (نقيض الحق) مأخوذة من كلمة بَطَلَ، ويقال: بُطْل الشيء يُبْطَلُ بُطْلاً وبطولاً وبطلاناً (بضمهن)، فسد وسقط حكمه، فهو باطل(١).

أما التعريف الفقهي فقد تعددت تعاريف الفقهاء للبطلان، فمنهم من عرفه بأنه: " الجزاء الذي يترتب على مخالفة قاعدة إجرائية قصد بها حماية الشرعية الجنائية سواء كان ذلك لمصلحة المتهم أو غيره من الخصوم أو للمصلحة العامة التي تتمثل في ضمان الإشراف القضائي على الإجراءات الجنائية"(٢).

ويُعرَّف البطلان أيضاً بأنه: " جزاء إجرائي يرد على العمل الإجرائي المخالف لبعض القواعد الإجرائية فيهدر آثاره القانونية"(٣).

كما يُعرَّف البطلان بأنه: " جزاء إجرائي يرد على العمل الإجرائي المخالف لبعض أو كل القواعد الإجرائية فيهدر آثاره القانونية"(٤).

إذاً البطلان هو الجزاء الذي يلحق إجراء نتيجة مخالفته أو إغفاله لقاعدة جوهرية في الإجراءات يترتب عنه عدم انتاجه لأي أثر قانوني(٥).

وبالتالي فإن البطلان معناه عدم ترتب الأثر القانوني الذي نصت عليه القاعدة الإجرائية لأن العمل الإجرائي المتخذ بناء عليه لم يستكمل شروط صحته

---

(١) المنجد الأبجدي، الطبعة الثامنة، دار المشرق، بيروت، لبنان، ١٩٦٧م، ص٢٠٤.

(٢) د. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، ٢٠٠٣م، ص١٣٦.

(٣) د. أحمد فتحي سرور، نظرية البطلان، المرجع السابق، ص١١١.

(٤) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٦٧.

(٥) أحمد الشافعي،البطلان في قانون الإجراءات الجزائية، دراسة مقارنة، الطبعة الثانية، دار هومة، الجزائر، ٢٠٠٥م، ص ١١.

أو شكله أو صيغته أو الكيفية المنصوص عليها في القانون فيصبح الإجراء وما يترتب عليه من الإجراءات لا قيمة لها قانوناً[١].

والانعدام هو أكثر الجزاءات الإجرائية اختلاطاً بالبطلان، وهو جزاء يترتب على افتقاد الإجراء لأحد مقوماته الأساسية[٢]. وهناك من يُعرِّف الانعدام بأنه: " جزاء عدم توافر أركان العمل القانوني فيكون هذا العمل غير قائم أصلاً"[٣].

ونظرية الانعدام تقوم على فكرة الوجود القانوني للعمل الإجرائي، فإذا لم يوجد هذا العمل فلا يمكن أن نعتبره صحيح أو باطل[٤].

وبناء عليه حتى نصف إجراء معين بالصحة والبطلان، فلابد من أن نتحقق أولاً من وجوده فإذا لم يوجد فإنه لا يوصف بالصحة أو البطلان إنما بالانعدام، فالإنعدام فكرة منطقية تفرضها طبيعة الأشياء[٥].

إذاً الفرق بين الانعدام والبطلان يجد مصدره في التباين بين عدم الوجود وعدم الصحة، فمظهر عدم الوجود هو الانعدام، وجزاء عدم الصحة البطلان، وهكذا فإن العمل المنعدم يختلف عن العمل الباطل فهما وأن التقيا في تعطيل آثار العمل القانوني، إلا أن الفرق بينهما يبرز في سبب هذا التعطيل، فالانعدام يعني أن العمل غير موجود وبالتالي فلا أثر له، أما البطلان فإنه يعني أن يتجرد العمل من آثاره القانونية بأمر قضائي وذلك بالرغم من وجود العمل[٦].

---

(١) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٦٨.

(٢) فمن المعلوم أن لكل إجراء أركانه الأساسية التي بدونها يكون أو لا يكون.

(٣) د. رمسيس بهنام، الإجراءات الجنائية تأصيلاً وتحليلاً، ج٢، الطبعة الأولى، منشأة المعارف، الإسكندرية، مصر، ١٩٧٨م، ص٧٢.

(٤) د. رمسيس بهنام، المرجع السابق، ص٧٢.

(٥) محمد ذيب محمود نمر، المرجع السابق، ص٣٠.

(٦) د. أحمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجنائية، المرجع السابق، ص٥٤٩.

**ب- موقف التشريعات من نظرية البطلان:**

انقسمت التشريعات الجزائية المقارنة في أخذها لنظرية البطلان إلى ثلاثة مذاهب، هي مذهب البطلان القانوني، ومذهب البطلان الذاتي، ومذهب لا بطلان بغير ضرر.

**١-مذهب البطلان القانوني:**

مضمون هذا المذهب أن المشرع هو الذي يحدد حالات البطلان، فلا بطلان بغير نص[١]، ويفترض أن القانون هو الذي يتولى وحده دون غيره تحديد حالات البطلان مسبقاً جزاء عدم مراعاة القواعد الإجرائية التي نص عليها[٢]، وبالتالي يجب على القاضي أن يقوم بتقرير البطلان جزاءً لمخالفة القاعدة القانونية ولا يستطيع القاضي الامتناع عن تقرير البطلان[٣].

وتتفرع عن هذا المبدأ قاعدتان: الأولى هي أنه لا يحق للقاضي أن يقرر البطلان جزاءً لمخالفة قاعدة لم يقرر لها المشرع هذا الجزاء.

والثانية أنه لا يجوز للقاضي الامتناع عن تقرير البطلان في الأحوال التي يقررها المشرع[٤].

ويمتاز هذا البطلان بالوضوح والتحديد وسهولة التطبيق، ومن ثم لا مجال للاجتهاد أو الخلاف في الرأي الذي قد يؤدي إلى تضارب الأحكام القضائية، ولكن

---

(١) فاروق الكيلاني، محاضرات في قانون أصول المحاكمات الجزائية الأردني والمقارن، ج٢، د.ط، دار الفارابي، عمان، الأردن، ١٩٨٥م، ص٩٥.

(٢) د. سليمان عبد المنعم، بطلان الإجراء الجنائي، محاولة تأصيل أسباب البطلان في ظل قضاء النقض في مصر ولبنان وفرنسا، د.ط، دار الجامعة الجديدة للنشر، القاهرة، مصر، ١٩٩٩م، ص٤٣.

(٣) د. إلياس أبو عيد، أصول المحاكمات الجزائية ، ج٢، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٧م، ص٤٨٥-٤٨٦.

(٤) د. محمود نجيب حسني، المرجع السابق، ص٣٦٠.

يُعاب على هذا المذهب الجمود، فالمشرع يضع قواعد عامة مجردة لا يستطيع أن يحيط بكل الفروض الواقعية، فثمة حالات يقتضي المنطق القانوني والمصلحة الاجتماعية تقرير البطلان فيها، فلا يجد القاضي وسيلة إلى ذلك[١].

لهذا ذهبت مختلف التشريعات إلى الأخذ بمذهب آخر أكثر مرونة وحماية لحقوق الدفاع والحريات الفردية فتبنت مذهب البطلان الذاتي.

**٢- مذهب البطلان الذاتي:**

يطلق على هذا المذهب مذهب البطلان غير المحدد، وجوهر هذا البطلان يقوم على أساس اعتراف المشرع للقاضي بسلطة تقديرية واسعة في تحديد القواعد التي يترتب على مخالفتها جزاء البطلان، وتمييز هذه القواعد عن الأخرى التي لا يترتب البطلان على الإجراء المخالف لها[٢].

ويتضح مما سبق أنه وفقاً لهذا المذهب فإن المشرع ليس بمقدوره أن يحصر مقدماً حالات البطلان، وأنه خشية للنتائج التي قد تترتب على هذا الحصر فإن المشرع ترك الأمر للسلطة التقديرية للقاضي يقدر فيها مدى جسامة المخالفة حتى لا يكون طوعاً لنصوص جامدة يشاهد العيب الجسيم في العمل الإجرائي ولا يستطيع أمامه أن يفعل أي شيء لمجرد أن القانون قد فاته النص على البطلان كجزاء لهذا الإجراء المعيب[٣].

---

(١) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٦٨-١٦٩.

(٢) د. عبد الوهاب حومد، أصول المحاكمات الجزائية، الطبعة الرابعة، المطبعة الحديثة، دمشق، سورية، ١٩٨٧م، ص ٧٦٦.

(٣)د. أحمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجنائية ،المرجع السابق، ص١١٧.

إذاً يقوم هذا المذهب على أن الوسيلة لتقرير البطلان ليست تشريعية بمعنى وجود نص صريح يوجبه، وإنما الوسيلة إلى ذلك قضائية[١]، بمعنى أن يترك للقاضي تقدير حالات البطلان في كل حالة على حدة، ويضع المشرع عادةً معياراً مجرداً يستعين به القاضي في التمييز بين القواعد التي يترتب على مخالفتها البطلان، وتلك التي لا يبطل الإجراء لمخالفتها، وهذا المعيار – يقوم على التفرقة بين القواعد الإجرائية الجوهرية، وهي التي تحمي مصالح أساسية، والقواعد غير الجوهرية وهي التي تحمي مصالح أقل أهمية، وتقرير البطلان جزاء لمخالفة الأولى دون الثانية[٢].

أي أن البطلان في منطق هذا المذهب انتقائي بحسب أهمية القاعدة الإجرائية.

ويتميز هذا المذهب بالمرونة، حيث يستطيع القاضي وهو على اتصال بالوقائع في كل حالة على حدة أن يوازن بين أهمية المخالفة والجزاء الذي يترتب عليها، ويُعاب على هذا المذهب صعوبة وضع معيار للتمييز بين القاعدة الجوهرية والقاعدة غير الجوهرية مما يفسح المجال للاجتهادات الفقهية والقضائية[٣].

والتشريعات التي أخذت بمذهب البطلان الذاتي هي التي لم تأخذ بنظرية معينة في البطلان، وهذه التشريعات هي: العراقي واللبناني والسوري[٤].

---

(١) حسن يوسف مقابلة، الشرعية في الإجراءات الجنائية، الطبعة الأولى، دار الثقافة للتوزيع والنشر، عمان، الأردن، ٢٠٠٣م، ص٢٠٨.

(٢) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٦٩.

(٣) حسن يوسف مقابلة، المرجع السابق، ص١٧٧.

(٤) انظر: المادة (٢٤٩) أصول عراقي، والمادة (١٨٥) أصول لبناني، والمادة (١٩٠) من قانون أصول المحاكمات الجزائية السوري. حيث وضع المشرع السوري مجموعة من الإجراءات ونص على وجوب احترامها ورتب جزاءً على مخالفتها وهو البطلان، لكنه لم

**٣- مذهب لا بطلان بغير ضرر:**

يعني هذا المذهب أن البطلان لايحكم به حتى مع النص عليه إلا إذا تحقق ضرر من المخالفة[١]. وأساس هذا المذهب يقوم على الهدف من القانون هو حماية مصلحة معينة، فإذا لم يمس هذه المصلحة ضرر فإن الحكم بالبطلان يعتبر مجافياً للعدالة ومنافي لإرادة المشرع[٢].

وقد أخذ القانون السوري بهذا المذهب أيضاُ بجانب مذهب البطلان الذاتي، وذلك في المادة (٣٩) من أصول المحاكمات الجزائية وذلك عندما اشترط لبطلان الإجراء شرطين:

١- أن يكون فيه عيب جوهري.

٢- أن يترتب عليه ضرر للخصم.

وقد أخذ به قانون المرافعات المصري في المادة (٢/٢٥) وقانون المرافعات الفرنسي في المادة (١/١٧٣).

**ونحن نرى أن المذهب الذاتي هو أفضل من مذهب البطلان القانوني، وذلك لأنه يعطي للقاضي سلطة واسعة في تقدير حالات البطلان، فالمشرع لا يستطيع تحديد حالات البطلان بشكل مسبق، وكذلك أفضل من مذهب لا بطلان بغير ضرر، لأن هذا المذهب أي مذهب لا بطلان بغير ضرر يحصر حالات البطلان**

---

ينظم نظرية خاصة في البطلان، لأن البطلان جاء في قانون أصول المحاكمات الجزائية السوري في شكل نصوص متفرقة لا ترقى إلى نظرية عامة للبطلان على عكس ما قامت به بعض التشريعات العربية كالمشرع الفلسطيني الذي نظم نظرية للبطلان في قانون الإجراءات الجزائية الفلسطيني رقم (٣) لسنة ٢٠٠١ في الباب الرابع تحت عنوان " البطلان" من خلال المواد (٤٧٤-٤٧٤)،كما خصص المشرع المصري لنظرية البطلان جزءاً يسيراً في قانون الإجراءات الجنائية وذلك في الفصل الثاني عشر من الباب الثاني.

(١) د. عبد الوهاب حومد، المرجع السابق، ص٧٧.

(٢) أسامة عبدالله محمد زيد الكيلاني، المرجع السابق،ص٤١

**بوقوع ضرر يصيب الخصم مع أن بعض الإجراءات تهدف إلى حماية المصلحة العامة والنظام العام وليس فقط المصالح الفردية الضيقة.**

**ثانياً: موقف الفقه والتشريع من جزاء عدم مشروعية الإجراءات للحصول على الدليل الإلكتروني:**

سنعرض موقف الفقه والتشريع من جزاء عدم مشروعية الإجراءات للحصول على الدليل الإلكتروني، كمايلي:

**أ-موقف الفقه:**

إن اللجوء إلى الطرق غير المشروعة يؤدي إلى بطلان هذه الإجراءات(١).

فيجب على سلطة التحقيق أن تراعي الضمانات الموضوعية والشكلية للقيام بالتفتيش- أياً كان محله- وذلك لأن مخالفة هذه القواعد ترتب البطلان(٢).

فمثلاً التفتيش يجب أن يكون بوشر لغاية معينة وهي الكشف عن أشياء تتعلق بالجريمة أو تفيد في إظهار الحقيقة، ولذلك يقع باطلاً التفتيش الذي يجرى لغاية أخرى خلاف ما حدده المشرع، لأن كل تفتيش يجري بغير أن يتبين وجه المصلحة منه يكون إجراءً تحكمياً وباطلاً(٣).

وتتعدد صور الدفع ببطلان التفتيش على نظم الحاسوب والإنترنت وهي كلها تنصب على مدى توافر حالاته وشروط صحة كل حالة من هذه الحالات، وهي لا تخرج عن صورتين:

---

(١) خالد عياد الحلبي، المرجع السابق، ص ١٤٨.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٦٥.

(٣) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص ٣٥٨.

**الصورة الأولى: الدفع ببطلان الإنابة في تفتيش نظم الحاسوب والإنترنت:**

وتتمثل بالدفع ببطلان الإنابة في التفتيش لعدم جدية التحريات، تأسيساً على أسباب متعددة منها: إصدار الإنابة بناءً على بلاغ تلقاه من مرشد سري أو شخص ما، بأن المشتبه به يحوز برنامج مخالف للقانون بقصد الاتجار به دون إجراء تحريات، وقد يكون الدفع ببطلان التفتيش الواقع على نظم الحاسوب والإنترنت، لصدور الإنابة بعد الضبط، أو لإجراء التفتيش قبل صدور الإنابة أو صدور الإنابة في ساعة سابقة على الساعة التي أثبتت في محضر التحريات، وكذلك الدفع ببطلان التفتيش لعدم صدور إنابة من الجهة المختصة أصلاً أو لحصوله بناء على إنابة باطلة، أو صدور الإنابة من شخص غير مختص، أو صدوره من شخص لا يملكه، وبعبارة أخرى لعدم اختصاص من أصدر الإذن، وقد تكون الإنابة خالية من بيان اسم من يقوم بتنفيذها، أي المأذون له بإجراء التفتيش، أو حصول التفتيش بمعرفة شخص غير مختص، أو أن من أجراه لم يكن مأذون له به قانوناً، وقد تصدر الإنابة باسم آخر غير المشتبه به، أو باسم أضيف إليه اسم آخر، ويلحق بذلك خلو الإذن أو التحريات من تحديد عنوان مسكن المشتبه به المطلوب تفتيشه، وقد يبطل التفتيش لعدم تسبيب الإنابة.

وقد تكون الدفوع متعلقة بتنفيذ الإنابة، فقد يثار الدفع ببطلان التفتيش الواقع على نظم الحاسوب والإنترنت، لأن ما أسفر عنه غير ما انصبت عليه الإنابة، أو لوقوع التفتيش على برامج ونظم موجودة على جهاز الحاسوب، لم يرد ذكره في الإنابة، أو لعدم شمول الإنابة لموقع على الإنترنت أو للمكان الذي وقع فيه التفتيش، كما يدفع ببطلان التفتيش للتعسف في تنفذ الإنابة، أو لتكرار وقوعه على المشتبه به تنفيذاً لإنابة واحدة، وكما يجوز الدفع ببطلان التفتيش لإجرائه في غيبه المشتبه به، أو ربما لعدم تحرير محضر خاص به[١].

---

(١) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٧٨-١٧٩-١٨٠.

**الصورة الثانية: الدفع ببطلان التفتيش في الحالات الأخرى:**

كما يمكن الدفع ببطلان تفتيش نظم الحاسوب والإنترنت، إذا كان الهدف من التفتيش الاطلاع غير المصرح به على ملفات البيانات المخزنة داخل نظام الحاسوب لإحدى المؤسسات أو الشركات فيُعد هنا إجراء التفتيش باطلاً ويشكل جريمة إلكترونية عبر الإنترنت(١). وكذلك فإن التفتيش الذي يقع من أجل فعل لا يشكل جريمة يعد باطلاً(٢). وأيضاً إذا لم تتوافر دلائل قوية لتوجيه تهمة لشخص أو لعدة اشخاص أو تبين عدم جديتها كان للمحكمة أن تعد التفتيش باطلاً (٣).

كما أن الضبط عندما يكون نتيجة حتمية للتفتيش فيترتب على ذلك أن بطلان التفتيش يؤدي إلى بطلان الضبط أيضاً، لأن التفتيش في هذه الحالة وسيلة للضبط(٤).

وأيضاً تبطل الخبرة إذا لم يؤد الخبير اليمين القانونية، بل يبطل الحكم المبني عليها متى كان تقرير الخبير هو الدليل الوحيد في الدعوى(٥).

كما أنه إذا خالفت إجراءات جمع الأدلة المتحصلة من المراقبة الإلكترونية القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة(٦).

---

(١) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٤٤.

(٢) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٦٣.

(٣) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٧٠.

(٤) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٣٨.

(٥) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق،ص١٣٤.

(٦) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٥٢.

فمثلاً المراقبة الإلكترونية تكون غير المشروعة في إجراءات الدعوى الجزائية للكشف عن الحقيقة في حال عدم مراعاة الضوابط والضمانات القانونية، بسبب ما تحمله هذه الوسائل من تعد على حرمة الحياة الخاصة للأفراد، وبالتالي يمكن القول إن استخدام وسائل المراقبة الإلكترونية في إجراءات الدعوى الجزائية دون مراعاة الضمانات القانونية للكشف عن مرتكبي الجرائم، يُعد إجراء باطل لمساسه بالنظام العام(١).

ومن أمثلة الطرق غير المشروعة أو غير النزيهة أيضاً والتي يمكن أن تستخدم في الحصول على الأدلة الجنائية من خلال الحاسوب، إكراه المتهم المعلوماتي (مادياً أو معنوياً) من أجل فك شفرة الدخول إلى النظم المعلوماتية، أو كلمة السر اللازمة للدخول إلى ملفات البيانات المختزنة، أو الاستجوابات المنهكة لقوى المتهم المعلوماتي، كأن يستدعى للتحقيق معه لمدد طويلة بغية معرفة معلومات معينة حول قاعدة بيانات أو نظام إدارة قواعد البيانات أو قنوات إرسال البيانات. وتتسم بعدم المشروعية أيضاً، أعمال التحريض على ارتكاب الجريمة الإلكترونية من قبل أعضاء الضابطة العدلية، كالتحريض على التجسس المعلوماتي أو المراقبة الإلكترونية عن بُعد دون مسوغ قانوني، مثال ذلك أيضاً أن يستدل بما أسفر عنه التفتيش الباطل أو الاعتراف المشوب بالإكراه من دليل، أو الاعتداد بمعلومات وصلت إلى الشاهد عن طريق مخالف للنظام العام أو حسن الآداب كاستراق السمع، أو عن طريق إفشاء لسر المهنة، أو أن يستخدم رجال الشرطة أساليب معلوماتية(*Procédés informatiques*) في أعمال التصنت على المحادثات التليفونية (*L'écoute téléphonique*)(٢).

---

(١) د. محمد أمين الخرشة، المرجع السابق، ٢٤٧-٢٤٨.

(٢) د. جميل عبد الباقي الصغير، المرجع السابق، ص١١١ - ١١٢.

وكذلك تُعد من الطرق غير المشروعة أيضاً استخدام التدليس أو الغش أو الخداع في الحصول على الأدلة الإلكترونية[١]، وأيضاً المراقبة الإلكترونية عن بعد لشبكات الحاسوب دون مسوغ قانوني مشروع، والاتهام المتأخر لمرتكب الجريمة الإلكترونية أو المشارك فيها[٢].

**ب-موقف التشريع:**

تقرر قوانين أصول المحاكمات الجزائية البطلان كجزاء إجرائي على العمل المخالف للقانون[٣].

ووقفت التشريعات المختلفة مواقف عدة إزاء مسألة الإجراءات الجزائية ومنها إجراءات الحصول على الأدلة ومدى مشروعيتها، فقد يرسم القانون طريق مباشرة الإجراء مع ذكر الجزاء عند مخالفته، وقد يكتفي القانون بذكر الإجراء دون بيان جزاء مخالفته، تاركاً للمحكمة الاهتداء بحكمة التشريع لتقرير بطلان الإجراء من عدمه، وفي أحيان أخرى يسكت القانون عن كيفية مباشرة الإجراء والجزاء المترتب على مخالفته[٤].

ويلاحظ أن الحرية الشخصية للمتهم تراعى أكثر في التشريعات التي تتسع فيها دائرة بطلان الإجراءات المخالفة للقواعد الإجرائية، بغض النظر عما إذا كانت هذه الإجراءات تؤدي إلى كشف الحقيقة أم لا، في حين التشريعات التي تضيق فيها دائرة البطلان، فإنه يؤخذ بالدليل المستمد من الإجراء الباطل، إذا تعزز بأدلة

---

(١) معمر علي إبراهيم محمد، المرجع السابق، ص ١٥٥.

(٢) أ. د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص ٧٥٤.

(٣) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٦٧.

(٤) كوثر أحمد خالند، المرجع السابق، ص٦٠ – ٦١.

أو قرائن أخرى أو أدى إلى كشف الحقيقة[١]، وهذا ما أكدت عليه بعض أحكام المحاكم[٢].

ومعيار مشروعية الأدلة الجزائية مقرر لاحترام ضمانات المتهم، حتى لا يتغلب حق الدولة على جانب احترام الحرية الفردية التي لا يجوز إهدارها من أجل الحصول على الأدلة، وهذا ما أخذ به النظام اللاتيني الذي ينادي بعدم قبول الأدلة التي كانت ثمرة للإجراءات غير المشروعة، بخلاف النظام الانجلوسكسوني الذي يسمح للقاضي بالاعتماد على الأدلة غير المشروعة كقرائن في الدعوى لصالح المتهم[٣].

ودرج القانون الأمريكي في بداية عهده على تطبيق قواعد القانون العام التي لا تشترط لقبول الدليل سوى تعلقه بموضوع الدعوى ومناسبته لها، دون النظر إلى الوسيلة التي تم الحصول عليه من خلالها، أي حتى لو تم بطرق غير مشروعة[٤].

أما المشرع الفرنسي فقد نص صراحة في المادة (٧/١٠٠) من قانون الإجراءات الجنائية على بطلان مخالفة الضمانات والضوابط التي نظمت إجراء التصنت والتسجيل[٥].

---

(١) كوثر أحمد خالند، المرجع السابق،ص٢٦.

(٢) فجاء في قرار لمحكمة النقض السورية أنه: "لا يؤخذ بالاعتراف الحاصل نتيجة ضرب مالم يكن مؤكداً بأدلة أخرى". وفي قضية أخرى قررت محكمة النقض السورية "إن مخالفة رجال الشرطة لا يؤدي إلى إنكار ما نشأ عنه من الأمر الواقع والمشاهدة المحسوسة". ياسين الدركزلي وأديب استانبولي، المجموعة الجزائية لقرارات محكمة النقض السورية من عام ١٩٤٩ – ١٩٩٠م، ج١، الطبعة الثانية، ١٩٩٢م، ص٢٠ – ٣٠.

(٣) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٥١ – ٥٥٢.

(٤) د. محمد أمين الخرشة، المرجع السابق، ص٢٤٨.

(٥) المادة (١٠٠-٧) من قانون الإجراءات الجنائية الفرنسي والتي تم تعديلها بموجب القانون رقم ٢٠٠٤-٢٠٤ المؤرخ ٩ /٣/٢٠٠٤م حيث نصت الفقرة الأخيرة منها على: " إن مخالفة الشكليات في هذه المادة يكون معاقب عليها بعقوبة البطلان" .
موقع التشريعات الفرنسية:

كما قرر المشرع المصري البطلان كجزاء لتخلف كل أو بعض شروط صحة الإجراء الجزائي، ويترتب عليه عدم إنتاج الإجراء آثاره المعتادة في القانون. فقواعد قانون الإجراءات الجنائية لا يجوز أن تبقى محض قواعد نظرية، وإنما يتعين عند مخالفتها جزاء يحدد قيمة العمل الذي خالفها، ومدى ما له من فاعلية في سير الدعوى نحو غايتها المتمثلة في صدور حكم بات فاصل في موضوعه[١].

**ونرى بضرورة تقرير بطلان الإجراء غير المشروع للحصول على الدليل الإلكتروني الذي خالف ضمانات إجراءه، ذلك لأنه لا يجوز الاستناد على إجراء غير مشروع ينتهك حقوق وحريات المشتبه به، وإلا أصبح مبدأ المشروعية الإجرائية حبراً على ورق.**

## الفرع الثاني

## أحكام بطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني

هنالك مجموعة من الأحكام يقتضي بحثها عند دراسة بطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني، ومن ذلك معرفة أولاً الأثار المترتبة على بطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني، وثانياً طبيعة بطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني، وثالثاً، شروط التمسك ببطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني.

---

https://www.legifrance.gouv.fr. تاريخ الدخول في ٢٠١٩/٣/٢م.

(١) د. جميل عبد الباقي الصغير، المرجع السابق، ص١١١.

**أولاً: الأثار المترتبة على بطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني:**

إن بحث الأثار المترتبة على بطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني يقتضي منا بينان أثرها على الدليل المستمد منها وأثر بطلان هذه الإجراءات على الإجراءات السابقة والإجراءات اللاحقة بها.

**أ- أثر بطلان الإجراءات على الدليل المستمد منها:**

هناك من يرى[١] أن إجراءات الحصول على الأدلة الجزائية يجب أن تكون ضمن الإطار العام الذي حدده الدستور وإلا فإن الدليل المستمد بطريق مخالف للأحكام الواردة في الدستور يكون باطلاً.

ويؤدي الحكم بالبطلان إلى بطلان الإجراء وزوال أثره القانوني فيما يتعلق بقطع التقادم للدعوى الجزائية[٢].

وترتيباً على ما تقدم، فإنه يتعين على القاضي الجزائي أن لا يقضي بإدانة المتهم إلا من خلال إجراءات مشروعة تحترم فيها الحريات، وتؤمن فيها الضمانات التي رسمها القانون، ولا يحول دون ذلك أن تكون الأدلة – سواء كانت تقليدية أم كانت ناتجة عن الآلة أو التطور العلمي البيولوجي – صارخة على إدانة المتهم، طالما كانت هذه الأدلة مشبوهة ولا يتسم مصدرها بالنزاهة واحترام القانون[٣].

ويكون الدليل باطلاً إذا استحصل عليه بالمخالفة للقانون، وحتى لو كان الدليل الباطل هو الدليل الوحيد الذي يصح الاستناد عليه في إدانة المتهم[٤].

---

(١) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٥٢.

(٢) د. سليمان عبد المنعم، المرجع السابق، ص ٩٧ .

(٣) د. جميل عبد الباقي الصغير، المرجع السابق، ص١١١.

(٤) سهى إبراهيم داود عريقات، المرجع السابق،ص٢٩ – ٣٠. .

وفي حالة تقرير بطلان أي إجراء، فإنه يتناول جميع الآثار التي تترتب عليه مباشرة، ولزُم إعادته متى أمكن ذلك، ومن ثم إذا حكم بالبطلان فإن أول إجراء يتأثر بهذا الحكم هو ذات الإجراء الذي حكم بإبطاله، وبالتالي زوال جميع آثاره القانونية كأنها لم تكن ويتعين إهدار الدليل المستمد منه، وإلا أصبحت الضمانات التي يقررها القانون للحفاظ على حقوق الإنسان وحرياته عديمة الجدوى(١).

فمتى كان التفتيش باطلاً، فإن البطلان يتناول جميع الآثار القانونية المترتبة عليه مباشرة، لذلك يجب على المحكمة أن تطرح الدليل المستمد منه(٢).

فمثلاً الدليل الإلكتروني المتحصل من تفتيش نظم الحاسوب والإنترنت لا يكون مشروعاً ويعد باطلاً إذا تم الحصول عليه دون مراعاة الضمانات المحددة قانوناً(٣).

وأيضاً بطلان التسجيلات الصوتية ينسحب على الدليل المستمد منها(٤)، كما ينبني عليه بطلان كل إجراء يكون مبنياً عليه أو متفرعاً عنه(٥)، ولا تقبل شهادة من قام بإجراء المراقبة الباطلة، لأن من يقوم بإجراء باطل لا تقبل منه الشهادة عليه(٦)، وكذلك عدم إبلاغ المتشبه به بإجراء المعاينة أو عدم تمكينه من الحضور يجعل الإجراء باطلاً (٧).

---

(١) د. محمد أمين الخرشة، المرجع السابق، ص ٢٤٧.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص367.

(٣) معمر علي إبراهيم محمد، المرجع السابق، ص١٥٢.

(٤) نقض ١٩٨٩/٦/١م، مجموعة أحكام النقض، س٤٤، رقم١٠٠، ص٥٩٤.
د. محمد أمين الخرشة، المرجع السابق، ص٢٥٢.

(٥) نقض ١٩٩٦/١/١٤م، مجموعة أحكام النقض، س٤٧، رقم ٩، ص٧٢.
د. محمد أمين الخرشة، المرجع السابق، ص٢٥٢.

(٦) نقض ١٩٩٤/٩/٢٠م، مجموعة أحكام النقض، س٤٥، رقم ١٢١، ص٧٧٦.
د. محمد أمين الخرشة، المرجع السابق، ص٢٥٢.

(٧) آمال عبد الرّحمن يوسف حسن، المرجع السابق، ص١٤٤.

كما يترتب على تقرير بطلان التفتيش، إعادة الإجراء الباطل كلما أمكن ذلك وإعادة الإجراء الباطل تعني استبعاده، وإحلال إجراء صحيح محله، ويمكن إعادة التفتيش الباطل إذا توافر شرطان: الشرط الأول– أن تكون الظروف الخاصة بمباشرة الإجراء مازالت قائمة، والشرط الثاني– ضرورة الإعادة– أما إذا كانت الغاية من الإجراء قد تحققت من إجراء آخر أو لم يُعد لها فائدة في الدعوى فلا تلتزم المحكمة بإعادة الإجراء الباطل(١).

كما أنه إذا تقرر بطلان إجراء المراقبة الإلكترونية فتكون كافة الأدلة المستمدة منه باطلة، لأنها نتاج إجراء باطل حمل بين طياته انتهاكاً للخصوصية التي يتمتع بها الفرد(٢).

وفي أمريكا في عام ١٩١٤م، وبالتحديد في قضية (*Weeks*) تبنت المحكمة الفيدرالية العليا قاعدة استبعاد الدليل متى تم الحصول عليه بطريقة مخالفة للتعديل الدستوري الرابع، ثم سارت المحكمة في ذات الاتجاه بعد ذلك، وقضت باستبعاد الدليل المستمد من تنصت رجال الشرطة على المتهم بواسطة أحد مكبرات الصوت، والذي تم زرعه في منزل مجاور لمنزل المتهم، وذلك بعد توصيله بجهاز التدفئة الموجود بمنزله، وكانت الشرطة قد قدمت ذلك الدليل ضد المتهم كدليل في قضية قمار (٣).

إلا أن نطاق تطبيق قاعدة الاستبعاد كان مقصوراً على القضايا الفيدرالية، فلم تلتزم به محاكم الولايات، ففي قضية (*Schwort*) قضت محكمة ولاية تكساس بقبول الدليل المستمد من تسجيل المحادثات بصورة غير مشروعة، وهو ما أيدته أيضاً محكمة الاستئناف في ولاية تكساس، وقد اعترض القاضي (*Dauglas*)

---

(١) د. مأمون محمد سلامة، المرجع السابق، ص٩٩٤.

(٢) د. محمد أمين الخرشة، المرجع السابق، ص٢٤٨. .

(٣) د. محمد أمين الخرشة، المرجع السابق، ص٢٤٨ – ٢٤٩. .

على هذا الحكم استناداً إلى أن تسجيل الحديث يتعارض مع التعديل الدستوري الرابع، ومن ثم يتعين استبعاد الدليل المستمد من الإجراء الباطل(١).

وإذا كانت المحكمة الفدرالية العليا، قد صرحت بأن قاعدة الاستبعاد لا تلزم محاكم الولايات، إلا أنها عادت وغيرت موقفها وألزمت محاكم الولايات بتطبيق قاعدة الاستبعاد، حيث اتجهت المحكمة الفيدرالية العليا إلى القضاء بعدم دستورية قانون ولاية نيويورك الذي يجيز لرجال الأمن مراقبة المحادثات الهاتفية وتسجيلها إلا بعد الحصول على إذن قضائي(٢)، وأصبحت القاعدة مطبقة في كافة أرجاء الولايات المتحدة الأمريكية فلا يجوز قبول دليل مستمد من تنصت أو تسجيل باطل والاستناد إليه في إدانة المتهم(٣).

ودرج القضاء الفرنسي على عدم الاعتداد بالدليل الناجم عن إجراءات باطلة، مع احتفاظه بسلطة تقديرية في تحديد المخالفة الإجرائية التي من شأنها أن تفضي إلى هذا الأثر(٤)، وقد أدان ذات القضاء التنصت أثناء التحقيق الذي تجريه الشرطة، سواء كان أولياً أو في جريمة متلبس بها(٥)، كما رفض الدليل المستمد من قيام أحد رؤساء المنشأة بالتنصت على محادثات مرؤوسه، محاولاً استخدام

---

(١) د. محمد أمين الخرشة، المرجع السابق، ص٢٤٩.

(٢) بنت المحكمة حكمها على أساس أن قانون ولاية نيويورك يكتفي بالحصول على إذن من القاضي المختص، دون أن يحدد طبيعة الجريمة موضوع المراقبة، ولا طبيعة المحادثات محل المراقبة، فضلاً عن عدم تحديد المدة اللازمة لعملية المراقبة. د. محمد أمين الخرشة، المرجع السابق، ص٢٤٩.

(٣) د. محمد أمين الخرشة، المرجع السابق،ص٢٤٩ – ٢٥٠.

(4) Pradel J ; La preuve en procédure pénal comparé, Rapport in Revue Internationale de droit pénal,1992, PP .27.
Cass crim 9 October 1980, Dalloz,1981, P. 332.

(5) Cass crim 13 Juin 1989, Bull, PP.254.
Laure rassat M ; Traité de procédure Penale, P U F, Paris, France, 2000 ,PP . 343.

مضمون المحادثة التي سجلت كدليل إدانة، تأسيساً على أن التسجيل تم بطريقة غير مشروعة[١].

وفي الجزائر فإن أي دليل يتم الحصول عليه بطريقة غير مشروعة يتم إبطاله حتى الدليل الإلكتروني، وهذا ما نص عليه قانون الإجراءات الجزائية الجزائري في المواد (١/١٥٧، ١٠٥، ١٩١) [٢].

ويمكن تصحيح الإجراء الباطل ويكون ذلك بإعادته مع تلافي العيب الذي كان قد شابه وأدى إلى بطلانه[٣].

والغاية من تخويل القاضي سلطة تصحيح البطلان هو الحد من آثار البطلان وخاصة عندما يستنتج أن بطلان الإجراء سيترتب عليه بطلان إجراءات تالية له ومترتبة عليه مباشرة، فيستبدل القاضي بالإجراء الباطل إجراء صحيحاً فيستقيم بذلك السير بالدعوى، والقاضي يستعمل هذه السلطة من تلقاء نفسه، أي دون انتظار من أن يحتج من قبل صاحب المصلحة في ذلك، وتصحيح الإجراء الباطل يكون بإعادته مع تلافي العيب الذي أصابه ورتب بطلانه، ولا يكون للتصحيح أثر رجعي وينبني على ذلك أن الإجراء الجديد لا ينتج أثره إلا من تاريخ اتخاذه[٤].

ونص المشرع المصري على تصحيح الإجراء الباطل في المادة (٣٣٥) من قانون الإجراءات الجنائية المصري التي نصت على: " يجوز للقاضي أن يصحح ولو من تلقاء نفسه كل إجراء يتبين له بطلانه".

**ولم ينص على تصحيح الإجراء الباطل المشرع السوري على الرغم من أهميته الكبرى في الحد من آثار البطلان.**

---

(1) Cass crim 28 Juin 1983, Bull crim no 201.
Laure rassat M ; op, cit, P.344.

(٢) هلال آمنة، المرجع السابق، ص٩٩.

(٣) تصحيح البطلان يعني أن العمل المعيب الذي كان قابلاً للإبطال، يصبح غير قابل له. أسامة عبد الله محمد زيد الكيلاني، المرجع السابق، ص٨٨-٨٩.

(٤) د. عبد الحكم فوده، البطلان في قانون الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، مصر، ١٩٩٦-١٩٩٧م، ص٤٧٣.

ويرى بعض الفقه [١] أن طبيعة البطلان المطلق (المتعلق بالنظام العام) وآثاره متميزة عن طبيعة البطلان النسبي وآثاره، فمن البديهي القول أن السلطة الممنوحة للقاضي في المادة (٣٣٥) من قانون الإجراءات الجنائية المصري لجهة تصحيح الإجراء الباطل، تقف عند طبيعة ونوع البطلان مما يستدعي القول أن البطلان المطلق غير قابل للتصحيح.

**ونرى أن هذا الرأي الأخير بأن تصحيح الإجراء الباطل يقتصر على البطلان النسبي ولا يمتد إلى البطلان المطلق هو محق وصائب.**

**ب-أثر بطلان لإجراءات على الإجراءات السابقة واللاحقة لها:**

يرى بعض الفقه[٢] أنه لا يرتب التفتيش الباطل أي أثر على الإجراءات السابقة له، وبالتالي تبقى منتجة جميع آثارها، بينما تمتد آثار التفتيش الباطل إلى الإجراءات اللاحقة له، إذا كانت هذه الإجراءات ترتبت عليه مباشرة.

وبالنسبة لموقف التشريعات فقد نص المشرع الأردني على أثر بطلان لإجراءات على الإجراءات السابقة واللاحقة، صراحة في الفقرة (٤) من المادة (٧) من قانون أصول المحاكمات الجزائية الأردني بأنه: " لا يترتب على بطلان الإجراء بطلان الإجراءات السابقة له، أم الإجراءات اللاحقة به فلا تكون باطلة، إلا إذا كانت مبنية على الإجراء الباطل".

أما المشرع المصري فقد تحدث عن آثار البطلان في المادة (٣٣٦) من قانون الإجراءات الجنائية المصري فقضت بأنه: "إذا تقرر بطلان أي إجراء فإنه يتناول جميع الآثار التي تترتب عليه مباشرة، ويلزم إعادته متى أمكن ذلك". وتطبيقاً لذلك قضى بأنه إذا كان القبض باطلاً أهدر الدليل الذي كشف عنه.

**ولم يعالج القانون السوري عدم تأثر الإجراءات السابقة ببطلان العمل الإجرائي، وهذه ثغرة كان عليه معالجتها كما فعل كلاً من القانون المصري والأردني.**

---

(١) د. أحمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجنائية، المرجع السابق، ص١٤٣

(٢) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص ١٧٦.

وإذا كانت القاعدة هي أن بطلان الإجراء يتناول جميع الآثار التي تترتب عليه مباشرة، فإن التساؤل يثور عن المعيار الذي يبين مدى العلاقة التي تربط بين العمل الإجرائي الباطل والأعمال التالية له حتى يمتد إليها البطلان. والمعيار السائد في مصر هو أن العمل اللاحق يُعد مرتبطاً بالإجراء السابق إذا كان هذا الأخير مقدمة ضرورية لصحة العمل اللاحق. فإذا أوجب القانون مباشرة إجراء معين قبل آخر بحيث يصبح الإجراء الأول بمثابة السبب الوحيد للإجراء الذي تلاه، كان الإجراء الأول شرطاً لصحة الإجراء التالي له، فإذا بطل ترتب عليه بطلان الإجراء الذي بنى عليه.

وعلى العكس من ذلك فإن بطلان الإجراء لا ينصرف إلى الإجراءات التالية له أو اللاحقة عليه إذا كانت مستقلة عنه، ويستفاد ذلك بمفهوم المخالفة من نص المادة (٣٣٦) من قانون الإجراءات الجنائية المصري التي تقرر أن البطلان يمتد إلى جميع الآثار التي تترتب عليه مباشرة[١].

ويُترك لقضاء الموضوع تقدير ما إذا كان الإجراء الباطل يمتد إلى الإجراءات اللاحقة عليه أم أن نطاق البطلان يقتصر على الإجراء المعيب وحده[٢].

ومن تطبيقات محكمة النقض المصرية حول عدم امتداد أثر البطلان إلى الإجراء اللاحق المستقل عن المراقبة الإلكترونية الباطلة، حيث قضت بأنه: "متى كان الحكم المطعون فيه قد استند في إدانة المتهم إلى التسجيلات الصوتية، وكان الدفاع قد نازع في أن ما سجل ليس بصوت المتهم، فإنه كان يتعين على المحكمة أن تحقق في هذا الدفاع الجوهري عن طريق المختص فنياً، أما وهي لم تفعل فإن حكمها يكون معيباً لإخلاله بحق الدفاع، ولا يدفع هذا العيب أن يكون الحكم قد

---

(١) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٥٤.

(٢) د. جميل عبد الباقي الصغير، المرجع السابق، ص١١٢ – ١١٣.

استند في إدانة المتهم إلى أدلة أخرى، ذلك بأن الأدلة في المواد الجنائية متساندة يكمل بعضها البعض الآخر، فتتكون عقيدة القاضي منها مجتمعة، بحيث إذا أسقط أحدها أو استبعد تعذر التعرف على مبلغ الأثر الذي كان للدليل الباطل الذي انتهت إليه المحكمة، أو الوقوف على ما كانت تنتهي إليه من نتيجة، ولو أنها فطنت إلى أن هذا الدليل غير قائم"(١).

وفي المقابل إذا ثبت أن الإجراء اللاحق لم يكن مترتباً على المراقبة الإلكترونية الباطلة، بل إنه مستقل عنها، فإن البطلان الذي شاب المراقبة لا يمتد إليه، ويبقى صحيحاً، ويجوز الأخذ به، وفي هذا الصدد قضت محكمة النقض المصرية بأن بطلان التسجيلات بفرض وقوعه لا يحول دون أخذ القاضي بجميع عناصر الإثبات الأخرى المستقلة عنه والمؤدية إلى النتيجة التي أسفرت عنها التسجيلات(٢).

وفي الجزائر أثيرت مسألة مهمة حول المعيار الذي يبين العلاقة التي تربط بين العمل الإجرائي والأعمال التالية له، حتى يمتد إليها البطلان، وقد تعددت المعايير التي جاء بها الفقه إلا أن المعيار السائد في الجزائر هو أن العمل اللاحق يعد مرتبطاً بالإجراء السابق، إذا كان هذا الإجراء ضرورياً لصحة العمل اللاحق، فإذا أوجب القانون مباشرة إجراء معين قبل الآخر بحيث يصبح الأول بمثابة السبب الوحيد للإجراء الذي تلاه، كان الإجراء الأول شرطاً لصحة الإجراء التالي له أي اللاحق، فإذا بطل ترتب عليه بطلان الإجراء الذي بني عليه(٣).

---

(١) نقض ١٩٩١/٦/٦م، مجموعة أحكام النقض، س٤٢، رقم ١٢٥، ص٩١٣.
د. محمد أمين الخرشة، المرجع السابق، ص٢٥٢.

(٢) نقض ١٩٧٦/١/٥م، مجموعة أحكام النقض، س٢٧، رقم ٣، ص٣٦.
د. محمد أمين الخرشة، المرجع السابق، ص٢٥٣.

(٣) هلال آمنة، المرجع السابق، ص٩٩.

**ونرى أنه لا يترتب على بطلان الإجراءات أي أثر على الإجراءات السابقة لها، وبالتالي تبقى منتجة جميع آثارها، كما أنه لا يترتب على بطلان الإجراءات أي أثر على الإجراءات اللاحقة لها، إلا إذا كانت هذه الإجراءات ترتبت عليها مباشرة.**

**ثانياً: طبيعة بطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني:**

اختلف الفقه والقضاء حول نوع البطلان المترتب على مخالفة ضمانات وضوابط التفتيش والمراقبة الإلكترونية التي تشمل مراقبة المحادثات الهاتفية والإلكترونية، وتسجيل الأحاديث الخاصة، فذهب رأي إلى أنه بطلان مطلق، ورأي آخر يرى أنه بطلان نسبي، بينما اتجه رأي ثالث إلى اعتباره متعلقاً بالنظام العام في أحوال دون أحوال أخرى، وسنعرض ذلك كمايلي:

ميز الفقه بين طبيعة بطلان التفتيش غير المشروع وطبيعة بطلان إجراءات المراقبة الإلكترونية.

**أ-طبيعة بطلان التفتيش غير المشروع:**

إذا كانت القاعدة الإجرائية تنص على أن مخالفة قواعد التفتيش يترتب عليها البطلان، فإن ما يثير الجدل هو تحديد نوع البطلان الناتج عن مخالفة هذه القواعد[١]، واختلف الفقه الجزائي في شأن ترتيب البطلان على مخالفة القواعد الخاصة بالتفتيش:

فيذهب الرأي الغالب في الفقه إلى أن البطلان الذي يترتب على مخالفة ضمانات التفتيش (الموضوعية والشكلية) بطلان نسبي (أي يتعلق بمصلحة

(١) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٧٣.

الخصوم) [١]، لذلك فإنه لا يجوز التمسك به سوى أمام محكمة الموضوع، ولا تجوز إثارته لأول مرة أمام محكمة النقض [٢].

ومن مبررات أصحاب هذا الرأي أن الشروط الخاصة بالتفتيش، وضعت لحماية مصلحة الخصوم في عدم انتهاك حرمات مساكنهم وأشخاصهم، وأنه إذا كانت هذه الحماية تتعلق بالنظام العام إلا أن ذلك يأتي تبعاً لحماية مصلحة الخصوم، وأن الرضا يصحح بطلان التفتيش[٣].

وذهب رأي ثاني إلى أن بطلان التفتيش نسبي باستثناء شرطي الاختصاص وحضور المتهم[٤].

وهناك رأي ثالث يرى أن بطلان التفتيش يتعلق بالنظام العام استناداً إلى أن أحكام التفتيش لم توضع لحماية مصلحة خاصة، وإنما لمصلحة عامة هي حرمة المسكن أو الحرية الشخصية[٥]، وبالتالي تملك المحكمة أن تقضي به من تلقاء نفسها، ويجوز التمسك به ولو لأول مرة أمام محكمة النقض[٦].

---

(١) انظر: د. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، الطبعة الحادية عشر، د.د.ن، القاهرة، مصر، ١٩٧٦م، ص١٣٣. د. عمر السعيد رمضان، المرجع السابق، ص٣٥٦. د. فوزية عبد الستار، شرح قانون أصول المحاكمات الجزائية اللبناني، د.ط، دار النهضة العربية، بيروت، لبنان، ١٩٧٥م، ص٤١٢. د. مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، ج١، دار النهضة العربية، القاهرة، مصر، ١٩٨٨م، ص٦٢٣.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٦٥-٣٦٦.

(٣) د. مأمون محمد سلامة، المرجع السابق، ص٦٢٣.

(٤) د. أحمد فتحي سرور، الوسيط في الإجراءات الجنائية، المرجع السابق، ص٦١٤.

(٥) أ. عبد الأمير العكيلي، أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية، ج١، الطبعة الأولى، مطبعة المعارف، بغداد، العراق، ١٩٧٥م، ص٣٤٨.

(٦) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٦٥-٣٦٦.

بينما اتجه رأي رابع إلى أن بطلان التفتيش يتعلق بالنظام العام إذا كان مترتباً على مخالفة الضمانات الموضوعية (المحل والسبب والاختصاص)، لأنها مقررة لمصلحة العدالة بينما يكون نسبي أي متعلقاً بمصلحة الخصوم إذا ما ترتب عليه مخالفة الضمانات الشكلية[١].

ويترتب على التمييز بين البطلان المطلق المتعلق بالنظام العام والبطلان النسبي المتعلق بمصلحة الخصوم عدة نتائج أهمها:

-البطلان المطلق المتعلق بالنظام العام تقضي به المحكمة من تلقاء نفسها، ولو بغير طلب، فمثلاً إذا تعلق بطلان التفتيش بالنظام العام، فيجوز الاحتجاج به في أية مرحلة من مراحل الدعوى الجزائية، ولكن لا يجوز الاحتجاج به لأول مرة أمام محكمة النقض إذ أن الدفع ببطلان التفتيش يختلط فيه الواقع بالقانون ويقتضي تحقيقاً موضوعياً لا تختص به محكمة النقض، وذلك مالم تكن مدونات الحكم تحمل مقومات البطلان[٢]، كما يجوز لكل ذي مصلحة التمسك به في أية مرحلة من مراحل الدعوى، ولو لأول مرة أمام محكمة النقض، أما البطلان النسبي المتعلق بمصلحة الخصوم فلا تقضي به المحكمة إلا إذا تمسك به الخصم صاحب المصلحة، ولا يجوز إثارته لأول مرة أمام محكمة النقض.

---

(١) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٧٥. د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٣٦٦.

(٢) د. محمود نجيب حسني، المرجع السابق، ص٥٥٨-٥٥٩.

– البطلان المطلق المتعلق بالنظام العام لا يجوز التنازل عنه صراحة أو ضمناً، أما البطلان النسبي المتعلق بمصلحة الخصوم فيجوز التنازل عنه صراحة أو ضمناً بقبول نتائجه أو بالسكوت عن الدفع به في حينه[١].

– يكون التقرير بالبطلان ذو طبيعة كاشفة إذا تعلق بالبطلان المطلق المتعلق بالنظام العام، ويكون التقرير به منشئ إذا كنا بصدد بطلان نسبي أو إجراء يتعلق بمصلحة الخصوم[٢].

**ونحن نرى أنه يجب التمييز بين الضمانات الموضوعية والضمانات الشكلية لإجراء التفتيش، فالضمانات الموضوعية للتفتيش تشكل ضمانات جوهرية ويترتب على مخالفتها بطلان مطلق متعلق بالنظام العام لأنه تتعلق بالمصلحة العامة وحسن سير العدالة، أما الضمانات الشكلية فيترتب عليها بطلان نسبي متعلق بمصلحة الخصوم.**

**أما بالنسبة لطبيعة بطلان الإجراءات التقليدية الأخرى للحصول على الدليل الإلكتروني من خبرة ومعاينة وضبط، وكذلك طبيعة بطلان الإجراءات المتعلقة بالبيانات الساكنة (التحفظ المعجل – تقديم بيانات عن المشترك) باستثناء الإجراءات المتعلقة بالبيانات المتحركة (المراقبة الإلكترونية)، فيكون البطلان نسبي متعلق بمصلحة الخصوم وذلك لأن هذه الإجراءات لا تبلغ في خطورتها إجراء التفتيش الذي يعد أخطر الإجراءات التقليدية للحصول على الأدلة لأنه يقع على مستودع السر وينتهك حريات الأفراد وحياتهم الخاصة.**

---

(١) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٧٣–١٧٤.

(٢) أسامة عبدالله محمد زيد الكيلاني، المرجع السابق، ص٧٤.

**ب- طبيعة بطلان إجراءات المراقبة الإلكترونية:**

كما ظهر اضطراب واضح في الفقه حول تحديد طبيعة البطلان المترتب على مخالفة ضمانات وضوابط المراقبة للحصول على الدليل الإلكتروني، حيث ذهب جانب من الفقه إلى أن بطلان الدليل المستخلص عن طريق ارتكاب جريمة يكون باطلاً بطلاناً مطلقاً ومتعلقاً بالنظام العام، ويجوز لكل ذي مصلحة التمسك به كما أن للمحكمة أن تقضي به من تلقاء نفسها(١)، وحجته في ذلك أن المصلحة التي تحميها ضمانات المراقبة الإلكترونية مثلاً تهدف إلى تحقيق مصلحة عامة، ومن ثم فإن مخالفتها يترتب عليها بطلان مطلق.

وقد اتجه أغلب الفقهاء إلى القول إن البطلان المترتب على مخالفة ضوابط وضمانات المراقبة هو بطلان نسبي، حجتهم في ذلك أن الغرض من هذه الضمانات والضوابط هو تحقيق مصلحة المتهم والخصوم.

وذهب جانب آخر من الفقه بأن الأصل في بطلان المراقبة أن يكون نسبياً، ومع ذلك فإن البطلان من الممكن أن يكون مطلقاً في حالتين: الأولى: إذا كان دليل المراقبة مثلاً مستمداً من جريمة، والحالة الثانية: إذا تم مخالفة ضابط الاختصاص بالمراقبة، ومن ثم يترتب البطلان المطلق في حالة إجراء المراقبة دون الحصول على إذن القاضي الجزائي في الأحوال التي يستوجب القانون الحصول على هذا الإذن(٢).

والرأي الراجح هو إن البطلان المترتب على مخالفة ضمانات وضوابط المراقبة الإلكترونية وبالتالي الدليل الإلكتروني الناتج منها هو بطلان مطلق وليس نسبي، ويجوز إثارته في أي حالة تكون عليها الدعوى، وعلى المحكمة أن تقضي به من تلقاء نفسها، وساق هذا الرأي حجتين لتأييد رأيه هما:

---

(١) معمر علي إبراهيم محمد، المرجع السابق، ص ١٥٣.

(٢) د. محمد أمين الخرشة، المرجع السابق، ص٢٣٥.٢٣٤..

الحجة الأولى: إن المراقبة تحمل بين طياتها انتهاكاً للخصوصية التي يتمتع بها الفرد، وهي مصونة بنص الدستور، وبالتالي فإن مخالفة ما نص عليه الدستور يورث بطلاناً مطلقاً.

الحجة الثانية: إن المراقبة إجراء منتج للدليل، والدليل المستمد من جريمة يكون باطلاً بطلاناً مطلقاً.

**ونحن نرى أن عدم مراعاة ضمانات المراقبة الإلكترونية التي تعد بحق إجراء خطير ينتهك حق الفرد في أن تبقى أحاديثه الشخصية مصانة ومحمية يترتب عليها البطلان المطلق وهذا البطلان متعلق بالنظام العام ويجوز إثارته في أي مرحلة من مراحل الدعوى.**

أما بالنسبة لموقف القضاء، فلم تستقر محكمة النقض المصرية في أحكامها على وصف بطلان المراقبة، ولم تجر أحكامها في هذا الشأن على وتيرة واحدة، فنجدها في بعض الأحكام تأخذ بالبطلان النسبي، وفي أحكام أخرى تتجه إلى الأخذ بفكرة البطلان المطلق.

**١- الاتجاه الأول: البطلان النسبي:**

اعتنقت محكمة النقض المصرية في بعض أحكامها فكرة البطلان النسبي، فاشترطت توافر الصفة، فيمن يدفع ببطلان المراقبة فقضت بأن: "لما كان الحكم المطعون فيه قد عرض للدفع ببطلان إذن النيابة العامة بالتسجيل لإجرائه على هاتف لا يخص الطاعن، ورد عليه بقوله على فرض أن الهاتف غير خاص بالمتهم وخاص بغيره، فإن الدفع في هذا الشأن لا يقبل من غير حائزه، باعتبار أن الحائز هو صاحب الصفة في ذلك، وأن الصفة تسبق المصلحة، فإن لم يثره الحائز أو المالك، فليس لغيره أن يبديه، ولو كان يستفيد منه، لأن هذه الفائدة لا تتحقق بالتبعية وحدها، وإذا كان ما خلص إليه الحكم في طرح ما دفع به الطاعن

متفقاً وصحيح القانون، فإن ما يؤخذ على الحكم في هذا الصدد يكون غير مقبول"[١].

ويظهر من خلال هذا الحكم أنه لا يستقيم مع فكرة البطلان المطلق، لما هو مقرر من أن لكل ذي مصلحة أن يتمسك بهذا البطلان سواء وقع الإجراء الباطل عليه أم على غيره.

واشترطت محكمة النقض للدفع ببطلان المراقبة سبق إثارته أمام محكمة الموضوع وعللت ذلك بأن الإجراءات السابقة على المحاكمة لا تجوز إثارتها أمام محكمة النقض[٢].

**٢- الاتجاه الثاني: البطلان المطلق:**

ظهر هذا الاتجاه في بعض أحكام محكمة النقض المصرية، فقضت هذه المحكمة بأنه: "من المقرر أن الدفع ببطلان..و..وتسجيل المحادثات، إنما هو من الدفوع القانونية المختلفة بالواقع، التي لا يجوز إثارتها لأول مرة أمام محكمة النقض، ما لم يكن قد دفع به أمام محكمة الموضوع، أو كانت مدونات الحكم تحمل مقوماته نظراً لأنه يقتضي تحقيقاً تتأتى عنه وظيفة هذه المحكمة، ولما كان الثابت من محضر جلسة المحاكمة أن أياً من الطاعن أو المدافع عنه لم يدفع ببطلان إذن رئيس المحكمة...و...وتسجيل المحادثات لعدم اختصاص مصدره، ولخلوه من تاريخ إصداره، وكانت مدونات الحكم قد خلت مما يرشح لقيام ذلك البطلان، فلا يقبل إثارته لأول مرة أمام محكمة النقض"[٣].

---

(١) نقض ١٣/٤/١٩٩٨م، مجموعة أحكام النقض، س٤٩، رقم٧٣، ص٥٦٣.
د. محمد أمين الخرشة، المرجع السابق، ص٢٣٥.

(٢) نقض ٤/١/١٩٨٣م، مجموعة أحكام النقض، س٣٤،رقم٤،ص٣٦.
د. محمد أمين الخرشة، المرجع السابق، ص٢٣٦.

(٣) نقض ٢٦/٩/١٩٩٦م،مجموعة أحكام النقض، س٤٧،رقم١٢٨،ص٨٩٢.
د. محمد أمين الخرشة، المرجع السابق، ص٢٣٦.

ونخلص مما تقدم إلى أن محكمة النقض في أحكامها السابقة تجيز إثارة بطلان المراقبة لأول مرة أمامها، إذا كانت الوقائع الثابتة بالحكم دالة على هذا البطلان، أي أنها تعد بطلان المراقبة الإلكترونية من النظام العام.

**ونرى أن بطلان إجراء المراقبة الإلكترونية والمترتب على مخالفة ضمانات مشروعية المراقبة الإلكترونية هو بطلان مطلق يتعلق بالنظام العام، وبالتالي يجوز لمحكمة الموضوع أن تقضي به من تلقاء نفسها، ولو لم يطلبه أحد الخصوم، ويجوز الدفع به لأول مرة أمام محكمة النقض.**

**ثالثاً: شروط التمسك ببطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني:**

يشترط لصحة التمسك بالبطلان الشروط التالية:

**أ-شرط المصلحة:**

المصلحة هي الفائدة أو المنفعة العملية المشروعة التي يراد تحقيقها من التمسك بالبطلان، وليس شرطاً أن تكون الفائدة أو المنفعة محققة، بل يكفي أن تكون محتملة(١).

حيث يجب أن يكون للمتمسك بالبطلان مصلحة فيه، والمصلحة هي السلطة أو الحق في التمسك بالبطلان، ولا تنشأ الا لمن له مصلحة في تقريره، والقاعدة أنه لا يقبل أي طلب أو دفع لا يكون لصاحبه فيه مصلحة قائمة يقررها القانون ولا يشترط في المصلحة أن تكون محققة، بل يكفي مجرد احتمال الفائدة(٢).

---

(١) د. سميح عبد القادر المجالي، أثر الإجراء الجزائي الباطل في المركز القانوني للمتهم، دراسة مقارنة، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، الأردن، ٢٠٠٦م، ص ٣٠١.

(٢) محمد الطاهر الرحال، المرجع السابق، ص٤٥.

وهذا الشرط يطبق أيضاً على التفتيش الواقع على النظم المعلوماتية وبالتالي لا يقبل الدفع ببطلان التفتيش إلا ممن شرع البطلان لمصلحته، وهو حائز جهاز الحاسوب أو البرنامج الذي جرى تفتيشه أو الشخص الذي فُتش[١]

ولا يجوز لمن كان سبباً في بطلان العمل الإجرائي أن يتمسك به، ولو كانت القاعدة المخالفة مقررة لمصلحته وفقاً للقواعد العامة، ويمكن الأخذ بهذا المبدأ دون نص عليه لأنه يعد تطبيقاً للقواعد العامة. ويشترط لأعمال هذه القاعدة أن يكون الخصم والذي يريد التمسك بالبطلان قد تسبب فيه، على أنه لا يشترط أن يكون المتسبب هو الخصم نفسه، فيكفي أن يكون شخصاً آخر يعمل باسم الخصم[٢].

وينحصر مجال تطبيق هذه القاعدة في البطلان المتعلق بمصلحة الخصوم دون البطلان المتعلق بالنظام العام، وعلة ذلك، في أساس القاعدة المتقدمة وهو التنازل الضمني عن مراعاة القاعدة الإجرائية المخالفة المقررة لمصلحة الخصم الذي يتمسك بالبطلان[٣].

**ب-شرط الصفة:**

كان المشرع الفرنسي لا يقر بحق المتهم والمدعي المدني في الطعن بالبطلان في إجراءات التحقيق أمام غرفة الاتهام قد عدل عن موقفه حيث فسح المجال أمامها للطعن بالبطلان وذلك اثر تعديل قانون الإجراءات الجزائية بموجب قانوني في ١٢ /١٩٩٣/٨[٤].

---

(١) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٧٧.

(٢) أسامة عبدالله محمد زيد الكيلاني، المرجع السابق، ص٦٩.

(٣) د. أحمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجنائية، المرجع السابق، ص٣٥٠.

(٤) د. أحمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجنائية، المرجع السابق، ص٣٥٣.

كما أن القانون الجزائري أعطى المتهم والمدعي المدني أو محاميهما الطعن بالبطلان إذا وجدوا أن هنالك إجراء مشوب بعيب البطلان ومن شأنه التأثير على حقوقهم في الدفاع.

ولم يبين كل من المشرع السوري والمصري من هم الأطراف الذين يحق لهم طلب إبطال الإجراء، مما يقتضي إلى الرجوع إلى القواعد العامة في ذلك، التي تعطي كل من له صفة في الدعوى في إبطال الإجراء.

**ونحن نرى أن شرط المصلحة يطبق- في حال كان البطلان نسبي وليس مطلق- وشرط الصفة يطبق على من يتمسك بإبطال الإجراءات غير المشروعية للحصول على الدليل الإلكتروني.**

## المطلب الثاني
## المؤيدات العقابية والمدنية والتأديبية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني

إن الإجراءات التي تقوم بها الضابطة العدلية أو جهات التحقيق قد تُعد إجراءات غير مشروعة، ومن الممكن أن تضع الجهات التي تقوم بها تحت طائلة المسؤولية(١).

فجزاء مخالفة القانون في الحصول على الأدلة يترتب عليها جزاءات جزائية وإدارية فضلاً عن الحكم بالتعويض(٢).

وبالتالي يتمثل جزاء عدم مشروعية الدليل الإلكتروني بالنسبة لمسؤولية الأشخاص في قيام مسؤوليتهم الجزائية والمدنية والمسلكية، لذلك لابد لنا من دراسة هذه المؤيدات في الفرعيين التاليين:

---

(١) أمجد خليل حمودة، المرجع السابق، ص١٢٠.

(٢) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٨٥. معمر علي إبراهيم محمد، المرجع السابق، ص ١٥٣.

**الفرع الأول: المؤيدات العقابية والمدنية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني.**

**الفرع الثاني: المؤيدات التأديبية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني.**

## الفرع الأول

## المؤيدات العقابية والمدنية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني

سنبحث المؤيدات العقابية والمدنية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني المتخذة من قبل أجهزة العدالة والتي تخالف وتخرق ضمانات مشروعية هذه الإجراءات، وذلك أولاً ببيان مفهوم الحق في الحياة الخاصة، وثانياً ببيان المؤيدات العقابية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني، وثالثاً ببيان المؤيدات المدنية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني.

### أولاً: مفهوم الحق في الحياة الخاصة:

تعددت التسميات التي تطلق على الحق في الحياة الخاصة[١]، فقد يسمى الحق في الفردية أو الحق في العزلة أو الحق في السرية أو الحق في الألفة وكل هذه التسميات تعكس جوانب متعددة لحياة الإنسان الخاصة الأمر الذي يجعلها متداخلة مع بعض الأفكار أو متداخلة معها أو شبيها لها[٢].

---

(١) تستعمل التشريعات اللاتينية مصطلح الحق في الحياة الخاصة، بينما تستعمل التشريعات الأنكلوسكسونية الحق في الخصوصية. د. أحمد فتحي سرور، الحماية الحنائية لأسرار الفرد في مواجهة النشر، د.ط، دار النهضة العربية، القاهرة، مصر، ١٩٩١م، ص٣٩.

(٢) د. محمد ثامر، الحماية القانونية والقضائية لحق الإنسان في الخصوصية، كلية القانون، جامعة ذي قار، العراق، ٢٠١٥/٥/٥م. متاح على الموقع التالي:
http://www.alnoor.se/article.asp?id=274740.

**وعـرَّف المشـرع السـوري** فـي المـادة الأولـى مـن قـانون مكافحـة الجريمـة المعلوماتيـة **الخصوصية** بأنها: "حق الفرد في حماية أسراره الشخصية والملاصقة للشخصية والعائلية، ومراسلاته، وسمعته وحرمة منزله، وملكيته الخاصة، وفي عدم اختراقها أو كشفها دون موافقته".

ولا يمكن تحديد نطاق لخصوصية الإنسان وهذا هو مكمن أهمية هذا البحث في الحق في الخصوصية أو في توفير الضمانات القانونية لهذا الحق ذلك أن تعدد نشاطات الإنسان وحركاته ومهامه وأعماله وتوجهات مشاعره وعواطفه وأحاسيسه وعلاقاته بما حوله من أشياء وأشخاص تتضمن جميعها مفردات من خصوصية الإنسان ينبغي على القانون أن يوفر لها الحماية وينبغي للقضاء أن يجسد هذه الحماية ويوسع من نطاقها. وإن القضاء الأوربي والمقصود هنا المحكمة الأوربية لحقوق الإنسان كان لها فضل السبق والانجاز والابتكار في تصوير مفهوم الخصوصية وكذلك اللجنة الأمريكية، والظاهر أن تدخل القضاء في تحديد نطاق الحق في الخصوصية والحماية القانونية لهذا الحق وخصوصاً ما يرتبط منها بإجراءات التفتيش ودخول المنازل والتصرفات والإجراءات المتبعة من قبل رجال الشرطة والتي يمكن أن تكشف عن خصوصية الإنسان الذي ما كان له أن يظهر إلى العلن والإشهار لولا قيام الشرطة بمثل هذا الإجراء ، هذا بالإضافة إلى إجراءات النشر في وسائل الإعلام[١].

وللإنسان خصوصياته التي يجب أن ينفرد معها إلى نفسه، وهو مطمئن إلى خلوته، مطمئن إلى أن أحداً لن يقطع تلك الخلوة، أو يقتحم عليه خصوصياته[٢].

وكفلت الأديان السماوية حرمات وحريات الإنسان قبل أن تكفلها الدساتير والقوانين، ولا تختلف هذه الحرمات وتلك الحريات في مضمونها من بلد إلى آخر، ولكن قد تختلف وسائل حمايتها[١].

---

(١) د. محمد ثامر، المرجع السابق.

(٢) د. جميل عبد الباقي الصغير، المرجع السابق، ص٧٣.

فالإعلان العالمي لحقوق الإنسان لسنة ١٩٤٨م، اعترف بالحق في الخصوصية، وذلك في المادة (١٢) منه التي نصت على أنه: "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات".

كما أقرت الاتفاقية الأوربية لحقوق الإنسان لسنة ١٩٥٠م، الحق في الخصوصية، وذلك في المادة الثامنة منها التي نصت على أنه "كل شخص الحق في أن تحترم حياته الخاصة وحياته العائلية ومسكنه ومراسلاته".

وقد تضمّن قانون العقوبات السوري نصوصاً تعاقب على خرق حرمة المنزل وعلى إفشاء الأسرار[٢].

كما أن أغلب دساتير العالم تضمنت مبدأ المحافظة على الأسرار الخاصة للأشخاص. حيث نص الدستور المصري لعام ٢٠١٤م، صراحة على الحق في الخصوصية في المادة (٥٧) منه بقولها: " للحياة الخاصة حرمة، وهي مصونة لا تمس .وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك".

كما أنه كفل المشرع الفرنسي حماية خاصة للحياة الخاصة وأسرارها حيث تنص المادة التاسعة من القانون المدني الفرنسي على حق الإنسان في احترام حرمة حياته الخاصة، وتفسيراً لهذا الحق انتهى الفقه إلى أن هذا الحق يشمل

---

(١) د. جميل عبد الباقي الصغير، المرجع السابق، ص٧١.

(٢) المواد ٥٥٧ و ٥٥٨ و ٥٦٥ وحتى ٥٦٧ من قانون العقوبات السوري.

حق الإنسان في عدم التقاط صور له أثناء مباشرة حياته الخاصة دون إذن منه، وكذلك حقه في عدم تسجيل صوته والحق في عدم الاطلاع على خطاباته ومراسلاته الخاصة ولا يجوز دون موافقة مسبقة منه ولا يجوز إجباره على الموافقة تحت تهديد حرمانه من مزايا مادية أو معنوية[١].

وعدد المشرع الفرنسي الحالات التي يجوز فيها للسلطات العامة التدخل في الحياة الخاصة للأفراد والتي يتعين أن تكون محددة مسبقاً بمقتضى القانون وهي الأمن القومي والأمن العام والمصالح الاقتصادية للبلاد والأمن والنظام وحماية المجتمع من الجريمة وحماية الصحة والآداب العامة وحماية حقوق وحريات الغير[٢].

**ونحن بدورنا ندعو المشرع السوري أن يقوم بسن نصوص عقابية وإجرائية تتكفل بحماية الحياة الخاصة المخزونة في الحاسوب والإنترنت، بحيث تمنع اقتحام الملفات الشخصية دون سند قانوني، حماية للحقوق والحريات الفردية التي كفلها الدستور السوري بالإضافة إلى المواثيق الدولية.**

## ثانياً: المؤيدات العقابية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني:

إن استراق السمع والتصنت على الأحاديث الخاصة وتسجيلها يُعد اعتداء صارخ على الحياة الخاصة[٣].

ومن أهم صور خرق حرمة الحياة الخاصة والتي تشكل الركن المادي فيها هي إن الملفات قد تحتوي على أسرار شخصية للإنسان العادي أو ملفات تتعلق بمعاملات المؤسسات والشركات حيث يمكن حمايتها عن طريق كلمة السر (password)، ولا يمكن فتح هذه الملفات والوصول إلى ما فيها دون كسر كلمات

(1) KAYSER PIERRE, La protection de la vie privée Economique , 2édition ,Presses universitaires d'AIX - MARSEILLE, France, 1990, PP224 - 226.
(2) KAYSER PIERRE, op,cit,PP224 - 226.
(٣) د. جميل عبد الباقي الصغير، المرجع السابق، ص٧٣.

السر، ولذلك ظهرت برمجيات عديدة تساعد في كسر كلمات سر الملفات المحمية أو تكشف كلمة سر حفظ الشاشة، بل وحتى كلمة سر مدير الشبكة ذاته، وهذا الأمر يفيد أعضاء الضابطة العدلية عند البحث عن أدلة أو التحقيق فيها، ولكن هذه البرمجيات كما أنه تقدم خدمة لكشف الحقائق لأعضاء الضابطة العدلية وأجهزة العدالة، فقد يساء استخدامها، وتوظف في أعمال غير مشروعية أو حتى إجرامية مثل الدخول إلى شبكات الإدارات الحكومية والمؤسسات والمصارف والتلاعب بالمعلومات أو إلغائها أو تحويل الأموال من الحسابات بطريقة غير مشروعية(١).

وبالنسبة لموقف التشريعات، قامت التشريعات الإنكلوسكسونية بإيراد نصوص خاصة تسري على الاتصالات الالكترونية التي تتم بواسطة الكومبيوتر والتي تتخذ شكل البريد الإلكتروني، إضافة إلى الاتصالات السلكية واللاسلكية، وعلى رأسها التشريع الأمريكي حيث عاقب القانون الفدرالي الأمريكي – Chapter 119Part 1 - – على من يعترض المراسلات الإلكترونية، ووضعها في نفس Title 18Sec.2511 مكان الاتصالات السلكية، وقرر عقوبات على كل من اعترض أو حاول اعتراض أو ساعد غيره على أن يعترض أي اتصال سلكي أو شفري أو إلكتروني(2).

وبالنسبة لموقف التشريعات اللاتينية، فقد وفر المشرع الفرنسي حماية للمراسلات الخاصة التي يتم نقلها عن طريق وسائل الاتصال من تسجيلها أو اختلاسها أو استخدامها أو إفشائها وعاقب على ارتكاب مثل هذه الأفعال بسوء قصد في (المادة ٢٢٦ – ٢/١٥ من قانون العقوبات الفرنسي الجديد) وبالتأكيد فإن الحماية التي يوفرها المشرع الفرنسي للمراسلات الخاصة تسري بشأن تلك التي تتم بطريق الإنترنت والبريد الإلكتروني وفقاً لمفهوم الاتصالات الوارد بالقانون الصادر في عام

---

(١) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص١٤٧ – ١٤٨.

(٢) هلال آمنة، المرجع السابق، ص٦٦.

١٩٨٦[١]، كما تعاقب المادة (٢٢٦ – ٣) على تصنيع واستيراد واستئجار وبيع الأدوات التي تستخدم في ارتكاب الأفعال المشار إليها بالمادة (٢٢٦ – ١٥) والتي يجب لحيازتها الحصول على إذن مسبق من وزير المواصلات.

كما فرض قانون العقوبات الفرنسي بالمادة (٤٣٢ – ٩) عقوبات مشددة بشأن ممثلي السلطة العامة والحاصلين على امتياز يتعلق بالاتصالات الذين يسمحون بمراقبة المراسلات والاتصالات الخاصة في غير الأحوال المصرح بها قانوناً[٢].

وفي إطار مشروعية الدليل الإلكتروني، فإن الفقه والقضاء في فرنسا اتجه إلى فرض عقوبات جزائية على السلطات المختصة بالتحقيق الذين يحصلون على هذا الدليل بشكل غير مشروع سواء في مجال التنقيب عن الجرائم التقليدية، أم في مجال التنقيب عن جرائم الحاسوب والاتصالات.

كما أن المادة (٣٠٩) مكرر[٣] من قانون العقوبات المصري عاقبت بالحبس مدة لا تزيد على السنة كل من اعتدى على حرمة الحياة الخاصة للمواطن، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه: أ – استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون".

كما ضمن الدستور الجزائري لسنة ١٩٩٦ في المادة (٣٩) فقرة (٢) الاتصالات بمختلف أنواعها حيث نصت على: "سرية المراسلات والاتصالات بكل أشكالها مضمونة". كما عاقب المشرع الجزائري لأول مرة على اعتراض الاتصالات

---

(١) HUET PIERRE, op, cit, no.23.

(٢) د. مدحت رمضان، المرجع السابق، ص٧٧.

(٣) أضيفت بالقانون رقم (٣٧) لسنة ١٩٧٢م بشأن ضمان حريات المواطنين ( الجريدة الرسمية، العدد ٣٩ في ٢٨ أيلول سنة ١٩٧٢م.

السلكية واللاسلكية دون إذن بمقتضى المادة (٣٠٣) مكرر[١] من قانون العقوبات الجزائري حيث نصت على أنه: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من ٥٠٠٠٠ د.ج إلى ٣٠٠٠٠٠ د.ج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك عند:

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

التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه".

كما أنه عاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة.

ويضع صفح الضحية حداً للمتابعة الجزائية، باعتبار أن الضحية المتضرر من هذا الأمر قد صفح، وصفحه هذا يضع حداً للمتابعة[٢].

ويلاحظ أن المشرع الجزائري لم يورد نصوصاً تعاقب على اعتراض الاتصالات التي تتم عن طريق الكومبيوتر، فهو عاقب فقط على اعتراض الاتصالات السلكية واللاسلكية، وبالتالي عليه التدخل لوضع نصوص خاصة في هذا الشأن حتى لا يتركها لاجتهاد المحاكم[٣].

كما جرم المشرع السوداني فعل التنصت غير المشروع وعد كل من يتنصت على رسائل عن طريق شبكة المعلومات أو أجهزة الحاسوب وما حكمها أو يلتقطها أو يعترضها دون تصريح بذلك من النيابة العامة أو الجهة المختصة أو الجهة

---

(١) أدرجت المادة (٣٠٣) مكرر بموجب القانون رقم ٢٢/٦ المؤرخ في ٢٠٠٦/١٢/٢٠م، المعدل لقانون العقوبات الجزائري.

(٢) هلال آمنة، المرجع السابق، ص٦٥.

(٣) عائشة بن قارة مصطفى، المرجع السابق، ص١٦٩ - ١٧٠.

المالكة للمعلومة يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً[١].

كما نص المشرع الفلسطيني في المادة (٧) من قانون الجرائم الإلكترونية الفلسطيني رقم (١٦) لعام ٢٠١٧م، على أنه: " كل من التقط ما هو مرسل عن طريق الشبكة، أو إحدى وسائل تكنولوجيا المعلومات، أو سجله، أو اعترضه، أو تنصت عمداً دون وجه حق، يعاقب بالحبس، أو بالغرامة التي لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني أو بالعقوبتين كلتيهما".

وأيضاً نص المشرع الأردني في المادة (٣٤٧) من قانون العقوبات الأردني على أنه: " ١-من دخل مسكن آخر أو ملحقات مسكنه خلافاً لإرادة ذلك الآخر، وكذلك من مكث في الأماكن المذكورة خلافاً لإرادة من له الحق في إقصائه عنها عوقب بالحبس مدة لا تتجاوز الستة أشهر"، وكذلك نص المادة (٣٥٥) من قانون العقوبات الأردني التي جاء فيها: " يعاقب بالحبس مدة لا تزيد على ثلاث سنوات كل من: ١-حصل بحكم وظيفته أو مركزه الرسمي على أسرار رسمية وأباح هذه الاسرار لمن ليس له صلاحية الاطلاع عليها أو إلى من لا تتطلب طبيعة وظيفته ذلك الاطلاع وفقاً للمصلحة العامة. ٢- من كان يقوم بوظيفة رسمية أو خدمة حكومية واستبقى بحيازته وثائق سرية أو رسوماً أو مخططات أو نماذج أو نسخاً منها دون أن يكون له حق الاحتفاظ بها أو دون أن تقتضي ذلك طبيعة وظيفته. ٣-من كان بحكم مهنته على علم بسر وأفشاه دون سبب مشروع)، ولم يقتصر المشرع في حمايته لأسرار الأفراد على الاطلاع بطرق عادية بل شمل حتى الأسرار داخل المراسلات والبرقيات، فنصت المادة (٣٥٦) عقوبات أردني على أنه: " ١-يعاقب بالحبس من شهر إلى سنة كل شخص ملحق بمصلحة البرق والبريد يسيء استعمال وظيفته هذه بأن يطلع على رسالة مظروفه أو يتلف أو يختلس إحدى الرسائل أو يفضي بمضمونها إلى غير المرسل إليه. ٢- ويعاقب

---

(١) معمر علي إبراهيم محمد، المرجع السابق، ص٧٨.

بالحبس مدة ستة أشهر أو الغرامة حتى عشرين ديناراً من كان ملحقاً بمصلحة الهاتف وأفشى مخابرة اطلع عليها بحكم وظيفته أو عمله".

وبالتالي يمكن انطباق العقوبات التقليدية على هؤلاء المذكورين في النصوص السابقة، في حال اطلاعهم بحكم وظائفهم على أسرار المواطنين عبر أجهزة الحاسوب أو شبكاته من خلال أدائهم لوظائفهم[١].

وقرر المشرع البحريني في المادة (٢/١٦) من قانون جرائم تقنية المعلومات البحريني رقم (٦) لسنة ٢٠١٤م، على الأشخاص أو مزودي الخدمات الذين يقومون بإفشاء أي سر يتعلق بدليل من أدلة الدعوى أو حتى أخبار المتهم، وأيضاً أي محاولة من قبلهم للانتفاع من هذه الأدلة، عقوبة تصل في حدها الأقصى السجن مدة لا تزيد عن سنتين وغرامة لا تتجاوز مائة ألف دينار، وفي حال كان الشخص موظفاً عاماً أو مكلفاً بخدمة عامة، فإن العقوبة قد تصل إلى السجن في حدها الأقصى إلى خمس سنوات.

وأيضاً جرم المشرع القطري في المادة الرابعة من القانون رقم (١٤) لسنة ٢٠١٤م الخاص بمكافحة الجرائم الإلكترونية، فعل التنصت والالتقاط غير المشروع حيث نص فيها على أنه: " يعاقب بالحبس مدة لا تجاوز سنتين، وبالغرامة التي لا تزيد على (١٠٠,٠٠٠) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من التقط أو اعترض أو تنصت عمداً، دون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور".

كما عاقبت بعض القوانين على التنصت والاعتراض المتعمد للاتصالات إذا وقعت هذه الأفعال بشكل غير مشروع، حيث نص قانون الإمارات العربية المتحدة لمكافحة جريمة تقنية المعلومات رقم (٢) لعام ٢٠٠٦م، في المادة (٨) منه على

---

(١) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٨٥. معمر علي إبراهيم محمد، المرجع السابق، ص١٨٦.

أنه: " كل من تنصت أو التقط أو اعترض عمداً، دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، يعاقب بالحبس أو بالغرامة أو بإحدى هاتين العقوبتين".

**ونحن نرى أن هذه العقوبات تشمل الأشخاص المكلفون بالحصول على الدليل الإلكتروني عندما يحصلون عليه بإجراءات تفتقد إلى الضمانات التي تكفل مشروعيتها.**

وكذلك نصت المادة (٢٣) من قانون مكافحة الجريمة المعلوماتية السوري رقم (١٧) لعام ٢٠١٢م، على ما يلي:

" يُعاقَب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، كل من نشر عن طريق الشبكة معلومات تنتهك خصوصية أي شخص دون رضاه، حتى ولو كانت تلك المعلومات صحيحة".

**ونحن نرى أن نص المادة السابقة منتقد لأن المشرع السوري اشترط النشر عن طريق شبكة معلومات وحبذا لو لم يشترط ذلك.**

كما أن المشرع السوري نص على عقوبات جزائية في قانون العقوبات السوري على القائمين على أعمال التحقيق والذين يخالفون واجباتهم في الحصول على الأدلة بشكل غير مشروع، حيث نص في المادة (٥٦٥) من قانون العقوبات السوري لعام ١٩٤٩م، على أنه: " من كان بحكم وضعه، أو وظيفته، أو مهنته أو فنه على علم بسر وأفشاه دون سبب مشروع، أو استعمله لمنفعته الخاصة، أو لمنفعة آخر عوقب بالحبس سنة على الأكثر".

ونصت المادة (٥٦٦) من القانون نفسه على أن: " يعاقب بالحبس من شهرين إلى سنتين كل شخص ملحق بمصلحة البريد والبرق يسئ استعمال صفته هذه بأن يطلع على رسالة مختومة أو يتلف أو يختلس إحدى الرسائل أو يفضي بمضمونها إلى غير المرسل إليه".

كما نصت المادة (٥٦٧) من القانون نفسه على أن: " ١-كل شخص آخر يتلف أو يفض قصداً رسالة أو برقية غير مرسلة إليه أو يطلع بالخدعة على مخابرة هاتفية يعاقب بغرامة لا تتجاوز ألفي ليرة سورية. ٢- يقضى بالعقوبة نفسها على من اطلع على رسالة أو مخابرة برقية أو هاتفية في إذاعتها إلحاق ضرر بآخر فأعلم بها غير من أرسلت إليه".

**ونرى أن هذه العقوبات التي وردت في قانون العقوبات السوري تنطبق على الأشخاص الذين يطلعون على أسرار المواطنين بشكل غير مشروع عبر أجهزة الحاسوب وشبكات الاتصالات خلال القيام بأعمال وظيفتهم.**

وبذلك توفر قاعدة مشروعية الدليل حماية كافية لحرية الإنسان، إذا ما اتخذت ضده إجراءات ماسة بحريته من غير الطريق القانوني(١).

## ثالثاً: المؤيدات المدنية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني:

في جميع الحالات يرتب العمل المخالف للقانون لمن وقع عليه الحق بالتعويض(٢).

وتتمثل الحماية المدنية لحقوق الإنسان وضماناته الأساسية خلال مراحل الدعوى الجزائية في التعويضات المدنية المناسبة لإصلاح الضرر الذي أصاب الفرد نتيجة انتهاك القائم بأعمال التحقيق، والبحث عن الأدلة لتلك الحقوق الإنسانية خاصة ما تعلق منها بحق الفرد في حياته الخاصة(٣).

ومن أمثلة الحكم بالتعويض المدني لعدم مراعاة ضمانات التفتيش الواقع على نظم الحاسوب والإنترنت، ما قامت به قوات البوليس السري الأمريكي في

---

(١) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٥٣.

(٢) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص١٨٦.

(٣) د. محمد أمين الخرشة، المرجع السابق، ص٣٠٩.

شهر أذار لعام ١٩٩٠م، حيث قامت بتفتيش شركة ستيف جاكسون للألعاب وضبطت أجهزة حاسوب وملحقاتها ومجموعة من البرامج وكمية من الأسطوانات وملفات خاصة بجريدة إلكترونية، وكذلك آلة حاسبة شخصية ووضعت الأختام على المضبوطات، لاشتباه الشرطة بوجود صور فاضحة على الإنترنت مصدرها هذه الشركة، وقد تعرضت الشركة لخسائر مالية كبيرة ولم توجه تهمة لصاحب الشركة أو لأي من العاملين معه، لذلك قام صاحب الشركة بمطالبة البوليس السري الأمريكي بتعويضه عن الأضرار التي أصابته من هذا الإجراء، وفي النهاية تبين أن التفتيش لم يكن متعلقاً به أو بعمله، وأن أحد العاملين بالشركة كان الهدف من الإجراء والذي لم توجه له التهمة، وكانت المعلومات المطلوب ضبطها موجودة بمنزله، ولذلك حكم القضاء الأمريكي بتعويض ستيف جاكسون(١).

كذلك نتج عن الاستخدام غير المشروع للمراقبة الإلكترونية في التحقيقات الجنائية سعياً وراء الكشف عن الحقيقة، لما تحمله هذه المراقبة بين طياتها من تعديات وانتهاكات على حق الإنسان في حرمة حياته الخاصة، فقد أصبح الإنسان عارياً أمامها بما لديها من قدرة فائقة على اختراق حجز الخصوصية، والاطلاع على أخص شؤون حياته، دون علم منه، فمن يخضع لتطفل هذه الأجهزة لا يستطيع أن ينجو منها(٢).

وإن استخدام تلك الأجهزة – مدار البحث – في هذا المجال يحدث دائماً وأبداً ضرراً بالغاً، فالحقوق المحمية هنا تعني الاعتراف بنوع معين من القيم الإنسانية الضرورية، إذا فقدها الإنسان وجد الضرر بصورة كبيرة(٣).

---

(١) د. مدحت رمضان، المرجع السابق، ص ٧٣-٧٤. د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٧١.

(٢) د. محمد أمين الخرشة، المرجع السابق،ص٣١٠.

(٣) د. محمد أمين الخرشة، المرجع السابق،ص٣١٠.

ويتم الحصول على التعويض في حالات الاعتداء على حقوق الأفراد وضماناتهم الأساسية خلال إجراءات الدعوى الجزائية من خلال رفع دعوى التعويض العادية، وفقاً لقواعد القانون المدني ضد مسببه، كالتي ترفع ضد عضو الضابطة العدلية أو دعوى المخاصمة ضد القضاة أو أعضاء النيابة العامة، إذا وقع منهم غش أو تدليس أو خطأ مهني جسيم في عملهم(١).

## الفرع الثاني

## المؤيدات التأديبية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني

يتعرض الأشخاص المعهود إليهم بسلطة التحقيق الجنائي، والبحث عن الأدلة – سواء أكان قاضياً أم عضواً من أعضاء النيابة العامة، أم أحد أعضاء الضابطة العدلية – للمسؤولية التأديبية، إذا أخل بوجبات الوظيفة أو خالف ما تقضي به القوانين أو اللوائح التنظيمية، فاتخاذ أي إجراء من إجراءات التحقيق بشكل مخالف لما ينص عليه المشرع قد يترتب عليه عدم الاعتداد بما نتج عنه من أثار، وقد يترتب عليه مساءلة متخذه جنائياً، إذا كان فعله يشكل جريمة، بالإضافة إلى ذلك فإن مسلك الموظف بشكل مخالف للقانون يرتب مسؤوليته الإدارية، إذ يُعد مرتكباً لذنب إداري يسوغ للإدارة تأديبه، وذلك بتوقيع الجزاء المناسب عليه بحسب الشكل والأوضاع المرسومة قانوناً(٢).

وإن بحث المؤيدات التأديبية كجزاء لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني، يقتضي منا أولاً بيان مفهوم الجريمة التأديبية، وثانياً الحماية التأديبية في التشريعات.

---

(١) د. محمد أمين الخرشة، المرجع السابق، ص٣١١.

(٢) د. محمد أمين الخرشة، المرجع السابق، ص٢٩٤.

**أولاً: مفهوم الجريمة التأديبية:**

تعرف الجريمة التأديبية بأنها: "كل فعل أو امتناع يرتكبه الموظف ويجافي واجبات منصبه"(١). أو هي: "إخلال بواجبات الوظيفة إيجاباً أو سلباً، ويقصد بالواجبات تلك التي يقتضيها حسن انتظام واضطراد العمل في المرفق ولو لم يُنص عليها"(٢).

والجريمة التأديبية تختلف عن الجريمة الجزائية، فلا يلزم ثبوت مسؤولية الموظف جزائياً حتى يتم مساءلته تأديبياً. كما أن مصادر الحماية التأديبية ليست واحدة، فهي تتعدد حسب الجهات التي تباشر إجراءات التحقيق، وكل جهة من هذه الجهات تخضع في تنظيم شؤونها لتشريع معين، فقد يكون ذلك في قانون الإجراءات الجنائية، أو في اللوائح التي تضعها الهيئات المختصة، ومنها ماهو متعلق بقانون السلطة القضائية، بالإضافة إلى أن السلطة المختصة بالرقابة التأديبية تختلف باختلاف الموظف الذي ارتكب المخالفة الإدارية(٣).

**ثانياً: الحماية التأديبية في التشريعات:**

ففي التشريع **المصري**، واستناداً لنص المادة (٢٢) من قانون الإجراءات الجنائية المصري، فإن النائب العام له حق الإشراف على أعضاء الضابطة العدلية، فيما يتعلق بأعمال وظائفهم، حيث تنص تلك المادة على أن: "يكون مأمورو الضبط القضائي تابعين للنائب العام وخاضعين لإشرافه، فيما يتعلق بأعمال وظيفتهم، وللنائب العام أن يطلب إلى الجهة المختصة النظر في أمر كل من تقع منه مخالفات لواجباته، أو تقصير في عمله، وله أن يطلب رفع الدعوى التأديبية عليه، وهذا كله لا يمنع من رفع الدعوى الجنائية".

---

(١) د. سليمان الطماوي، القضاء الإداري، قضاء التأديب، د.ط، دار الفكر العربي، مصر، ١٩٧٧م، ص٤٩.

(٢) د. محمد جودت الملط، المسؤولية التأديبية للوظف العام، رسالة دكتوراه، جامعة القاهرة، القاهرة، مصر، ١٩٦٧م، ص٨٠.

(٣) د. محمد أمين الخرشة، المرجع السابق، ص٢٩٤ – ٢٩٥.

نستنتج من ذلك أنه إذا تبين لهذه السلطات أن عضو الضابطة العدلية إذا أهمل أو قصر أو ارتكب عملاً غير مشروع، فإنها تقوم بمساءلته إدارياً، إما بتوقيع جزاء إداري مباشر من السلطة الرئاسية، وإما بإحالته إلى مجلس التأديب.

كما نصت المادة (١/٤٧) من قانون الشرطة المصري رقم (١٠٩) لسنة ١٩٧١م، على أن: "كل ضابط يخالف الواجبات المنصوص عليها في هذا القانون أو في القرارات الصادرة من وزير الداخلية أو يخرج عن مقتضى الواجب في أعمال وظيفته أو يسلك سلوكاً، أو يظهر بمظهر من شأنه الإخلال بكرامة الوظيفة يعاقب تأديبياً".

وفي **التشريع الفرنسي**، فقد خول المشرع الفرنسي النائب العام في المادة (١٢) من قانون الإجراءات الجنائية سلطة الرقابة التأديبية على أعضاء الضابطة العدلية، حيث نصت على أنه: " تمارس الضابطة العدلية، تحت إشراف النائب العام، من قبل الضباط والمسؤولين والوكلاء المعينين في هذه الصفة "[(١)].

فله مجازاتهم عن الأخطاء التي تقع منهم نتيجة ممارستهم نشاط الضابطة العدلية، حيث تكون سلطة التأديب في هذه الحالة للجهاز الإداري الذي يتبعونه[(٢)]، والذي يوقع الجزاءات التأديبية بنفسه كالإنذار أو سحب أهلية الضابطة العدلية من العضو المخطئ، وإذا كان الخطأ المنسوب إلى عضو الضابطة العدلية جسيماً، فله أن يرفع أمر ذلك العضو إلى غرفة الاتهام[(٣)].

---

(١) Article 12 :

''La police judiciaire est exercée, sous la direction du procureur de la République, par les officiers, fonctionnaires et agents désignés au présent titre''.

موقع التشريعات الفرنسية:

https://www.legifrance.gouv.fr. تاريخ الدخول في ٢٠١٩/٣/١١م.

(٢) د. رضا عبد الحكيم إسماعيل رضوان، الضبط القضائي بين السلطة والمسؤولية، دراسة مقارنة مع التشريع الفرنسي، رسالة دكتوراه، أكاديمية الشرطة، القاهرة، مصر، ١٩٩٢م، ص٣٠٥.

(3) Leborgne G ; Le contrôle des actes des agents de la police judiciaire, R. S.C, 1987, PP .48 - 49.

وتنظم المواد (٢٣٠ – ٢٢٤) من قانون الإجراءات الجنائية الفرنسي أحكام الرقابة التأديبية التي تباشرها غرفة الاتهام على أعضاء الضابطة العدلية، حيث تباشر رقابتها بناء على طلب من النيابة العامة، أو من تلقاء نفسها من خلال ما يتكشف لها من فحص الإجراءات التي تفرض عليها[١]، ولها أن تقوم بإجراء تحقيق تستمع فيه لأقوال النيابة العامة، وعضو الضابطة العدلية المخالف وله الحق في الاطلاع على ملف التحقيق للتعرف على ما نسب إليه، وله أن يستعين بمحام للدفاع عنه[٢]، ولغرفة الاتهام إذا ثبت لها ارتكاب عضو الضابطة العدلية للمخالفة المنسوبة إليه أن توقع عليه عقوبة المنع النهائي، أو المؤقت عن ممارسة وظيفة الضابطة العدلية، والجزاءات التي يحكم بها على عضو الضابطة العدلية تبلغ بواسطة النيابة العامة للسلطات المعنية بعضو الضابطة العدلية، وللجهة الإدارية التي يتبعها عضو الضابطة العدلية أن تحقق معه بشأن المخالفة التي ارتكبها أثناء قيامه بوظيفته القضائية، ولها أن توقع عليه العقوبة التأديبية التي تتناسب مع جسامة المخالفة[٣].

وفي التشريع السوري نصت الفقرة (٢) من المادة (٨٩) من قانون أصول المحاكمات الجزائية السوري على أنه: " إن دخول القاضي أحد المنازل بحال عدم توفر الشروط المذكورة آنفاً يعتبر تصرفاً تعسفياً من شأنه فسح المجال للشكوى من الحكام".

**ومن هذه المادة نستنتج أن المشرع السوري أخذ بالمسؤولية التأديبية للمحققين الذين لا يراعوا ضمانات وضوابط التفتيش وهذا النص يطبق على عدم مراعاة ضمانات التفتيش الإلكتروني بغرض الحصول على الدليل الإلكتروني، وأيضاً في حال عدم مراعاة ضمانات الحصول عليه في الإجراءات الأخرى.**

---

(١) المادة (٢٢٥) من قانون الإجراءات الجنائية الفرنسي.

(٢) المادة (٢٦٦) من قانون الإجراءات الجنائية الفرنسي.

(3) Leborgne G ;Op,cit,PP.49.

ونحن نرى أن قاعدة استبعاد الأدلة الإلكترونية المتحصلة بطرق غير مشروعة أي تقرير بطلانها هو الوسيلة المثلى لاحترام حقوق الإنسان وحرياته المنصوص عليها في جميع الدساتير والقوانين، وذلك لأن الوسائل الأخرى لا تحول دون قيام رجال السلطة العامة من انتهاك حقوق الأفراد وحرمة حياتهم الخاصة، إذ من النادر من الناحية العملية أن يُقدم أحدهم إلى القضاء، وأن يوقع عليه جزاء، سواء أكان عقابياً أم مدنياً أم إدارياً، ولهذا كان استبعاد الأدلة الباطلة أكثر جدوى، لأن علم رجل السلطة العامة سلفاً بنتيجة الإجراء الباطل الذي يقوم به وهو طرح القضاء للدليل وعدم الأخذ به كفيل بحمله على الكف عن مخالفة القانون حتى لا يذهب جهده سدى.

وفي هذا المبحث قمنا بدراسة مؤيدات عدم مشروعية إجراءات الحصول على الدليل الإلكتروني، فدرسنا المؤيدات الإجرائية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني، وتبين لنا أن هذا الجزاء هو بطلان الإجراء غير المشروع بغرض الحصول على الدليل الإلكتروني، وكذلك درسنا المؤيدات العقابية والمدنية والتأديبية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني، وتبين لنا أن يترتب مسؤولية جزائية ومدنية وتأديبية على الأشخاص المكلفين بالحصول على الدليل الإلكتروني في حال مخالفتهم الضمانات المقررة لإجراءات الحصول على الدليل الإلكتروني.

وبعد أن انتهينا في هذا المبحث من دراسة المؤيدات الإجرائية والمؤيدات العقابية والمدنية التأديبية للدليل الإلكتروني غير المشروع، سننتقل لدراسة نطاق العمل بالدليل الإلكتروني في المبحث الثاني.

# المبحث الثاني
# نطاق العمل بالدليل الإلكتروني

من أهم الآثار المترتبة على الاعتراف بمشروعية الدليل الإلكتروني في مجال الإثبات الجزائي هو معرفة نطاق العمل به، ومدى الاستفادة منه في إثبات الجرائم، فهل يقتصر العمل فيه فقط في نطاق الجرائم الإلكترونية أم يمتد إلى الجرائم التقليدية أيضاً؟

وسنتناول في هذا المبحث نطاق العمل بالدليل الإلكتروني، وذلك بمعرفة الجرائم التي يصلح الدليل الإلكتروني ليكون دليلاً لإثباتها، وبناء على ذلك سنقسم هذا المبحث إلى المطلبين التاليين:

**المطلب الأول: نطاق العمل بالدليل الإلكتروني في الجرائم الإلكترونية.**

**المطلب الثاني: نطاق العمل بالدليل الإلكتروني في الجرائم التقليدية.**

## المطلب الأول
## نطاق العمل بالدليل الإلكتروني
## في الجرائم الإلكترونية

تُعرَّف الجريمة في نطاق القانون الجزائي بأنها: "السلوك الإنساني المحظور الذي يخل بأمن المجتمع وسلامته، أو كل فعل أو تصرف أو ترك حرمه المشرع، وقرر له العقوبة المناسبة أو التدابير الاحترازية أو الاصلاحية".

وأغلب التشريعات العربية جاءت بتعريفات للجريمة مكتفية بالنصوص التي تبين مختلف الجرائم، ووضع تعريف عام للجريمة أمر لا فائدة منه، لأن المشرع يقرر الفعل الذي يُعد جريمة، ويحدد العقوبة المقررة لكل من يرتكب هذا الفعل، حيث أن وضع تعريف محدد للجريمة لن يأتي جامعاً لكل المعاني المطلوبة، لأن

موضوع الجريمة يتبدل بتبدل الأزمنة والأمكنة والشعوب والحضارات ومراحل تطورها[١].

وتُعد الجرائم الإلكترونية[٢] ظاهرة حديثة نسبياً قياساً بغيرها من الجرائم التقليدية في العالم بشكل عام، وفي العالم العربي بشكل خاص، وربما مرد ذلك إلى أن الدول العربية حديثة العهد بتقنيات الحاسوب، وحينما يكون الحديث عن الدليل الإلكتروني، ففي المقابل يجب أن يكون الحديث عن الجريمة الإلكترونية التي تُعد نطاقاً للعمل بالدليل الإلكتروني، أو محلاً له[٣].

وهذا يتطلب منا تحديد ماهية الجرائم الإلكترونية، ومن ثم بحث ملاءمة إثباتها بالدليل الإلكتروني، وأخيراً الحجج المبررة لإثباتها بالدليل الإلكتروني، لذلك لا بد لنا من تقسيم هذا المطلب إلى ثلاثة فروع نبحث في:

**الفرع الأول: ماهية الجرائم الإلكترونية (Cyber Crime).**

**الفرع الثاني: ملاءمة الدليل الإلكتروني لإثبات الجريمة الإلكترونية.**

**الفرع الثالث: الحجج المبررة لملاءمة إثبات الجريمة الإلكترونية بالدليل الإلكتروني.**

---

(١) خالد عياد الحلبي، المرجع السابق، ص٢٦.

(٢) للتوضيح الجرائم الإلكترونية هي الجرائم المتعلقة بالحاسوب والانترنيت، فاصطلاح الجرائم الإلكترونية عام ويشمل التقنيات الحالية والمستقبلية كلها المستخدمة في التعامل مع المعلومات بما في ذلك الحاسوب وشبكة الانترنت مع ملاحظة أن جريمة الحاسوب هي الجريمة التي تقع بواسطة الحاسوب أو على مكوناته المادية والمعنوية، أما جرائم الانترنت فهي الجرائم العابرة للحدود والتي ترتكب بواسطة الانترنيت أو عليه من شخص ذا دراية فائقة بها. أنظر: أ.م. جاسم خريبط خلف، المرجع السابق، ص١٤.

(٣) هلال آمنة، المرجع السابق،ص٢٣.

## الفرع الأول

## ماهية الجرائم الإلكترونية (Cyber Crime)[١]

تجدر الإشارة إلى أنه لا توجد تسمية موحدة للدلالة على هذه الظاهرة الإجرامية، فهناك تباين في التسميات التي أطلقت عليها[٢]، وقد يكون مرد هذا الأمر إلى نشأة وتاريخ وتطور تكنولوجيا المعلومات، وكذلك اختلاف وجهات النظر بين المتخصصين في مجال الإعلام، وأيضاً بين رجال القانون وعلماء النفس والاجتماع[٣].

**ونحن نرى بضرورة وضع مصطلح موحد وشامل لهذه الجرائم وذلك بتوحيد هذه التسميات تحت مسمى الجرائم الإلكترونية لدلالتها على هذه الجرائم بدقة وذلك لأنها تنشأ في وسط افتراضي أو إلكتروني.**

إن دراسة ماهية الجرائم الإلكترونية، يقتضي أولاً، تعريف الجرائم الإلكترونية، وثانياً، محل الجرائم الإلكترونية، وثالثاً، أنواع الجرائم الإلكترونية، ورابعاً، تصنيف الجرائم الإلكترونية، وخامساً، الخصوم في الجرائم الإلكترونية.

**أولاً: تعريف الجرائم الإلكترونية:**

إن الجرائم الإلكترونية، تقاوم التعريف، ولا مصطلح متفق عليه للدلالة عليها، ويعزى ذلك إلى أن ما انشغل من الكتابات بتناولها شرحاً وتوضيحاً لأساليب

---

(١) النطاق (Cyber) نطاق ذو دلالة على شبكة الإنترنت، يحدد بأن الكلمة التي ستلي هذا النطاق لها علاقة بالإنترنت مثل (Cyber Café) مقهى إلكتروني للإنترنت، (Cyber Cash) نقود إلكترونية، وهكذا. د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١٨.

(٢) ومن هذه التسميات جرائم الكومبيوتر والانترنت، وجرائم التقنية العالية، والجريمة الإلكترونية، والاحتيال المعلوماتي،والجريمة المعلوماتية، و الجرائم عبر الكومبيوترcyber crime، وجرائم أصحاب الياقات البيضاء، وغيرها من التسميات. د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١٨، وجعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، الطبعة الأولى، دار البداية، عمان، الأردن، ٢٠١٠م، ص١٠٧ – ١٠٨.

(٣) هلال آمنة، المرجع السابق،ص٢٣.

ارتكابها وبياناً لأنواعها ووسائل مكافحتها يزخر، حسب تعبير البعض، "بملايين الكلمات"، التي سطرت في محاولات عديدة لصياغة ودحض تعاريفها[١]، وسنعرض تعريف الجريمة الإلكترونية، وذلك بعرض التعريف الفقهي ، ومن ثم التعريف التشريعي.

**أ-التعريف الفقهي للجريمة الإلكترونية:**

بدايةً هنالك صعوبة يواجهها الفقه في تعريف الجريمة الإلكترونية – لها أسبابها- فالظاهرة الإجرامية برمتها المتصلة بالحاسوب جديدة، والاجتهاد التشريعي والقضائي والفقهي مازال في بدايته، والاتفاق حول تحديد الأفعال المتضمنة في هذه الظاهرة والحق المعتدى عليه، حتى حجم مخاطرها لم يتحدد حتى الآن، لهذه الأسباب ولأسباب أخرى يبدو من الصعب تحديد حجم الجريمة الإلكترونية والإرادة الجرمية والشروع فيها[٢].

وبالنسبة لتعريف الجريمة الإلكترونية يرى جانب من الفقه[٣] أن تعريفها يجب أن يكون من الناحية الفنية والقانونية، فالتعريف الفني لها هو: "نشاط إجرامي تستخدم فيه تقنية الحاسوب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود".

أما التعريف من الناحية القانونية فيتطلب تعريف المفردات الضرورية المتعلقة بأركان جرائم الحاسوب الآلي[٤].

---

(١) د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، المرجع السابق، ص٤٠٦.

(٢) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٦٤.

(٣) د.عبد الفتاح بيومي حجازي، جرائم الكومبيوتر والإنترنت، بهجات للطباعة والتجليد، القاهرة، مصر، ٢٠٠٩م، ص١.

(٤) هلال آمنة، المرجع السابق،ص٢٤.

وهناك تعريفات مختلفة تستند إلى معايير مختلفة بالنظر إلى موضوعها أو وسيلة ارتكابها أو حسب توافر المعرفة بتقنية المعلومات أو استناداً لمعايير أخرى حسب القائلين بها، ومن أهم هذه التعريفات:

**١-التعريف المستند إلى موضوع الجريمة "الاتجاه الموضوعي":**

هناك مجموعة من التعريفات استندت إلى موضوع الجريمة وإلى أنماط السلوك محل التجريم، فالذين يُعرِّفون الجريمة الإلكترونية بالنظر إلى موضوعها، لا ينظرون للحاسوب الآلي بوصفه أداة ارتكاب الجريمة الإلكترونية، بل إن الجريمة تقع على الحاسوب الآلي ذاته، وقد تقع داخل نظامه، ومن أمثلة هذه التعريفات تعريف الأستاذ (Rosblat): "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تُحول عن طريقه"[١].

**لكن نرى أن هذا التعريف يقصر موضوع الجرائم الإلكترونية على مكونات الحاسوب فقط ولا يشمل الجرائم التي تقع على الإنترنيت.**

أو هي حسب تعريف الدكتورة هدى قشقوش بأنها: "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"، أو هي كما عرفها الأستاذ (Artar Solerz) "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطاً بتقنية المعلومات"[٢].

كما عرَّفها مكتب المحاسبة العامة للولايات المتحدة الأمريكية (GOA) بأنها: "الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام

---

(١) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص ١٨. وخالد عياد الحلبي، المرجع السابق، ص ٢٨.

(٢) خالد عياد الحلبي، المرجع السابق، ص ٢٨.

المخرجات، إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيداً من الناحية التقنية مثل تعديل الكومبيوتر"[١].

وأيضاً عرفت بأنها: "سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها"[٢].

وعُرفت منظمة التعاون الاقتصادي والتنمية (OCDE)؛ الجريمة الإلكترونية في اجتماع باريس عام (١٩٨٣م) بأنها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرَّح به، يتعلَّق بالمعالجة الآلية للبيانات أو بنقلها"[٣].

لكن هنالك من انتقد تعريف منظمة التعاون الاقتصادي والتنمية (OCDE) [٤]– ونحن نؤيده – لأنه فيه من المرونة والسلوك الذي لا يرتب سوى استهجانه أخلاقياً، ذلك أن لا تلازم دائماً مابين الفعل المستهجن أخلاقياً، وذلك المؤثم قانوناً.

وهناك من يرى[٥] – ونحن نؤيده – إلى أن معيار موضوع الجريمة كأساس للتعريف يُعد من أهم المعايير وأكثرها قدرة على إيضاح طبيعة ومفهوم الجريمة محل التعريف، إلا أن هذا المعيار لا يحيط بكل الأفعال المشكلة للجريمة الإلكتروني، وإذا سعى إلى الإحاطة بها فإنه سيغرق بالتفصيل الذي لا يستقيم وغرض وشكل التعريف، هذا بالإضافة إلى عدم وجود اتفاق حتى الآن، على الأفعال المنطوية تحت وصف الجرائم الإلكترونية.

---

(١) خالد عياد الحلبي، المرجع السابق، ص ٢٨ – ٢٩.

(٢) د. علي القهوجي، الحماية الجنائية لبرامج الحاسوب، د.ط، الدار الجامعية للنشر، الإسكندرية، مصر، ١٩٩٧م، ص٢.

(٣) هذا التعريف اقترحه مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية كأساس للنقاش في اجتماع عقد بباريس في عام ١٩٨٣م، وذلك لبحث الجريمة المرتبطة بالمعلوماتية.

(٤) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص ١٩.

(٥) د. عيسى مدالله المخول، المرجع السابق، ص١٦.

**٢-التعريف المستند إلى أداة ارتكاب الجريمة "الاتجاه الفني":**

يرى أصحاب هذا الاتجاه، أنه لابد لقيام الجريمة الإلكترونية، من أن يكون الحاسوب هو وسيلة ارتكابها [١]، مثل التعريف الذي جاء به الفقيه الألماني "تيدمان" الذي عرفها بأنها: "كل أشكال السلوك غير المشروع – أو الضار بالمجتمع – الذي يرتكب باستخدام الحاسوب".

وعرفها " توم فوريستر" بأنها " فعل إجرامي يتم باستخدام الحاسوب كأداة رئيسية"[٢].

أو هي "الجرائم التي تلعب فيها البيانات الكومبيوترية والبرامج المعلوماتية دوراً رئيساً"، وذلك حسب تعريف مكتب تقييم التقنية في الولايات المتحدة الأمريكية، أو هي "فعل إجرامي يستخدم الحاسوب في ارتكابه كأداة رئيسية"[٣]. أو هي "تلك الجرائم التي يكون قد حدث في مراحل ارتكابها بعض عمليات فعلية داخل الحاسوب"[٤].

ويبدو أن هذا الاتجاه هو ما تبناه " نظام مكافحة جرائم المعلوماتية السعودي" رقم (٧٩) الصادر في (١٤٢٨/٣/٧هـ) بالقول " الجريمة المعلوماتية، أي فعل يرتكب متضمناً الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[٥]، وكذلك القانون المصري النموذجي الموحد الخاص بمكافحة سوء

---

(١) د. عمار عباس الحسيني، جرائم الحاسوب والإنترنت الجرائم المعلوماتية، الطبعة الأولى، منشورات زين الحقوقية، بيروت، لبنان، ٢٠١٧م، ص٣٧.

(٢) د. عمار عباس الحسيني، المرجع السابق، ص٣٧.

(٣) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص ١٨.

(٤) هلال آمنة، المرجع السابق،ص٢٤.

(٥) الفقرة الثامنة من المادة الأولى منه والتي اختصت بتعريف أهم الألفاظ الواردة في هذا النظام.

استخدام تكنولوجيا المعلومات والاتصالات الذي عرَّفها في المادة الأولى منه بأنها: "كل فعل مؤثم يتم ارتكابه عبر أي وسيط إلكتروني".

والاعتماد في تعريف الجريمة الإلكترونية على الوسيلة المستخدمة في ارتكابها يوجه إليه نقداً مفاده أنه: "لكي نعرف الجريمة يجب الرجوع إلى العمل الأساسي المكون لها وليس، فحسب إلى الوسائل المستخدمة لتحقيقه". وليس لمجرد أن الحاسوب قد استخدم في جريمة كما يقول فريق آخر، يتعين أن نعدها من الجرائم الإلكترونية(١). ويعزز هذا النقد الأستاذ اندرسون بقوله أنه (ليس لمجرد أن الحاسوب قد استخدم في جريمة، يمكن أن نعتبرها من الجرائم المعلوماتية) (٢).

كما انتقدت هذه التعريفات لأنها عامة وواسعة وتدخل فيها أيضاً الجرائم التقليدية، كما أنها غير منطقية(٣).

**ونحن نرى أن هذه التعاريف تقصر هذه الجرائم على التي ترتكب على الحاسوب فقط مع أنه يمكن أن ترتكب أيضاً بواسطة أجهزة أخرة كالهاتف النقال(٤) وكذلك بواسطة شبكة الإنترنيت.**

**٣-التعريف المستند إلى المعرفة التقنية لدى مرتكب الجريمة " الاتجاه الشخصي":**

هو ما يسمى بـ" بالمعيار الشخصي" والذي يتطلب لقيام الجريمة الإلكترونية، أن يكون الفاعل ملماً بتقنية المعلومات(٥)، أي حسب هذا الاتجاه أن الجرائم الإلكترونية، هي تلك التي يكون لمقترفها معرفة كافية بالحاسوب

---

(١) أ. د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، المرجع السابق، ص٤٠٦.

(٢) د. عيسى مدالله المخول، المرجع السابق، ص١٧.

(٣) هلال آمنة، المرجع السابق،ص٢٤.

(٤) بات عمل العديد من أجهزة الهاتف النقال مماثلاً لعمل جهاز الحاسوب كالاتصال بشبكة الإنترنت والاستفادة من البرامج المتاحة التي تتم من خلالها العديد من الجرائم الإلكترونية.

(٥) د. عمار عباس الحسيني، المرجع السابق، ص٣٨.

ومشتملاته[١]، ومن التعريفات التي تقوم على أساس سمات شخصية لمرتكب الفعل، حيث عرفَّتها وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام ١٩٨٩م، فجاء في التعريف المقترح منها: "أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها"[٢].

وكذلك عرفها (DAVID THOMPSON) بأنها: "أية جريمة يكون متطلباً لاقترافها، أن يتوافر لدى فاعلها معرفة بتقنية الحاسوب"[٣].

ومن هذه التعريفات أيضاً: "الجرائم التي تتطلب إلماماً خاصاً بتقنيات الحاسوب ونظم المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعليها على الجريمة"[٤].

ومع ذلك فقد انتقد البعض[٥] هذا الاتجاه الأخير في تعريف الجريمة الإلكترونية بالقول " أن هذا الاتجاه يُضيق على نحو كبير من الجريمة الإلكترونية.... وإن الجريمة الإلكترونية من وجهة نظر هذا الاتجاه سوف تصبح أشبه بالخرافة، فهذا الاتجاه يحصر الجريمة الإلكترونية في الحالات التي تتطلب قدراً كبيراً من المعرفة التقنية في ارتكابها، وهو إن تحقق في بعض الأحوال، فإنه لا يتحقق في كثير منها، ففي كثير من الحالات يرتكب الجناة الفعل الإجرامي دون الحاجة إلى هذا القدر الكبير من المعرفة والخبرة....".

كما يذهب بعض الفقه [٦] في معرض تقدير هذه التعريفات المستندة إلى شخصية الفاعل إلى القول: " أن شرط المعرفة التقنية، شرط شخصي متصل

---

(١) خالد عياد الحلبي، المرجع السابق، ص ٢٩.

(٢) هلال آمنة، المرجع السابق،ص٢٤.

(٣) David Thompson, current trends in computer crime, computer control quarterly, vol, 9, no, I, 1991, P.2.

(٤) هلال آمنة، المرجع السابق،ص٢٤.

(٥) د. عمار عباس الحسيني، المرجع السابق، ص٣٩.

(٦) د. عيسى مدالله المخول، المرجع السابق، ص١٧-١٨.

بالفاعل، غير أن هذه الجرائم في أمثلة عديدة يُرتكب جزء كبير منها من قبل مجموعة تتوزع أدوارهم بين التخطيط والتنفيذ والتحريض والمساهمة، وقد لا تتوفر لدى بعضهم المعرفة بتقنية المعلومات، ثم ما هي حدود المعرفة التقنية، وماهو معيار وجودها للقول بقيام الجريمة؟؟؟ أن التطور الذي شهدته وسائل التقنية نفسها أظهر الاتجاه نحو تبسيط وسائل المعالجة وتبادل المعطيات، وتحويل الأجهزة المعقدة فيما سبق إلى أجهزة تكاملية سهلة الاستخدام حتى ممن لا يعرف شيئاً في علوم الحاسوب، ولم يعد مطلوباً العلم والمعرفة العميقين ليتمكن شخص من إرسال آلاف رسائل البريد الإلكتروني دفعه واحدة إلى أحد المواقع لتعطيل عملها، كما لم يعد صعباً أن يضمن أي شخص رسالة بريدية فيروساً التقطه كبرنامج عبر الإنترنت أو من خلال صديق فيبثه للغير دون أن يكون عالماً أصلاً بشيء مما يتطلبه بناء مثل هذه البرامج الشريرة، كما أن ما يرتكب الآن باستخدام الهاتف الخلوي من أنشطة اختراق واعتداء أو ما يرتكب عليها من قبل أجهزة مماثلة يعكس عدم وجود ذات الأهمية للمعرفة التقنية أو الدراية بالوسائل الفنية".

**ونرى أنه على الرغم من المحاولات الفقهية لوضع تعريف للجرائم الإلكترونية إلا أنها جميعها كانت قاصرة لأنها تعتمد على معيار واحد، ولم تستطع من وضع تعريف جامع مانع، وهذا مرده إلى أن هذا النوع من الجرائم معقد وصعب وفي تطور دائم.**

وأمام قصور التعريفات المؤسسة على معيار واحد، سواء القائمة على معيار قانوني موضوعي أو فني أو شخصي، برز عدد من التعريفات التي ترتكز على أكثر من معيار لبيان الجريمة الإلكترونية، فقد جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا سنة ٢٠٠٠م، تعريف للجرائم الإلكترونية كما يلي: "يقصد بالجريمة المعلوماتية أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي،

والجريمة تلك تشمل من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[١].

ومن هذه التعريفات، ما يقرره الأستاذ جون كارول ويتناه الأستاذ جيون جرين من أن الجريمة الإلكترونية هي" أي عمل ليس له في القانون جزاء، يضر بالأشخاص أو الأموال، ويوجه ضد أو يستخدم التقنية المتقدمة لنظم المعلومات".

ويعتمد هذا التعريف معايير عدة، أولها، عدم وجود جزاء لمثل هذه الأفعال. وثانيهما، تحقيق الضرر للأشخاص أو الأموال. وثالثهما، توجه الفعل ضد أو استخدام التقنية المتقدمة لنظم المعلومات، وهو معيار يعتمد محل الجريمة (تقنية نظم المعلومات) ووسيلة ارتكابها (أيضاً تقنية نظم المعلومات) أساساً للتعريف[٢].

وقد عُرف الجريمة الإلكترونية خبراء متخصصون من بلجيكا بأنها: " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".

والتعريف البلجيكي السالف، متبنى من قبل العديد من الفقهاء والدارسين بوصفه لديهم أفضل التعريفات لأن هذا التعريف واسع يتيح الإحاطة الشاملة قدر الإمكان بظاهرة جرائم التقنية، ولأن التعريف المذكور يُعبر عن الطابع التقني الذي تنطوي تحته أبرز صورها، ولأنه أخيراً يتيح إمكانية التعامل مع التطورات المستقبلية التقنية.

وبالرجوع إلى التعريف المتقدم يلاحظ إلى أنه يشير إلى إمكان حصول الجريمة الإلكترونية بالامتناع، وحسناً فعل ذلك، إذ أغفلت معظم التعريفات الإشارة إلى شمول السلوك الإجرامي للجرائم الإلكترونية صورة الامتناع رغم تحقق السلوك بهذه الطريقة في بعض صور هذه الجرائم[٣].

---

(١) مؤتمر الأمم المتحدة لمنع الجريمة ومعاقبة المجرمين، فيينا ١٠ – ١٧ نيسان ٢٠٠٠م.

(٢) د. عيسى مدالله المخول، المرجع السابق، ص١٨.

(٣) د. عيسى مدالله المخول، المرجع السابق، ص١٩.

ومـن الفقـه الفرنسـي، يُعـرف الفقيـه ماسـي الجريمـة الإلكترونيـة بأنهـا: " الاعتداءات غير القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح".

والجرائم الإلكترونية لدى هذا الفقيه تعتمد على معيارين: أولهما الوسيلة (بواسطة المعلوماتية) أما المعيار الثاني، المتمثل بالهدف من الجريمة وهو تحقيق الربح، وينتقد بعض الفقه[١] –وهو محق في ذلك– هذا التعريف في أن الاعتداء في كثير من الجرائم الإلكترونية ينصب على المعلومات في ذاتها دون السعي لتحقيق الربح، ودونما أن تكون المعلومات مجسدة لأموال أو لأصول، عوضاً عن عدم صواب اعتبار المعلومات في ذاتها مالاً مالم يقر النظام القانوني هذا الحكم لها لدى سعيه لتوفير الحماية للمعلومات.

وهناك من عُرفها بأنها: "كل عمل أو امتناع يأتيه الإنسان إضراراً بمكونات الحاسوب المادية والمعنوية، وشبكات الاتصال الدولية للمعلومات باعتبارها من المصالح الوطنية التي توجب الحماية الجنائية لها"[٢].

وهكذا نستخلص أن هناك طائفتين من تعريفات الجريمة الإلكترونية:

–أولهما، طائفة التعريفات التي تقوم على معيار واحد، وهذه تشمل تعريفات قائمة على معيار قانوني، كتعريفها بدلالة موضوع الجريمة أو السلوك محل التجريم أو الوسيلة المستخدمة، وتشمل أيضاً تعريفات قائمة على معيار شخصي، وتحديداً تطلب توافر المعرفة والدراية التقنية لدى شخص مرتكبها.

– وثانيهما، طائفة التعريفات القائمة على تعدد المعايير، وتشمل التعريفات التي تُبرز موضوع الجريمة وأنماطها وبعض العناصر المتصلة بآليات ارتكابها أو بيئة ارتكابها أو سمات مرتكبها.

---

(١) د. عيسى مدالله المخول، المرجع السابق،ص٢١.

(٢) خالد عياد الحلبي، المرجع السابق، ص ١٥.

**ونحن بدورنا نميل ونؤيد تعريف الجريمة الإلكترونية حسب المعيار الموضوعي والفني معاً، لأنهما يصلحان معاً لكل الجرائم الإلكترونية، ومنها التحريض المعلوماتي والاختلاس المعلوماتي والاحتيال المعلوماتي وما شابهها من الجرائم التي لا يشترط أن تقع على بيانات إلكترونية فحسب وإنما لابد لقيامها أن تقع عن طريق الحاسوب الإلكتروني وما في حكمه من الأجهزة التقنية الأخرى، ونعارض الاتجاه الذي يجعل من الجريمة الواقعة على ماديات جهاز الحاسوب جريمة إلكترونية كسرقته أو أتلافه وماشابه، لأنها جرائم عادية تخضع للنصوص التقليدية في قانون العقوبات، كما نرفض الاتجاه الشخصي والذي يتطلب المعرفة التقنية للمجرم المعلوماتي لأنها الجرائم الإلكترونية من الممكن ارتكابها من أشخاص لا يتوافر بهم أي قدر من المعرفة التقنية.**

**وبالتالي يمكننا أن نعرف الجريمة الإلكترونية بأنها: " سلوك إيجابي أو سلبي يقع بواسطة الحاسوب الإلكتروني أو أي جهاز تقني آخر أو بواسطة شبكة الإنترنت ويكون السلوك فيها مستهدفاً المكونات المعنوية كالبرامج والبيانات والمعلومات الإلكترونية).**

**ب-التعريف التشريعي للجريمة الإلكترونية:**

انقسمت الدول في تجريمها للجرائم الإلكترونية إلى اتجاهين رئيسين:

**١-الاتجاه الأول: دول سنت تشريعات جديدة لتجريم الجرائم الإلكترونية:**

اتجهت كافة الدول المتقدمة تكنولوجياً إلى استخدام نصوص قانونية جديدة تُجَّرم الجرائم الإلكترونية، ومن أهم هذه الدول:

- **السويد:** والتي تُعد من أوائل الدول التي اتجهت إلى سن تشريعات قانونية جديدة خاصة بجرائم الإنترنت والحاسوب الآلي، حيث صدر أول قانون خاص بها سمي بقانون (البيانات) وقد صدر هذا القانون عام ١٩٧٣م.

– **الولايات المتحدة الأمريكية**، وهي الدولة الثانية التي تبعت السويد في إصدار قوانين خاصة بها تجرم الجرائم الإلكترونية حيث شرعت قانوناً خاصاً بحماية أنظمة الحاسوب الآلي (١٩٧٦–١٩٨٥م) وفي عام ١٩٨٦ م، صدر قانوناً آخر يحمل الرقم (١٢١٣) عرف المصطلحات الضرورية لتطبيق القانون على الجرائم الإلكترونية كما وضع المتطلبات الضرورية اللازمة لتطبيقه، وعلى أثر ذلك قامت الولايات الداخلية بإصدار التشريعات بكل منها على حدة للتعامل بها مع تلك الجرائم ومن تلك القوانين القانون الخاص بولاية تكساس لجرائم الحاسوب الآلي.

– **بريطانيا:** حيث أصدرت قانون إساءة استخدام الحاسوب لسنة ١٩٩٠م، وبدء سريانه بتاريخ ١٩٩٠/٨/٢٩م.

– **إيطاليا:** أصدرت قانون تكنولوجيا المعلومات والاتصالات في تشرين الثاني ١٩٩٧م، وهناك قانون سابق لجرائم الحاسوب ١٩٩٢م.

–**الإمارات:** أصدرت الإمارات قانون الأمارات الاتحادي رقم (٢) لسنة ٢٠٠٦م، في شأن مكافحة جرائم تقنية المعلومات.

– **السعودية:** أصدرت السعودية نظام مكافحة جرائم المعلوماتية عام ٢٠٠٧م.

– **قطر:** أصدر المشرع القطري القانون رقم (١٤) لسنة ٢٠١٤ م، الخاص بمكافحة الجرائم الإلكترونية.

–**فلسطين:** أصدر المشرع الفلسطيني قانون الجرائم الإلكترونية رقم (١٦) لسنة ٢٠١٧م.

– **سورية:** أصدر المشرع السوري قانون مكافحة الجريمة المعلوماتية وتنظيم التواصل عبر الشبكة رقم (١٧) لعام ٢٠١٢م[١].

---

(١) تضمن الفصل الثالث من قانون مكافحة الجريمة المعلوماتية السوري النماذج القانونية لمختلف صور الجريمة المعلوماتية وهي: ( جريمة الدخول غير المشروع إلى منظومة معلوماتية وجريمة شغل موقع إلكتروني وجريمة إعاقة الوصول إلى الخدمة وجريمة اعتراض المعلومات وجريمة تصميم البرمجيات الخبيثة واستخدامها وجريمة إرسال البريد الواغل

**٢-الاتجاه الثاني: دول اتجهت إلى تعديل قانون العقوبات لديها بإضافة نصوص خاصة بالجرائم الإلكترونية:**

ومن هذه الدول:

-**فرنسا:** وهي الدولة التي اهتمت بتطوير القوانين الخاصة بها للملاءمة مع جرائم التكنولوجيا الحديثة- جرائم الإنترنت- فقد طورت فرنسا قوانينها الجزائية لتتوافق مع المستجدات الإجرامية حيث أصدرت أول قانون خاص بها في ١٩٩٨/١/٥م القانون رقم (٨٨-١٩) والذي أضاف إلى قانون العقوبات الجزائي في المادة (٤٦٢) منه جرائم الحاسوب الآلي والعقوبات المقررة لتلك الجرائم كما تم في عام ١٩٩٣م، تعديل قانون العقوبات لديها ليشمل مجموعة جديدة من القواعد القانونية الخاصة بالجرائم الإلكترونية[١].

-**أستراليا:** عدل المشرع قانون العقوبات في عام ١٩٨٣م، بإضافة المادة (٢٧٦) إليه.

-**الجزائر:** قام المشرع الجزائري بتجريم أفعال المساس بأنظمة الحاسوب الآلي، نتيجة للتأثر بالثورة المعلوماتية، وهذا الأمر دفع بالمشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون ١٥/٤ المؤرخ في ٢٠٠٤/١١/١٠م، المتمم للأمر رقم ٦٦/ ١٥٦ والمتضمن قانون العقوبات، ونص عليها في القسم السابع مكرر بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات" وتضمن ثمانية مواد، من المادة (٣٩٤) مكرر حتى المادة (٣٩٤) مكرر٧، كما أقر المشرع الجزائري بمسؤولية

---

وجريمة الاحتيال عن طريق الشبكة وجريمة الاستعمال غير المشروع لبطاقات الدفع وجريمة انتهاك حرمة الحياة الخاصة).

(١) لا يوجد في قانون العقوبات الفرنسي مبحث خاص بجرائم الحاسوب الآلي وإنما وزعها المشرع الفرنسي بين عدة مطالب منها: المادة (١٥-٢٢٦) التي عالجت الاعتداء على سرية المراسلات ضمن بحث يسمى " الاعتداءات على الشخصية والانتهاكات على حقوق الإنسان الناتجة عن ملفات الكومبيوتر أو معالجتها وأيضاً الاعتداءات على أنظمة معالجة البيانات الآلية من المادة (٣٢٣-١ إلى المادة ٧-٣٣٢).

الشخص المعنوي، وعاقب على الاشتراك في هذه الجرائم، كما أدخل تعديل آخر على قانون العقوبات في ٢٠٠٦ بموجب القانون ٢٣/٦ المؤرخ في ٢٠٠٦/١٢/٢٠ الذي قام فيه بتشديد العقوبات[١].

ومن أهم التعريفات التشريعية للجريمة الإلكترونية ما جاء به القانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات، حيث عرف الجريمة الإلكترونية في مادته الأولى بأنها: " الجريمة المعلوماتية هي كل فعل مؤثم يتم ارتكابه عبر أي وسيط إلكتروني".

كما عرَّف نظام مكافحة جرائم المعلوماتية السعودي الصادر في ٢٠٠٧/٣/٢٦م، الجريمة الإلكترونية في المادة الأولى الفقرة (٨) منه بأنها: " أي فعل يرتكب متضمناُ استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".

وعرَّفها المشرع القطري في المادة الأولى من القانون رقم (١٤) لسنة ٢٠١٤م، الخاص بمكافحة الجرائم الإلكترونية، بأنها: " أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة، بما يخالف أحكام القانون".

كما عرفها المشرع السوري في قانون مكافحة الجريمة المعلوماتية وتنظيم التواصل عبر الشبكة رقم (١٧) لعام ٢٠١٢م، بأنها: "جريمة ترتكب باستخدام الأجهزة الحاسوبية أو الشبكة أو تقع على المنظومات المعلوماتية أو الشبكة".

**ومن هذا التعريف نستنتج أن المشرع السوري قد اعتمد على المعيار الفني والموضوعي في تعريف الجريمة الإلكترونية ولم يأخذ بالمعيار الشخصي ونرى أنه قد أصاب في ذلك.**

---

(١) هلال آمنة، المرجع السابق،ص٢٤ – ٢٥.

**ثانياً: محل الجرائم الإلكترونية:**

يختلف محل الجريمة الإلكترونية بحسب ما إذا كانت موجهة ضد أحد مكونات النظام المعلوماتي بحيث يكون هذا الأخير موضوعها، أو مرتكبة من خلال هذا النظام بحيث يكون وسيلة تنفيذها وأداتها، ففي الحالة الأولى تجتمع الجرائم التقليدية البحتة والجرائم الإلكترونية بمعناها الفني، فتتوافر أولاهما إذا كانت المكونات المادية للنظام، كالأجهزة والمعدات والكابلات، هي محل الاعتداء أو موضوع الجريمة، ولم يكن ثمة أهمية للتقنية في ارتكاب الجريمة، كما هو الحال في سرقة أو إتلاف الحاسوب أو الشاشة، وتتوافر الثانية حينما تكون المكونات غير المادية للنظام، كالبيانات والبرامج في ذاتها، هي محل الاعتداء، كما هو الحال في الاعتداء على البيانات المخزنة في ذاكرة الحاسوب أو المنقولة عبر شبكات الاتصال بالسرقة أو التزوير، أو الاعتداء على البرنامج ذاته بادعاء ملكيته أو سرقته أو تقليده أو إتلافه أو محوه أو تعطيله، وصور الاعتداء الثانية، لا الأولى، هي التي لم يتم بسبب جدتها النسبية، معالجتها في معظم قوانين العقوبات القائمة(١).

فمحل الاعتداء في مجال الجرائم الإلكترونية التي تُعد ظاهرة إجرامية مستجدة يتمثل في معطيات الحاسوب، فقانون العقوبات ينطوي على نصوص تجرم الاعتداء على الأشخاص، الأموال، الثقة العامة...إلخ، لكن المستجد، هو الكيانات المعنوية ذات القيمة المالية أو القيمة المعنوية البحتة، أو كلاهما، ولولا هذه الطبيعة المستجدة في الأساس لما كنا أمام ظاهرة مستجدة برمتها، ولكان المستجد هو دخول الحاسوب عالم الإجرام، تماماً كما هو الشأن في الجرائم المنظمة، فهي في الحقيقة جرائم تقليدية المستجد فيها عنصر التنظيم الذي ينتج

---

(١) أ. د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، المرجع السابق، ص٤٤٣.

مخاطر هائلة واتساع نطاق المساهمة الجزائية وانصهار الإرادات الجرمية في إرادة واحدة هي إرادة المنظمة الإجرامية المعنية[١].

أي إن الجرائم الإلكترونية محلها الاعتداء على الكيان المعنوي للحاسوب أو الآلة أو على قاعدة البيانات أو المعلومات التي قد تكون على شبكة المعلومات العالمية، مثال انتهاك الملكية الفكرية، وجرائم القرصنة وغيرها[٢].

أما عندما يكون محل الجرائم جهاز الحاسوب الآلي أو الآلة بصفة عامة، بحيث يكون الاعتداء واقعاً على الكيان المادي للآلة، فهذه جريمة تقليدية ولا تُعد من قبيل الجرائم الإلكترونية[٣].

وينتج عن طبيعة الاعتداء الذي يشكل جريمة إلكترونية أن هذا الاعتداء لا يمكن أن يؤلف جرماً معاقباً عليه بشكل تقليدي في قانون العقوبات أو في التشريعات الجزائية الخاصة، ففي حال كان هذا الاعتداء يشكل نموذجاً قانونياً لإحدى الجرائم المنصوص عليها في القوانين الجزائية سواء قانون العقوبات أو التشريعات الجزائية الخاصة لكان اعتداءً تقليدياً بواسطة الحاسوب أو الإنترنت ولخرج من طائفة الجرائم الإلكترونية، فمعيار التمييز ما بين الجرائم الإلكترونية والجرائم التقليدية هو عدم تجريم القوانين الجزائية للاعتداء الإلكتروني بأحد أشكال الجرائم التقليدية، وهذا من الممكن تصوره في الحالات التي يكون محل الجريمة الإلكترونية حقاً غير محمي في هذه القوانين[٤].

ويمكن طرح بعض الأمثلة على الجرائم الإلكترونية المنصوص عليها في المرسوم التشريعي رقم (١٧) لعام ٢٠١٢م، الخاص بمكافحة الجريمة المعلوماتية السوري، فقد عاقبت المادة الثالثة منه كل من دخل قصداً إلى موقع على الإنترنت أو نظام معلوماتي بشكل غير مشروع، وكذلك المادة الرابعة التي عاقبت كل من

---

(١) د. عيسى مدالله المخول، المرجع السابق، ص٣٠-٣١.

(٢) أ. طارق محمد الجملي،المرجع السابق،ص٤٨،

(٣) أ. طارق محمد الجملي،المرجع السابق،ص٤٨،

(٤) د. عيسى مدالله المخول، المرجع السابق، ص٣٢.

أعـاق أو منـع قصـداً الـدخول إلـى الأجهـزة، أو الوصـول عـن طريـق الشـبكة المعلوماتية أو إحدى الوسائل الإلكترونية إلى الخدمة أو البرامج أو مواقع الإنترنت أو مصادر البيانات أو المعلومات[١].

في حين أنه من الممكن اعتباره من الجرائم التقليدية ما نصت عليه المادة السادسة من ذات المرسوم كل من استولى عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسوب أو ما في حكمها، على مال منقول أو عقار أو معلومات أو برامج ذات قيمة مالية أو على سند يتضمن تعهداً أو إبراء أو أي امتياز مالي آخر، وذلك عن طريق خداع المجني عليهن أو خداع الحاسوب أو الآلة الخاضعة لسيطرة المجني عليه، بأي وسيلة كانت، وكذلك المادة السابعة التي عاقبت كل من حصل دون وجه حق على بيانات أو أرقام بطاقة مصرفية باستخدام الشبكة المعلوماتية أو أحد أجهزة الحاسوب أو ما في حكمها، أو من قام بتزوير بطاقة مصرفية، أو استعمل بطاقة مصرفية مزورة أو مسروقة أو مفقودة في سحب النقود أو الوفاء، أو انتهك حرمة الحياة الشخصية، كما يمكن أن تُعد من الجرائم التقليدية جرائم تزوير التوقيع الإلكتروني أو استعمال التوقيع المزور وفقاً لما نص عليه قانون التوقيع الإلكتروني وخدمات الشبكة رقم (٤) لعام ٢٠٠٩م[٢].

ومن ذلك يتبين أن الاعتداء المكون للجريمة الإلكترونية لا يمكن أن يشكل النموذج القانوني لأية جريمة تقليدية منصوص عليها في قانون العقوبات أو التشريعات الجزائية الخاصة[٣].

**ونحن نرى أنه يشترط لنعد جريمة ما جريمة إلكترونية يجب أن يتوافر فيها كلا العنصرين التاليين:**

**العنصر الأول: إن يكون محل الجريمة الإلكترونية معطيات إلكترونية، وبهذا العنصر نستبعد الجرائم التي يكون محل الاعتداء فيها الكيانات المادية**

---

(١) د. عيسى مدالله المخول، المرجع السابق، ص٣٢.

(٢) د. عيسى مدالله المخول، المرجع السابق، ص٣٢-٣٣.

(٣) د. عيسى مدالله المخول، المرجع السابق، ص٣٣.

**للحاسوب وأجهزة الاتصال التي تخرج عن نطاق الجرائم الإلكترونية لأن هذه الكيانات تصلح محلاً للجرائم التقليدية كجرائم السرقة والتدمير والإتلاف وغير ذلك.**

**العنصر الثاني: لا يشكل الاعتداء المكون للجريمة الإلكترونية النموذج القانوني لأية جريمة تقليدية منصوص عليها في قانون العقوبات أو التشريعات الجزائية الخاصة، وبهذا العنصر نستبعد الجرائم التي يكون محل الاعتداء فيها معلومات موجودة داخل الحاسوب بالتحريف والتغيير التي من الممكن أن تشكل جرائم تقليدية كالتزوير والاحتيال، وكذلك فإن نشر بعض المعلومات عن طريق شبكة الإنترنت قد يشكل جرائم تقليدية أيضاً لجرائم الفتنة والترويج للإرهاب، وبالتالي يبرز هنا العنصر الأساسي للجريمة الإلكترونية وهو أن لا يشكل الاعتداء الإلكتروني أي نموذج قانوني لجريمة أخرى.**

## ثالثاً: أنواع الجرائم الإلكترونية:

للجرائم الإلكترونية أنواع متعددة، فهي تنقسم إلى جرائم الحاسوب، وجرائم الإنترنت، وجرائم الشبكة العالمية، وجرائم الاتصالات، وسوف ندرس هذه الأنواع كمايلي:

### أ – جرائم الحاسوب:

جرائم الحاسوب [١]هي النوع الأول من جرائم (Cyber Crime)[٢]، لذلك لابد لنا من تعريف جرائم الحاسوب، وأنواع هذه الجرائم.

---

(١) المقصود بجرائم الكومبيوتر أو جرائم الحاسوب ليست تلك الجرائم التي يكون فيها الحاسوب موضوعاً للجريمة كأن يسرق الجهاز أو يتلف، لأنه في هذه الحالة يعد من الأموال التي كفل القانون حمايتها من التعرض، وبالتالي فإن قانون العقوبات التقليدي يوفر الحماية لها. سهى إبراهيم داود عريقات، المرجع السابق، ص١١.

(٢) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٢٠.

**١ – تعريف جرائم الحاسوب:**

تطور الحاسوب من آلة حاسبة بسيطة إلى جهاز كهربائي يقوم بعدة عمليات فجمع بين الآلة الحاسبة والآلة الكاتبة وآلة تؤدي عدة عمليات[١]، وعُرِّف الحاسوب بأنه: "جهاز إلكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية للتعليمات المعطاة له بسرعة كبيرة تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة وبدرجة عالية الدقة، وله القدرة على التعامل مع كم هائل من البيانات وكذلك تخزينها واسترجعها عند الحاجة إليها"[٢].

وقد خلت الدراسات والمؤلفات التي في هذا الحقل (قديمها وحديثها) من تناول اتجاهات الفقه في تعريف جريمة الحاسوب عدا مؤلفين في البيئة العربية حيث عرَّفها بعضهم بأنها: "أي سلوك إنساني يشكل فعلاً غير مشروع قانوناً ويقع على أجهزة الكومبيوتر سواء وقع هذا السلوك غير المشروع على المكونات المادية Hard Ware أو المكونات المعنوية Soft Ware أو قواعد البيانات الرئيسية Data Base"[٣].

وتُعرَّف جريمة الحاسوب بأنها: "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[٤].

**ونحن نرى أن هذا التعريف قاصر لأنه اعتمد على المعيار الفني فقط وهو استخدام الحاسوب في ارتكاب الجريمة، وأغفل المعيار الموضوعي الذي يعتمد على محل الجريمة.**

---

(١) خالد عياد الحلبي، المرجع السابق، ص٣٩.

(٢) خالد عياد الحلبي، المرجع السابق، ص٤٠.

(٣) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٢٠.

(٤) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص ١٣.

كما تُعرَّف جرائم الحاسوب بأنها: تلك الجرائم التي ينصرف الاعتداء فيها إلى مكونات الحاسب الآلي المعنوية أو يكون النظام الآلي وسيلة لارتكاب الجريمة"[١].

كما تُعرَّف جريمة الحاسوب بأنها: " سلوك غير مشروع معاقب عليه قانوناً، وصادر عن إرادة جرمية محله معطيات الحاسوب"[٢].

**ونرى أن هذين التعرَّيفين الأخيرين قد أصابا عندما حددا محل جريمة الحاسوب بأنها تقع على معطيات الحاسوب وهذه المعطيات برأينا هي المكونات المعنوية للحاسوب والتي تشمل (البيانات والمعلومات والبرامج) ولا تشمل المكونات المادية التي هي ليست محلاً لجريمة الحاسوب كما بينا ذلك عند دراستنا لمحل الجريمة الإلكترونية.**

وذلك لأن محل جريمة الحاسوب هو دائماً المعطيات أما بذاتها أو بما تمثله هذه المعطيات التي قد تكون مخزنة داخل النظام أو على أحد وسائط التخزين أو تكون في طور النقل والتبادل ضمن وسائل الاتصال المندمجة مع نظام الحوسبة[٣].

**ونحن بدورنا يمكننا أن نُعرَّف جريمة الحاسوب معتمدين على المعيار الفني والموضوعي معاً بأنها: " سلوك إيجابي أو سلبي غير مشروع يقع باستخدام الحاسوب مستهدفاً معطيات الحاسوب".**

**٢ – أنواع جرائم الحاسوب:**

تتنوع جرائم الحاسوب فهناك من يعطي بعض الأمثلة عليها ومنها بث ونشر الفيروسات وتعديل أو محو البيانات الرئيسية وغيرها[٤].

---

(١) سهى إبراهيم داود عريقات، المرجع السابق، ص١١.

(٢) د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق، ص٦٤.

(٣) يونس عرب، جرائم الكمبيوتر والانترنت، (ايجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات)، ص٥.

(٤) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٢٠.

**ب- جرائم الانترنت[١]:**

يمكن تعريف الإنترنت بأنه: "عبارة عن مجموعة من الحاسبات الآلية متصلة بعضها ببعض بشكل مفتوح، أي أن أي جهاز منه مرتبط بالآخر وذلك عن طريق مراكز الخوادم العالمية (سيرفر) التي تزود هذه الخدمة"[٢].

وجرائم الإنترنت (Internet Crime) هي النوع الثاني من جرائم ( Cyber Crime)، وتاريخياً فإن أول جريمة انترنت حدثت في العالم كانت في الولايات المتحدة الأمريكية في عام ١٩٨٨م[٣]، وسنعرض تعريف جرائم الإنترنت، ومن ثم أنواعها المختلفة، كمايلي:

---

(١) ترجع الأصول التاريخية للإنترنت إلى مشروع ابرانت (مشروعات شبكة وكالة الأبحاث المتقدمة) (APRANET Advanced Research Projects Agency Network)، وقد بدأت هذا العمل وزارة الدفاع الأمريكية في عام ١٩٦٩م، وتم تطوير هذا المشروع عن طريق مراكز الأبحاث الجامعية أثناء الحرب الباردة، وكان الهدف منه إقامة شبكة بين خطوط الكومبيوتر طويلة المدى تقاوم التدمير الجزئي وتربط بين الحاسبات المختلفة وأنظمة الراديو والأقمار الخاصة بالولايات المتحدة الأمريكية في أنحاء العالم، وبحيث إذا تم تدمير جزئي لهذه الشبكة استمر العمل دون توقف وبذات الفعالية. وفي عام ١٩٨٣م نتيجة لنجاح المشروع رأت وزارة الدفاع الأمريكية فصل الشق العسكري MILNETعن الشبكة، وقامت الهيئة القومية للعلوم بإنشاء شبكة NSFnetبتوصيل خمسة حاسبات رئيسية لخدمة مركز البحوث الأمريكية بحيث حلت هذه الحاسبات والتي تعمل بسرعة فائقة محل النظام السابق. واعتباراً من عام ١٩٨٧م تزايدت أعداد المتعاملين مع هذه الشبكة وخصوصاً بعد السماح للأفراد العاديين باستعمالها وظهرت (بيتنت) ثم ظهر الإنترنت في صورته الحالية.

TORELLO NICOLE et LOINTIER PASCAL, internet pour les jurists, Dalloz,1996,pp2.

مشار إليه لدى: د. مدحت رمضان، المرجع السابق، ص٣ – ٤.

(٢) خالد عياد الحلبي، المرجع السابق، ص٥١.

(٣) حيث قام موريس (Morris) الطالب بالسنة الأولى لدرجة الدكتوراه بعلوم الكومبيوتر بجامعة كورنل (Cornell University)، والذي اكتسب خبرة كبيرة بعلوم الكومبيوتر، أثناء دراسته كطالب وعمله بجامعة هارفارد خلال الدراسة الجامعية الأولى، باستخدام حسابه على الإنترنيت لتطوير برنامج للكومبيوتر سمى فيما بعد بالدودة (Worm) أو الفيروس (Virus)، وكان هدف الطالب من تطوير هذا البرنامج أن يثبت عدم ملائمة أو فعالية الإجراءات

**١ - تعريف جرائم الإنترنت:**

تُعرَّف جرائم الإنترنت بأنها: "أي سلوك إنساني يشكل فعلاً غير مشروع قانوناً وتقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات"(١).

---

الأمنية القائمة لحماية شبكات الكومبيوتر وذلك بإظهار العيوب التي اكتشفها، وقام بتصميم البرنامج بحيث ينتشر بشبكة وطنية للكومبيوتر بعد أن يتم تشغيله عن طريق حاسب محلي متصل بها، وقام موريس بتشغيل البرنامج على الإنترنيت والذي يربط بين مجموعة من شبكات الكومبيوتر الأمريكية التي تربط بدورها بين أجهزة كومبيوتر بالجامعات والجهات الحكومية والعسكرية، وكانت خطة موريس أن ينتشر الفيروس دون أن يجذب الانتباه إليه وكان يتوقع أن يعمل الفيروس لفترة قصيرة من الوقت دون أن يشعر به المبرمجون أو يتمكنوا من القضاء عليه، وصمم الفيروس بحيث لا ينسخ نفسه على جهاز الكومبيوتر نسخ عليه أثناء عملية انتشاره مرة أخرى حتى لا يتم التعرف عليه، وتوقع موريس أن يتم القضاء على الفيروس بمجرد إيقاف الحاسب المصاب، وبعد أن تم نشر الفيروس اكتشف موريس أنه يقوم بالانتشار بسرعة كبيرة بما ترتب عليه توقف الكثير من أجهزة الكومبيوتر بأنحاء الولايات المتحدة الأمريكية عن العمل أو أنها صارت تعمل بصورة غير سليمة، وحاول أن يجد حلاً مع صديق بجامعة هارفارد واتفقا على إرسال رسائل لا تحمل اسمه حتى لا يمكن التعرف عليه لمبرمجي الكومبيوتر بأنحاء الولايات المتحدة الأمريكية لإخبارهم بوسيلة القضاء على الفيروس ولكنهما لم ينجحا في إرسال الرسالة الإلكترونية حيث أن الأجهزة المختلفة بجميع أنحاء الولايات المتحدة كانت قد أصيبت. وترتب على نشاط موريس غير المشروع أن أصيبت أجهزة الكومبيوتر الموجودة بجهات حيوية بالفيروس كالجامعات والمواقع العسكرية ومركز البحوث الطبية، وقدرت تكاليف إصلاح كل منشأة على حدة بمبلغ يتراوح فيما بين ٢٠٠ دولار إلى ٥٣.٠٠٠ دولار أمريكي، وحوكم موريس بمقتضى القانون الذي يجرم الدخول على جهاز من أجهزة الكومبيوتر الفيدرالية عمداً ودون تصريح وبأي وسيلة تؤدي إلى تخريب أو تدمير المعلومات الموجودة عليه، ولقد دافع المتهم عن نفسه استناداً إلى أنه لم تتوافر لديه نية تحقيق الضرر الذي وقع، وكان رد المحكمة أنه لا يشترط أن تتجه النية إلى تحقيق الضرر بل يكفي أن نية الجاني قد اتجهت إلى الدخول غير المشروع على نظام الحاسب الفيدرالي، ولقد أدين موريس بالوضع ثلاث سنوات تحت المراقبة والقيام بعمل لمدة ٤٠٠ ساعة في خدمة المجتمع وغرامة مقدارها ١٠,٠٥٠ آلاف دولار أمريكي بالإضافة إلى تكاليف وضعه تحت المراقبة، ولقد طعن موريس في الحكم بالاستئناف وأيدت الحكم المحكمة الاستئنافية. د. مدحت رمضان، المرجع السابق، ص١٢ - ١٣.

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٢١.

كما تُعرَّف بأنها: " كل فعل غير مشروع يقع على المواقع بقصد تعطيلها أو تشويهها أو تعديلها والدخول غير المشروع لمواقع غير مصرح بالدخول إليها، واستخدم عناوين غير حقيقية للدخول في شبكة المعلومات واقتحام الشبكات ونقل الفيروسات، وإرسال الرسائل بكافة أنواعها عبر البريد الإلكتروني مثل الماسة بكرامة الأشخاص أو المستهدفة ترويج مواد أو أفعال غير مشروعة"[١].

ولا يمكن الآن حصر من يرتكبون جرائم الإنترنت في طبقة أو فئة معينة أو جنس معين فمرتكب الجريمة قد يكون من البالغين أو الأحداث أو المتعلمين والمثقفين ومن الفقراء أو الأغنياء ومن الرجال أو من النساء[٢].

**٢ – أنواع جرائم الإنترنت:**

يعطي بعض الفقه[٣] أمثلة على أنواع جرائم الإنترنت، كجرائم الدخول غير المشروع لمواقع غير مصرح بها للدخول إليها واستخدام عناوين (IP) غير حقيقة أو زائفة للولوج إلى الشبكة العالمية للمعلومات وكسر البروكسي (Brokcey) أو تقنيات الحماية (Fire Wall) الخاصة بالجهات المتصلة بالشبكة.. وغيرها.

وبالواقع لا يمكن حصر جرائم الانترنت في نوع معين من الجرائم فقد تكون من الجرائم الماسة بأمن الدولة من الداخل أو من الخارج وقد تكون من جرائم الاعتداء على الأشخاص أو جرائم الاعتداء على الأموال[٤].

وهناك من يرى[٥] أن التمييز ما بين جرائم الحاسوب وجرائم الإنترنت ما هو إلا تمييز وهمي غير حقيقي، وفي الواقع إن الحاسوب والإنترنت ماهي إلا وسائل ترتكب من خلالها الجرائم الإلكترونية والجرائم التقليدية، لذلك يدعو هذا الرأي الفقه

---

(١) د. عيسى مدالله المخول، المرجع السابق، ص٣٤..

(٢) د. مدحت رمضان، المرجع السابق، ص١١.

(٣) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٢١.

(٤) د. مدحت رمضان، المرجع السابق، ص١١.

(٥) د. عيسى مدالله المخول، المرجع السابق،ص٢٩–٣٠.

الجزائي بدلاً من الالتفاف إلى إيجاد معيار اصطناعي وغير حقيقي للتمييز بين ما يسمى جرائم الحاسوب وجرائم الإنترنت، أن يكرس جهد الفكر القانوني نحو إيجاد معيار واضح للتمييز بين الجرائم الإلكترونية والجرائم التقليدية تمهيداً للوصول إلى مفهوم الجريمة الإلكترونية.

**جـ- جرائم الشبكة العالمية:**

إن جرائم الشبكة العالمية (Web Computer Crime) هي النوع الثالث من جرائم (Cyber Crime)، وتُعرَّف بأنها: "أي سلوك إنساني يشكل فعلاً غير مشروع قانوناً ويقع على أي وثيقة أو نص موجود بالشبكة"[١].

ويلاحظ أن ارتكاب هذه الجرائم عبر شبكة المعلومات يتطلب اتصال بالإنترنت واستخدام الحاسوب للوصول إلى قواعد البيانات للاطلاع عليها أو تغيرها [٢]على عكس جرائم الحاسوب التي قد يتصور حدوثها سواء كان هناك اتصالاً بالإنترنت أو عدمه[٣].

ومن أمثلة هذا النوع من الجرائم الإلكترونية، قرصنة المعلومات وسرقة أرقام بطاقات الائتمان وانتهاك الملكية الفكرية للبرامج [٤] والإنتاج الفني والأدبي[٥].

**د – جرائم الاتصالات:**

إن جرائم الاتصالات هي إحدى أنواع الجرائم الإلكترونية، وتستهدف جرائم الاتصالات ماديات الشبكة[٦].

---

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٢٠.
(٢) د. عيسى مدالله المخول، المرجع السابق، ص ٣٤.
(٣) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٢٠.
(٤) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٢٠.
(٥) د. عيسى مدالله المخول، المرجع السابق، ص٣٤.
(٦) د. عيسى مدالله المخول، المرجع السابق، ص٢٩.

ويمكن تُعريف جرائم الاتصالات بشكل عام بأنها جرائم ناعمة لا تترك أثاراً مادية، وهذه الميزة هي من أهم الأسباب التي تجعل هذه الجرائم صعبة الإثبات، ذلك لأنه لا يمكن الكشف عن الجريمة إلا من خلال الأدلة التي تتخلف عنها.

وقد نص قانون الاتصالات السوري رقم (١٨) لعام ٢٠١٠م، على العديد من الجرائم التي من شأنها أن تضر بقطاع الاتصالات، وذلك في المواد ٦٠ حتى ٦٧ فتحدث عن جريمة الإخلال بالتزامات العمل في الهيئة الناظمة لقطاع الاتصالات، وكذلك جريمة الإخلال بواجبات السرية وإنشاء شبكات أو تقديم خدمات الاتصالات من دون ترخيص، ونص على جرم تخريب شبكات أو تجهيزات الاتصالات وإساءة استخدام الترددات الراديوية، وكذلك إساءة تقديم خدمات الاتصالات، كما نص على جرم استعمال الوسائل الاحتيالية في الحصول على خدمات الاتصالات، كما منع استيراد وحيازة تجهيزات غير مرخصة.

**رابعاً: تصنيف الجرائم الإلكترونية:**

تعددت الاتجاهات الفقهية في تصنيف الجرائم الإلكترونية، وسنعرض أهم هذه التصنيفات:

**أ-تصنيف الجرائم الإلكترونية تبعاً لمحل الجريمة:**

هذا التصنيف يعكس التطور التاريخي لظاهرة الجرائم الإلكترونية، ولهذا نجد أن جرائم الإلكترونية بالاستناد إلى هذا المعيار يمكن تقسيمها ضمن الفئات الآتية:

**١-الجرائم الماسة بقيمة معطيات الحاسوب:**

وتشمل هذه الطائفة فئتين: أولهما، الجرائم الواقعة على ذات المعطيات، كجرائم الإتلاف والتشويه للبيانات والمعلومات وبرامج الحاسوب بما في ذلك استخدام وسيلة (الفيروسات) التقنية. وثانيهما، الجرائم الواقعة على ما تمثله المعطيات آلياً من أموال أو أصول، كجرائم الحاسوب التي تستهدف الحصول على

المـال، وجـرائم التحـوير والتلاعـب فـي المعطيـات المخزنـة داخـل نظـم الحاسـوب واستخدامها (تزوير المستندات المعالجة آلياً واستخدامها).

**٢-الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة:**

وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية، وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة.

**٣- الجـرائم الماسـة بحقـوق الملكيـة الفكريـة لبـرامج الحاسـوب ونظمـه (جـرائم قرصنة البرمجيات):**

وتشمل نسخ وتقليد البرامج وإعادة انتاجها وصنعها دون ترخيص واستغلالها مادياً والاعتداء على العلامة التجارية وبراءة الاختراع.

وبـالنظر إلـى هـذه الفئـات، فـإن الحـدود بينهـا ليسـت قاطعـة، فالتـداخل حاصـل ومحقـق، إذ أن الاعتـداء علـى معطيـات الحاسـوب بـالنظر لقيمتهـا الذاتيـة أو مـا تمثلـه، هـو فـي ذات الوقـت اعتـداء علـى أمـن المعطيـات، لكـن الغـرض المباشـر للاعتداء انصـب علـى قيمتهـا أو مـا تمثلـه، والاعتداء علـى حقـوق الملكيـة الفكريـة لبـرامج الحاسـوب، هـو اعتـداء علـى الحقـوق الماليـة واعتـداء علـى الحقـوق الأدبيـة لكنهـا تتميـز عـن الفئـات الأخـرى بـأن محلهـا هـو البـرامج فقـط، وجرائمهـا تسـتهدف الاستخدام غير المحق أو التملك غير المشروع لهذه البرامج.

هذا من جهة، ومن جهة أخرى، فإن الحماية الجزائية للمعلومات في نطاق القانون المقارن وفي إطار الجهود الدولية لحماية معطيات الحاسوب واستخدامه، اعتمدت علـى نحـو غالـب، التقسيم المتقدم فظهرت حمايـة حقـوق الملكيـة الأدبيـة للبـرامج، وحمايـة البيانـات الشخصـية المتصـلة بالحيـاة الخاصـة، وحمايـة المعطيـات بـالنظر لقيمتها أو ما تمثلها والذي عُرف بحماية (الأموال)، كل في ميدان وموقع مستقل، وهـو فـي الحقيقـة تمييـز ليس مطلـق بين حمايـة قيمـة المعطيـات، وأمنهـا، وحقـوق الملكية الفكرية، ولابد من الإشارة، أن حماية أمن المعطيات(الفئة الثانية) انحصر فـي حمايـة البيانـات الشخصـية المتصـلة بالحيـاة الخاصـة، أمـا حمايـة البيانـات

والمعلومات السرية والمحمية فقد تم تناوله في نطاق جرائم الفئة الثالثة الماسة بقيمة المعطيات بالنظر إلى الباعث الرئيسي للاعتداء والغرض من معرفة أو إفشاء هذه المعلومات غالباً كان الحصول على المال مما يُعد من الاعتداءات التي تندرج تحت نطاق الجرائم الماسة بقيمة المعطيات التي تتطلب توفير الحماية الجزائية للحقوق المتصلة بالذمة المالية التي تستهدفها هذه الجرائم[١].

**ب- تصنيف الجرائم الإلكترونية تبعاً لدور الحاسوب في الجريمة:**

يصنف بعض الفقه[٢] الجرائم الإلكترونية تبعاً لدور الحاسوب في ارتكابها:

**١-الحاسوب محل الاعتداء:**

بمعنى أن يستهدف الفعل المعطيات المعالجة أو المخزنة أو المتبادلة بواسطة الحاسوب والشبكات، كالاستيلاء على المعلومات واتلافها.

**٢-الحاسوب وسيلة ارتكاب جريمة أخرى، كجرائم الاحتيال.**

**٣-كما قد يكون الحاسوب مخزناً للمادة الجرمية:**

كأن يحتوي على بعض المواد المخلة بالأخلاق والآداب العامة.

وقد استفاد الاتجاه العالمي الجديد من هذا التصنيف في تطوير التدابير التشريعية لمكافحة الجريمة الإلكترونية، وأفضل ما يعكس هذ الأمر الاتفاقية الأوربية لجرائم الكومبيوتر والإنترنت لعام ٢٠٠١م (اتفاقية بودابست ٢٠٠١م)، حيث قسمت الاتفاقية المشار إليها الجرائم الإلكترونية إلى الفئات الآتية:

**الأولى:** الجرائم التي تستهدف عناصر السرية والسلامة وديمومة توفر المعطيات والنظم وتضم: الدخول غير القانوني، الاعتراض غير القانوني، تدمير المعطيات، اعتراض النظم، وإساءة استخدام الأجهزة.

**الثانية:** الجرائم المرتبطة بالحاسوب وتضم: التزوير المرتبط بالحاسوب والاحتيال المرتبط بالحاسوب.

---

(١) د. عيسى مدالله المخول، المرجع السابق،ص٤٤-٤٥.

(٢) د. عيسى مدالله المخول، المرجع السابق، ص٤٦.

**الثالثة:** الجرائم المرتبطة بالمحتوى وتضم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية واللأخلاقية.

**الرابعة:** الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة وهي قرصنة البرمجيات.

**جـ- تصنيف الجرائم ذات الطابع التقليدي:**

ممكن أن تكون الجرائم الإلكترونية ذات الطابع التقليدي جرائم تستهدف الأشخاص أو الأموال، أو جرائم تزوير أو مقامرة أو وجرائم أمن دولة، أو جرائم اقتصادية، وسنشرحها كمايلي:

**١- الجرائم التي تستهدف الأشخاص:**

وتضم طائفتين رئيستين هما:

**-الجرائم الواقعة على الحياة:**

إن الحماية الخاصة للأشخاص قد أقرتها القواعد الدستورية والقانونية، وهناك بعض الأسرار الخاصة بالإنسان لا يجوز الاطلاع عليها من الغير، وقد يقوم بتخزينها في الحاسوب الذي يخصه هو دون غيره، ولقد حرم المشرع الاعتداء على الأسرار وعاقب على إفشائها.

وإن دخول نظام المعالجة الآلية للمعلومات خلق أوضاعاً جديدة على المجتمع خاصة في مجال حماية الحياة الخاصة للأفراد، فأصبح الحاسوب مستودعاً لأسرارهم، وإن الحصول غير المشروع على هذه الأسرار هو اعتداء على شخص الإنسان.

وكذلك جرائم الذم والتحقير وجرائم التهديد، هي من الأمور التي يمكن حصولها عبر شبكة الإنترنت، وهي تعد من الجرائم الواقعة على الأشخاص[١].

وكذلك من الجرائم التي تستهدف الأشخاص ( Non Sexual Crimes against Persons) جرائم القتل بالحاسوب الآلي (Computer Murder) وجرائم

---

(١) خالد عياد الحلبي، المرجع السابق، ص ٦١.

الإهمال المرتبط بالحاسوب والتي تسبب الوفاة ( Negligent Computer Homicide) والتحضير على الانتحار والتحضير المتعمد عبر الإنترنت وهنالك جرائم التحرش والمضايقة عبر وسائل الاتصال والإضرار المتعمد وذلك بإحداث الضرر العاطفي أو تسبيب ضرر عاطفي عبر وسائل التقنية وغيرها [١].

**-الجرائم الواقعة على الأخلاق:**

وتشمل الجرائم الجنسية ومن أمثلتها: (نشر وتسهيل نشر واستضافة المواد الفاحشة عبر الإنترنت بوجه عام و تستهدف القاصرين بوجه خاص، نشر المعلومات عن القاصرين عبر الحاسوب من أجل أنشطة جنسية غير مشروعة، إغواء أو محاولة إغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة، حض وتحريض القاصرين على أنشطة جنسية غير مشروعة، التحرش الجنسي بالقاصرين عبر الحاسوب والوسائل التقنية، واستخدام الإنترنت لترويج الدعارة بصورة قصرية أو للإغواء أو لنشر المواد الفاحشة التي تستهدف استغلال عوامل الضعف والانحراف لدى المستخدم، للحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة جنسية)[٢].

**٢- الجرائم التي تستهدف الأموال:**

إن الهدف من الجرائم الإلكترونية هو الحصول على المال، لأن البرامج والمعلومات المخزنة في الحاسوب لها قيمة مادية في التعامل، فالحصول على البرامج بطريقة غير مشروعة كالسرقة والتقليد هي جرائم تقع على الحاسوب، وهي من جرائم الاعتداء على الأموال.

فجرائم الدخول إلى الحسابات المصرفية الخاصة بالعملاء في البنوك، من قبل أحد الموظفين، ونقل جزء منها إلى حسابه الخاص هو بهدف الإثراء غير

---

(١) د. يونس عرب، ورقة عمل حول الجرائم الالكترونية وأدلة إثباتها بين الواقع الماثل والمثال المأمول، ص٥.

(٢) سهى إبراهيم داود عريقات، المرجع السابق، ص١٥.

المشروع، والحصول على الأموال، ودون وجود الحاسوب لا تقع هذه الجرائم، فجميع جرائم الحاسوب هي من جرائم الاعتداء على الأموال، ويشترط في الجرائم الواقعة على الأموال مايلي:

١ – إن يكون محل جريمة السرقة له قيمة مادية في التعامل.

٢ – إمكانية الانتفاع به.

٣ – أن يكون المال منقولاً، أي يسهل نقل حيازته من شخص إلى آخر.

وإن المعلومات المخزنة في الحاسوب، والمتبادلة عبر شبكة الإنترنت هي من مكونات الحاسوب المعنوية غير المادية وهي هدف الجاني وغايته، فإذا تم الاعتداء عليها بالسرقة أو الاحتيال فإنها تُعد من جرائم الأموال(١).

وتشمل الجرائم التي تستهدف الأموال أنشطة الاقتحام أو الدخول أو الاتصال غير المرخص به مع نظام الحاسوب أو الشبكة وتخزين البيانات والنظم والممتلكات وخلق البرمجيات الخبيثة والضارة ونقلها عبر النظم والشبكات واستخدام اسم النطاق أو العلامة التجارية أو اسم الغير دون ترخيص وإدخال معطيات خاطئة أو مزورة إلى نظام الحاسوب (٢)، وكذلك جرائم الاحتيال والسرقة، وتشمل جرائم الاحتيال التلاعب بالبيانات والنظم أو استخدام البطاقات المالية للغير بدون ترخيص أو تدميرها، والاختلاس عبر الحاسوب أو بوساطتها وسرقة خدمات الحاسوب، وسرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الحاسوب (٣).

**٣–جرائم التزوير:**

وتشمل تزوير البريد الإلكتروني وتزوير الوثائق والسجلات وتزوير الهوية(٤).

---

(١) خالد عياد الحلبي، المرجع السابق، ص ٦٠.

(٢) د. عيسى مدالله المخول، المرجع السابق، ص٤٧.

(٣) سهى إبراهيم داود عريقات، المرجع السابق، ١٥ – ١٦.

(٤) د. عيسى مدالله المخول، المرجع السابق،ص٤٧.

**٤-جرائم المقامرة:**

وتشمل تملك وإدارة مشروع مقامرة على الإنترنت، وتسهيل إدارة مشاريع القمار على الإنترنت، والتحريض على إقامة مشروع مقامر عبر الإنترنت، واستخدام الإنترنت لترويج الكحول ومواد الإدمان للقصر[١].

**٥-جرائم الحاسوب ضد الدولة:**

إن الدخول على حاسبات الدولة التي تتضمن أسرارها والمعلومات المتعلقة بأمنها وجيشها، هو من الجرائم التي تقع على أمن الدولة، وإن إثارة الفتن الطائفية عبر البريد الإلكتروني والمواقع الإلكترونية، من الجرائم التي تمس أمن الدولة، وإن اختراق الأسرار السياسية والعسكرية للدولة من الجرائم الخطيرة التي تقع على أمنها، وكذلك إثارة الفتن فجميعها من الجرائم الواقعة على أمن الدولة[٢]، وكذلك جرائم تعطيل الأعمال الحكومية وتنفيذ القانون والإرهاب الإلكتروني [٣] والأنشطة الثأرية، وأنشطة التدمير والاختراق الإلكتروني [٤].

**٦- الجرائم الإلكترونية ضد الاقتصاد:**

تُعرف الجرائم الاقتصادية بأنها: "كل فعل أو امتناع يعاقب عليه القانون ويخالف السياسة الاقتصادية للدولة"[٥].

وإن انتشار التجارة الإلكترونية عبر الحاسوب في جميع دول العالم، أوجد الكثير من الجرائم الاقتصادية التي تضر باقتصاد البلد أو تضر بالأفراد[٦].

---

(١) د. عيسى مدالله المخول، المرجع السابق،ص٤٧.

(٢) خالد عياد الحلبي، المرجع السابق، ص ٦٢.

(٣) سهى إبراهيم داود عريقات، المرجع السابق،ص١٦. .

(٤) د. يونس عرب، ورقة عمل حول الجرائم الالكترونية وأدلة إثباتها بين الواقع الماثل والمثال المأمول ، ص٦.

(٥) د. عبود السراج، قانون العقوبات الاقتصادي، الطبعة السابعة، منشورات جامعة دمشق، دمشق، سورية،١٩٩٨م، ص١٠.

(٦) خالد عياد الحلبي، المرجع السابق، ص ٦٢.

**وهكذا نرى مدى تنوع أصناف الجرائم الإلكترونية والتي تعكس مدى التطور الهائل في تكنولوجيا المعلومات وتأثير هذا الإجرام في مختلف مناحي الحياة.**

**خامساً: الخصوم في الجرائم الإلكترونية:**

الخصوم في الجرائم الإلكترونية، عبارة عن فاعل الجريمة ومن يشترك معه في ارتكابها ويدعى الجاني، والشخص الذي وقعت عليه الجريمة ويدعى المجني عليه والنيابة العامة التي تمثل الحق العام، إذ إن دائرة الجريمة تنحصر في الخصوم الثلاثة باستثناء حالة اشتراك أشخاص آخرين مع فاعل الجريمة، حيث يدخلون في هذه الدائرة مع الفاعل والمجني عليه[١]، لذلك لابد لنا من دراسة هؤلاء الخصوم .

**أ – الجاني في الجرائم الإلكترونية:**

الإنسان هو الذي يرتكب هذه الجرائم، فهو إما أن يمثل نفسه ويدعى الشخص الطبيعي أو يمثل مؤسسة أو شركة وينفذ تعليماتها، وبالتالي فإن المؤسسة أو الشركة هي التي تكون مسؤولة وهو ما يسمى بالشخص المعنوي وكذلك الشخص الطبيعي المسؤول عن الشركة[٢].

ومن الناحية الجزائية تعني تسمية " المجرم المعلوماتي" ذلك الشخص الذي يمتلك مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسوب الإلكتروني والقادر على استخدام هذا التكتيك لاختراق " الكود" السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق الحاسوب نفسه"[٣].

---

(١) خالد عياد الحلبي، المرجع السابق، ص٣١.

(٢) خالد عياد الحلبي، المرجع السابق، ص٣٢.

(٣) د. عمار عباس الحسيني، المرجع السابق، ص٥٨.

فيما يميل البعض[١] إلى تسمية المجرم المعلوماتي بـ" المجرم الإلكتروني الرقمي" ويُعرفه بأنه: " من لديه القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الإلكتروني أو الرقمي وملحقاته ووسائل الاتصال الرقمية، وذلك بأداء فعل أو امتناع عنه مما يحدث اضطرابات في المجتمع الدولي أو المحلي نتيجة مخالفة قواعد الضبط الاجتماعي محلياً ودولياً".

والجاني أو الفاعل في الجرائم الإلكترونية لا يرتكب جريمته بالأساليب والطرق التي ترتكب بها الجرائم العادية، بل بأساليب حديثة تعتمد على الإلمام بآلية عمل الحاسوب ومعطياته وذلك للوصول إلى اختراق أجهزة الحاسوب للآخرين عن طريق الشبكات الإلكترونية، من أجل إتلاف أو شطب أو تعديل المعلومات المخزنة بها[٢].

وغالباً ما يهدف الجاني إلى تحقيق مصالحه المادية أو الانتقام من الغير، إلا إن الجرائم الإلكترونية قد ترتكب للتباهي أو التفاخر، بأن الجاني لديه المعرفة التامة لاختراق منظومة الحماية المختلفة للبرامج والمعلومات في الشركات والمؤسسات المالية والوصول إلى أسرارها، وكثيرة هي الأمثلة التي أرسل فيها الفاعل رسائل استهتار وازدراء لمؤسسات مالية، يتفاخر فيها بمقدرته على فك رموز نظم المعلومات في تلك المؤسسات[٣].

والجناة في الجرائم الإلكترونية أي (المجرمين المعلوماتيين) ينتمون إلى المجرمين ذوي الياقات البيضاء، وليس معنى ذلك أنهم أقل خطورة من الناحية الإجرامية عن المجرمين ذوي الياقات الزرقاء، بل يعني ذلك أنهم يختلفون عنهم في اتجاهات شخصياتهم، وعلى الرغم من انتمائهم بوجه عام إلى المجرمين ذوي الياقات البيضاء فإنهم طائفة متميزة عنهم تتخصص في جرائم الحاسوب، فهم إما

---

(١) د. عمار عباس الحسيني، المرجع السابق، ص٥٨.

(٢) خالد عياد الحلبي، المرجع السابق، ص٣١ – ٣٢.

(٣) خالد عياد الحلبي، المرجع السابق، ص٣٦.

أن يقوموا بالاعتداء على نظام الحاسوب أو يقوموا بالاستعانة بالحاسوب في ارتكاب جرائمهم(١).

ويتميز الأشخاص الذين يرتكبون الجرائم الإلكترونية أي (المجرم المعلوماتي)، بالخصائص والصفات التالية:

**١ – المجرم المعلوماتي مجرم ذكي:**

يتسم المجرم المعلوماتي بالذكاء والفطنة، والقدرة على التلاعب بالمعلومات وتغطية عمليات التلاعب وتحويل المكاسب إليه(٢).

ولا يمكن أن يقال أن المجرم المعلوماتي هنا ينتمي إلى طائفة المجرمين الأغبياء، فإذا كان من يسرق من منزل أو سيارة منخفض الذكاء في كثير من الأحيان، فإن من يستعين بالحاسوب من أجل سرقة أموال مصرف أو شركة هو مجرم يتميز بالمستوى المرتفع من الذكاء حتى يستطيع أن يتغلب على كثير من المشكلات والعقبات الفنية التي تواجهه(٣)، فهو أقرب إلى مرتكبي جريمة النصب منه إلى مرتكبي جريمة السرقة(٤).

**٢ – المجرم المعلوماتي مجرم غير عنيف:**

يقال في العادة أن الإجرام المعلوماتي هو إجرام غير عنيف مقارنةً بالإجرام التقليدي الذي يميل فيه المجرم إلى العنف، فإذا كان من الممكن تصور قيام

---

(١) د. غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكومبيوتر، بحوث مؤتمر القانون والكومبيوتر والإنترنت، من ١ – ٣ مايو، كلية الشريعة والقانون، جامعة الأمارات العربية المتحدة، المجلد الثاني، الطبعة الثالثة، ٢٠٠٤م، ص٦٢٨.

(٢) فمعظم الجرائم الإلكترونية تحتاج إلى ذكاء ودهاء وفطنة فهي لا تحتاج إلى جهد عضلي، بل إلى نشاط ذهني حيث يقوم الجاني بتزويد الحاسوب بالبرامج اللازمة لتنفيذ أهدافه. خالد عياد الحلبي، المرجع السابق، ص٣٦.

(٣) د. رامي متولي القاضي، مكافحة الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، ٢٠١١م، ص٥٥.

(٤) د. غنام محمد غنام، المرجع السابق، ص ٦٢٩.

العنف في جرائم الاعتداء على الحاسوب" ماديات الحاسوب"، إلا أن الإجرام المعلوماتي كإتلاف المعلومات لا يتطلب عنفاً كونه من تقنيات التدمير الناعمة"Soft Sabotage" التي تتمثل في التلاعب في المعلومات أو الكيانات المنطقية (المعنوية)، ومثل ذلك يقال أيضاً بالنسبة لسرقة البيانات أو الاحتيال المعلوماتي أو ماشابه من الجرائم الإلكترونية التي يتمثل سلوك الجاني فيها بشكل معالجة فنية هادئة للمعطيات الإلكترونية التي تتم بهدوء وبروية ومن دون أي عنف[١].

**٣-المجرم المعلوماتي مجرم متخصص:**

فقد ثبت من العديد من القضايا أن عدداً من المجرمين لا يرتكبون إلا جرائم الحاسوب أي إنهم يتخصصون في هذا النوع من الجرائم[٢]. فلا بد أن يتمتعوا بمعرفة فنية في عمل الحاسوب، وأن يلم بتشغيل الحاسبات وإدخال التعليمات غير المشروعة لمحو البرامج، والقيام بتعديل المعلومات من خلال التلاعب بالبيانات أو البرامج، وإدخال الفيروسات لإتلاف البرامج مع التعليمات غير المشروعة لمحو المعطيات[٣].

**٤- المجرم المعلوماتي مجرم عائد إلى الإجرام:**

إذ يعمد مجرمو المعلوماتية في الغالب إلى العودة مرة أخرى إلى ارتكاب جرائمهم انطلاقاً من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم ومن ثم كشف جرائمهم وتقديمهم إلى المحاكمة[٤].

---

(١) د. عمار عباس الحسيني، المرجع السابق، ص٦١.

(٢) د. غنام محمد غنام، المرجع السابق، ص٦٢٨.

(٣) خالد عياد الحلبي، المرجع السابق، ص٣٦.

(٤) د. عمار عباس الحسيني، المرجع السابق، ص٦٢.

**٥-المجرم المعلوماتي مجرم محترف:**

لا يسهل على الشخص الهاوي، إلا في حالات قليلة، أن يرتكب جرائم بطريق الحاسوب، فالأمر يقتضي كثيراً من الدقة والتخصص في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكومبيوتر كما يحدث في البنوك مثلاً[١].

وهذا الاحتراف أو المهارة يكتسبها المجرم المعلوماتي أما من الدراسة في مجال تكنولوجيا المعلومات أو عن طريق الخبرة العملية في هذا المجال أو التفاعل الاجتماعي مع الآخرين[٢].

**٦- المجرم المعلوماتي متكيف اجتماعياً:**

يُوصف المجرم المعلوماتي بأنه إنسان اجتماعي فهو لا يضع نفسه في حالة عداء سافر مع المجتمع الذي يحيط به، بل هو متكيف اجتماعياً انطلاقاً من كونه إنسان ذكي، وتطبيقاً لذلك فإن الكثير من الجرائم الإلكترونية ترتكب بدافع الكبرياء كالمستخدم المطرود من عمله أو ترتكب بدافع الاحتيال أو اللهو أو لإظهار مدى ما يتمتع به المجرم من تفوق في مواجهة أنظمة المعلوماتية[٣].

ويتضح من البحوث والدراسات التي أجريت على الجرائم الإلكترونية في أمريكا وأوربا، أن معظم مرتكبي هذه الجرائم ينتمون إلى الجيل الحديث من الشباب في المرحلة السنية مابين ٢٥ و٤٥ سنة[٤]، ويمكن تصنيف المجرمين في هذا المجال إلى ثلاثة أصناف:

---

(١) د. غنام محمد غنام، المرجع السابق، ص٦٢٨.

(٢) د. عمار عباس الحسيني، المرجع السابق، ص٦٢.

(٣) د. عمار عباس الحسيني، المرجع السابق، ص٦٢.

(٤) خالد عياد الحلبي، المرجع السابق، ص٣٣.

**-المجرمون المحترفون:**

وهم الذين يملكون المعرفة اللازمة والتقنية الكافية للتلاعب بالحاسوب وفقاً لهواهم وكذلك للتهرب من كشف جرائمهم والاحتراف في الجرائم الإلكترونية، وقد يكون الجاني في بعض الجرائم الإلكترونية مستخدماً فقط، وهو من تتوافر لديه المعرفة الكافية بآلية عمل الحاسوب ومكوناته ووظائفه الأساسية، ومعرفة بعض البرامج التي يجري العمل بها، كالبرامج المحاسبية والمالية والمصرفية والأمنية والاجتماعية[١].

**-المجرمون العاملون بمجال الحاسوب:**

لقد كثر عدد العاملين بمجال الحاسوب وتفوق مجموعة منهم، فأصبح هناك مبرمجون يتمتعون بمستوى عال من المهارة والتقنية في استخدام الحاسوب، وتميزت قدرتهم على اختراق الأنظمة الحاسوبية للغير والدخول إلى البرامج والمعلومات والبيانات وعلى إتلافها رغم الحذر والاحتياط، وأن أي استغلال سيء أثناء القيام بعملهم بتشغيل الحاسوب وإدخال البيانات والمعلومات مع المعرفة بقدرات الحاسوب، يؤدي إلى ارتكاب مجموعة من الجرائم غير المرئية[٢].

**-الهواة أو العابثون الصغار:**

اصطلح على تسمية العابثين بـ(hackers) وهي فئة من صغار السن مولعون بالحاسوب، يحاولون الدخول إلى المواقع المختلفة سواء عبر شبكة الإنترنت، أو عبر الشبكات المحلية للحاسوب، حيث ترتكب المخالفات غالباً عن غير قصد، أو عن غير إرادة شريرة وهي الفئة الأقل خطورة، ومن أشهر الأمثلة على ذلك المجموعة التي اشتهرت في أمريكا بارتكاب أكثر من ٦٠ تعرضاً أدت إلى تكلفة مبالغ طائلة، لأن عملها يقتصر على مجرد الاطلاع على البيانات،

---

(١) خالد عياد الحلبي، المرجع السابق، ص ٣٤.

(٢) خالد عياد الحلبي، المرجع السابق، ص ٣٤ – ٣٥.

ومحاولة نشر ما تطلع عليه هذه الفئة من معلومات وبيانات سرية على شبكة الإنترنت، وغالباً ما تكون هذه الفئة حسنة النية، لأنها تعتقد أن ما تقوم به من أعمال غير معاقب عليها[١].

والجرائم التي يرتكبها العابثون بالحاسوب هي جرائم تدمير وإتلاف البرامج والبيانات والمعلومات الخاصة بالغير والمخزنة على الحاسوب، وإدخال الفيروسات لتخريب محتوياته، وكذلك جرائم تعديل أو حذف أو تغيير البرامج والبيانات والمعلومات المخزنة على الحاسوب للغير بشكل غير مشروع، لمحاولة نقل أموال من حساب شخص آخر إلى حسابه الخاص أو إلى حساب شخص غيره، والدخول لحاسوب الجامعة ومحاولة شطب العلامات وتغييرها، ونشر المعلومات المتعلقة بالآخرين وإفشاء أسرارهم[٢].

**ب – المجني عليه في الجرائم الإلكترونية:**

المجني عليه في الجرائم الإلكترونية، هو من يكون ضحية الاعتداءات غير المشروعة على مكونات الحاسوب، وقد يكون شخصاً طبيعياً أو شركة أو مؤسسة تتعامل بمجال الحاسوب، أثناء ممارسة الأعمال التجارية أو الاقتصادية أو السياسية، والتي ينبغي أن تستغل الحاسوب في إدارة أعمالها، ويفترض أن يكون لدى المجني عليه حاسوب أو أكثر مرتبط بشبكات المعلومات الإلكترونية، لأن الجريمة تقع على ما يحتويه الحاسوب من برامج ومعلومات وبيانات، ولا تتم الجريمة إلا من خلال حاسوب آخر يخص الجاني[٣].

وتستهدف الجرائم الإلكترونية بشكل خاص البنوك، والمواقع الإلكترونية للمؤسسات المالية، وتفسير ذلك هو أن هذه القطاعات المستهدفة بهذه الجرائم

---

(١) خالد عياد الحلبي، المرجع السابق، ص ٣٥ – ٣٦.
(٢) خالد عياد الحلبي، المرجع السابق، ص ٣٦ – ٣٧.
(٣) خالد عياد الحلبي، المرجع السابق، ص٣٧.

تعتمد أكثر من غيرها على أجهزة الحاسوب وتُعد البنوك من أهم تلك القطاعات وأكثرها تضرراً[١].

فالإجرام المعلوماتي يصيب في الجزء الأعظم منه الأنشطة الاقتصادية والمالية للمجتمع، بيد أن المعلومات المجردة تُعد كذلك في الواقع المعاصر من أهم المصالح المستهدفة بعد الأموال، إذ أن لهذه المعلومات قيمة وثمن (prix) قد يكون عالي الأهمية، ويلجأ المجرم المعلوماتي ولغرض الحصول على المقابل والعوض، إلى طريقة المقايضة غير المشروعة لهذه المعلومات أو بيعها لغير أصحابها الشرعيين، ويمكن تصور ذلك بالنسبة للمعلومات التالية:

١-المعلومات المالية المرتبطة بالمركز المالي والحسابي والإداري وانتقال الأموال والاستثمارات.

٢-المعلومات التجارية، وخصوصاً فيما يتعلق بالتجارة الإلكترونية وعمليات التجسس والقرصنة الحاصلة عليها.

٣-المعلومات الشخصية، المرتبطة بخصوصيات الأشخاص الطبيعية أو المعنوية كالشركات وغيرها وسواء كانت المعلومات مخزنة في ذاكرات الحواسيب أو مدخلة في بنوك المعلومات في شبكة الإنترنت، إذ يتم تشويهها وإظهارها على غير حقيقتها ويدخل في هذا النوع ما يتعلق بأسرار الدولة والمشاريع الصناعية المرتبطة بالتسليح الحربي وغيرها، ويبدو أن المعلومات الأخيرة هي الأكثر تعرضاً للاعتداءات من غيرها[٢].

---

(١) إذ بلغت نسبة هذه الجرائم الموجهة ضد البنوك ١٩% من هذه الجرائم، والنسبة الموجهة للإدارة ١٦% ، والموجهة للإنتاج الصناعي ١٠%، وتليها شركات التأمين والشركات الخاصة. راجع: خالد عياد الحلبي، المرجع السابق، ص٣٧ – ٣٨.

(٢) د. سليم عبدالله الجبوري، الحماية القانونية لمعلومات شبكة الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠١١م، ص٣١٣-٣١٤.

وتجدر الإشارة إلى أن من الصعب تحديد ضحايا هذه الجرائم على وجه الدقة لأن هؤلاء الضحايا لا يعلمون شيئاً عنها إلا بعد أن تقع بالفعل، وفي هذه الحالة يرون أنه من الحكمة عدم الإبلاغ عنها، وبالتالي لا يحبذ أكثرهم أن يعترف بأن نظامه المعلوماتي قد وقع ضده انتهاك ما، وهذا السلوك السلبي يعد مغرياً لمرتكبي هذه الجرائم للاستمرار في نشاطهم(١).

## الفرع الثاني

## ملاءمة الدليل الإلكتروني لإثبات الجريمة الإلكترونية

هذا النوع من الجرائم يستخدم فيه الحاسوب الآلي أو الآلة بصفة عامة، بحيث يكون الاعتداء واقعاً إما على الكيان المادي للآلة – وهذه يمكن اعتبارها جريمة تقليدية تلحق النوع الأول – وإما أن يكون الاعتداء واقعاً على الكيان المعنوي للحاسب أو الآلة أو على قاعدة البيانات أو المعلومات التي تكون على شبكة المعلومات العالمية، مثل انتهاك الملكية الفكرية وجرائم القرصنة وغيرها، وهذا النوع من الجرائم هو ما يمكن تسميته بالجرائم الإلكترونية والتي يكون الدليل الإلكتروني هو الدليل الأفضل(٢) لإثباتها إن وجد(٣).

وبالتالي تستند عملية الإثبات الجزائي في جرائم الحاسوب والإنترنت – الجرائم الإلكترونية – على الدليل الإلكتروني باعتباره الوسيلة الوحيدة والرئيسة

---

(١) خالد عياد الحلبي، المرجع السابق، ص٣٧.

(٢) هنالك من يرى إن الجريمة الإلكترونية رغم شدة صلتها بالدليل الإلكتروني إلا أن إثباتها لا يقتصر عليه، فمن الممكن إثباتها بأدلة الإثبات التقليدية كالشهادة والاعتراف وغيرها انظر في ذلك: أ.م.د. علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب الثانوية والأمنية للعمليات الإلكترونية، مؤتمر نظمته أكاديمية شرطة دبي، مركز البحوث والدراسات رقم (١) في الفترة ٢٦ – ٢٠٠٣/٤/٢٨م، ص٢٣.

(٣) د. ميسون خلف حمد الحمداني، المرجع السابق، ٢٠٧.

لإثبات هذه الجرائم الحديثة العهد[١]، فنظراً لتعاظم دور تقنية المعلومات خاصة بعد دخول الإنترنت شتى مجالات الحياة، لذلك فإن الدليل الإلكتروني هو الدليل الأفضل لإثبات الجرائم التي تقع في هذا الوسط لأنه من الطبيعة ذاتها[٢].

كما أن الدليل الإلكتروني والخصائص التي يتمتع بها أكسبته طابعاً مميزاً جعلته الأفضل لإثبات الجرائم الإلكترونية، مثل جرائم الاعتداء على نظم المعالجة الآلية، لأنه من طبيعة الوسط الذي ارتكبت فيه[٣].

وفي تقدير البعض[٤] أن الأدلة الإلكترونية في إثبات الجرائم الإلكترونية أدلة قاطعة وجازمة إذا ما تم الحصول عليها بصورة فنية صحيحة فمثلاً عنوان البريد الإلكتروني هو عنوان لمستخدم واحد في ساعة معينة ودقيقة وثانية ومكان وعنوان هذا إذا كانت وسيلة الاتصال بالإنترنت مسجلة تسجيلاً صحيحاً فهو يذهب بالاتهام إلى شخص بعينه طبيعي أو اعتباري وعلى أقل تقدير يمكن محاكمته على المسؤولية التقصيرية إذا ثبت عدم علمه بما تم ارتكابه من جرائم إلكترونية عبر الإنترنت أو وسيلة الإنترنت المسجلة باسمه وهذا يمكن أن يستقر عليه القضاء سوابقاً ويعمل على إثبات الجرائم الإلكترونية.

ومن الملاحظ أنه قد يكون الدليل الإلكتروني متضمناً إثبات الجريمة ومرتكبها معاً، فجسم الجريمة الإلكترونية عادة هو الدليل الإلكتروني ذاته، وقد يكون هذا الجسم "الدليل الإلكتروني" متضمناً ما يفيد نسبة الجريمة لشخص ما، كما لو أرسل شخص لآخر رسالة عبر البريد الإلكتروني تتضمن فيروسات تؤدي إلى إتلاف الموقع الإلكتروني الخاص بذلك الشخص، فإن هذه الرسالة بذاتها تُعد

---

(١) خالد عياد الحلبي، المرجع السابق، ص٢٢٩.

(٢) د. ميسون خلف حمد الحمداني، المرجع السابق، ٢٠٧.

(٣) سهى إبراهيم داود عريقات، المرجع السابق،ص١٩.

(٤) معمر علي إبراهيم محمد، المرجع السابق، ص٣٩.

دليلاً على وقوع الجريمة، وفي الوقت نفسه ستُعد دليلاً على نسبة ارتكابها لشخص معين وهو المرسل إذا تضمنت بيانات تدل على شخصيته[١].

**لكن السؤال الذي يطرح نفسه هو: ماذا لو اقتصر الدليل الإلكتروني على إثبات الجريمة الإلكترونية دون إمكان نسبتها إلى مرتكبها، فهل يفقد صفته كدليل إثبات؟**

يذهب الرأي الراجح إلى أنه إذا كانت غاية الدليل عموماً إثبات الجريمة ونسبتها إلى مرتكبها، فإن هذا الدليل لا يكون قاصراً إذا اقتصر على مجرد إثبات وقوع الجريمة دون تحديد مقترفها، إذ مع ذلك تصح تسميته كدليل، وتبدو أهمية هذا النوع من الأدلة بالنسبة للجريمة الإلكترونية لصعوبة إثبات وقوعها عادة[٢].

ومما سبق يمكن القول أن الدليل الإلكتروني يصلح لإثبات الجريمة التي ترتكب ضد الكيان المعنوي للآلة أو ضد شبكة المعلومات العالمية[٣].

ومع ذلك هناك من يرى[٤] أن الجريمة الإلكترونية رغم شدة صلتها بالدليل الإلكتروني إلا أن إثباتها لا يقتصر عليه، فمن الممكن إثباتها بأدلة الإثبات التقليدية كالشهادة والاعتراف وغيرها، ولذلك يمكن القول أنه لا تلازم بين مشكلة الدليل الإلكتروني وإثبات الجريمة الإلكترونية، فلهذه الأخيرة إشكالات قانونية أخرى لا شأن لها بالدليل الإلكتروني.

**ونحن نرى أن الدليل الإلكتروني هو الأكثر ملاءمة والأفضل لإثبات الجرائم المستحدثة وعلى رأسها الجرائم الإلكترونية، لكنه ليس الدليل الوحيد لإثبات هذه الجرائم، فيمكن من وجهة نظرنا مثلاً التعويل على اعتراف المتهم بارتكابه جريمة**

---

(١) أ. طارق محمد الجملي، المرجع السابق، ص٤٩.

(٢) أ. طارق محمد الجملي، المرجع السابق، ص ٤٨. د. ميسون خلف حمد الحمداني، المرجع السابق، ص٢٠٨.

(٣) د. ميسون خلف حمد الحمداني، المرجع السابق، ٢٠٨.

(٤) أ. طارق محمد الجملي، المرجع السابق، ص ٤٨.

**إلكترونية والذي أدلى به عقب القبض عليه واستجوابه من قبل سلطة التحقيق ومواجهته، كما أن الخبرة يمكن أن تكون دليل لإثبات الجرائم الإلكترونية بالاستعانة بخبير معلوماتي، كما يعترف الفقه وخاصة الفقه الفرنسي والمصري بما يسمى الشاهد المعلوماتي، فيمكن لجهة التحقيق أن تستمع إلى الشاهد المعلوماتي والشهادة دليل إثبات تقليدي يمكن أن يعول عليه لإثبات الجرائم الإلكترونية، والصحيح أن بعض الجرائم الإلكترونية قد لا يتوافر فيها أدلة تقليدية، إلا إنه لا يمكن بأي حال من الأحوال تعميم الفكرة ورفض الأدلة التقليدية في مجال الجرائم الإلكترونية.**

## الفرع الثالث

## الحجج المبررة لملاءمة إثبات الجريمة الإلكترونية بالدليل الإلكتروني

إن اعتبار الدليل الإلكتروني هو الدليل الأفضل والأنجع في إثبات هذه الجرائم، يرتكز على الحجج التالية:

**أولاً: قصور الأدلة التقليدية في إثبات الجرائم الإلكترونية:**

ليس بخاف أن المستندات الورقية كمحل تقع عليه جرائم التزوير قد تغير مفهومها بسبب ثورة الاتصالات عن بُعد، فقد ظهرت اليوم المستندات الإلكترونية، وأصبحت هذه المستندات تصلح في كثير من التشريعات لتكون محلاً يقع عليه التزوير. ولا شك في أن ظهور هذه المستندات الرقمية سيغير من طرق الإثبات الجزائي بالنسبة للجرائم التي تقع عليها، ذلك أن الطرق التقليدية قد لا تقوى على إثباتها، ومن ثم فإن الأمر يحتاج إلى إثبات جزائي جديد يكون في استطاعته إثبات هذا النوع من التزوير، خاصة بعد أن ظهر التوقيع الإلكتروني، وأصبح يتمتع بحجية في الإثبات في الكثير من التشريعات[١]. فإذا كان الاعتراف هو سيد الأدلة، يليه

---

(١) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٥٩.

شهادة الشهود، فضلاً عن القرائن والآثار الناجمة عن النشاط الإجرامي بما لها من دور في إثبات الجريمة الإلكترونية وكشف الحقائق فيها، وهي أمور تعين المحقق على استجواب المتهمين وسؤال الشهود. وإذا صدق ما سبق بالنسبة لجرائم قانون العقوبات التقليدي، فإن قواعد هذا القانون تبدو قاصرة إزاء ملاحقة مرتكب الجريمة الإلكترونية مما حدا بالبعض إلى القول بأن قواعد قانون العقوبات التقليدية تواجه تحديات إزاء مواجهة الجريمة الإلكترونية، وتبدو قاصرة عن مواجهة العديد من الأفعال التي تهدد مصالح اجتماعية واقتصادية ارتبطت بظهور وانتشار جهاز الحاسوب الآلي وشبكة المعلومات الدولية (الإنترنت)[١].

وهناك من يرى[٢] أن الثورة العلمية في الاتصالات لم تؤثر فقط في نوعية الجرائم التي ترتبت عليها، وفي نوعية الجناة الذين يرتكبون هذه الجرائم، وإنما أثرت تأثيراً كبيراً على الإثبات الجزائي، وعلى طرق هذا الإثبات، بحيث يمكن القول أن أدلة الإثبات التقليدية قد أصبحت غير ناجعة بالنسبة لإثبات الجرائم الإلكترونية.

ونظراً لقصور الأدلة التقليدية في إثبات الجرائم الإلكترونية، يذهب بعض الفقه[٣] إلى أن بعض الأدلة التقليدية تحتاج لتطوير لتتناسب مع الطبيعة الخاصة لهذه الجرائم، فالخبرة مثلاً تصلح لإثبات الجريمة الإلكترونية إلا أنها تحتاج إلى أن يكون الخبير متمتعاً بمستوى عال من العلم والمهارة الفنية التي تمكنه من شق طريقه بنجاح في مجال إثبات هذه الطائفة من الجرائم.

كما أن الاستجواب في الجرائم الإلكترونية الناتج عنه اعتراف المتهم تحكمه ذات القواعد لاستجواب المتهم في أي جريمة تقليدية، لكن لابد من ضرورة تأهيل السلطة المختصة التي تتولى إجراء الاستجواب، ذلك أن المحقق

---

(١) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٩١.

(٢) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٥٩.

(٣) أ. طارق محمد الجملي، المرجع السابق، ص٤٨.

الجنائي لا بد أن يكون مؤهلاً للتحقيق في جرائم الحاسوب والإنترنت حتى يمكن له استيعاب واقعة التحقيق والتعامل مع مفردات الجريمة ومصطلحاتها، سيما أن المجرم الذي يحقق معه ليس مجرماً عادياً، فالمجرم في الجريمة الإلكترونية له طبيعة خاصة فيما يتعلق باستخدام تقنيات الحاسوب، وعلى ذلك فالقواعد العامة واحدة في استجواب الجريمة الإلكترونية والجريمة التقليدية، ولكن يتعين لنجاح إجراء الاستجواب في الجريمة الإلكترونية ضرورة تأهيل المحقق الجنائي بمفردات الحاسوب وتطبيقاته(١).

حيث أن مضمون الاستجواب في الجريمة الإلكترونية يتحدد بمدى إلمام المحقق الجنائي بمفردات هذه الجريمة وطبيعتها على نحو يمكنه من مواجهة المتهم بالأدلة حتى يعطى فرصة له للدفاع عن نفسه وتفنيد هذه الأدلة، ولاشك أن تأهيل المحقق الجنائي في مثل هذا النوع من الجرائم يجعله قادراً على استيعاب كل دفاع المتهم الأمر الذي يجعل حيادية المحقق والتحقيق حقيقة عملية(٢).

**ثانياً: مواكبة التطور العلمي:**

إن التطور العلمي قد أفرز ثورة الاتصالات عن بُعد، التي جاءت للبشرية بتكنولوجيا جديدة نراها في مختلف نواحي الحياة كالتجارة الإلكترونية وظهور الحاسبات الآلية وشبكات الاتصال المختلفة والإدارة الإلكترونية، فإنه يمكن القول إننا نعيش اليوم عصر الثورة الرقمية التي حلت فيها الذبذبات والنبضات محل الأوراق والكتابة والتوقيعات التقليدية(٣)، ونتيجة التطور العلمي وثورة المعلومات والأعمال الإلكترونية، فإن الدليل الجزائي التقليدي أصبح لا يتوافق بشكل كامل مع طبيعة

---

(١) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٤٠٤.

(٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٤٠٩.

(٣) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٥٧.

الوسط الذي ارتكبت فيه الجريمة حتى يستطيع القاضي أن يبني عليه القناعة الكاملة في الإثبات[١].

فقد أدى انتشار استخدام الحاسوب على نطاق عالمي إلى ضرورة تطوير أدلة الإثبات بما يواكب التطور في وسائل الإجرام المعلوماتي، وهذا الأمر هو الذي دفع المنظمة الأوربية للاقتصاد والتعاون والتنمية المعروفة باسم (OECD) والمجلس الأوربي إلى إعداد دليل لقواعد استخدام الحاسوب عام ١٩٨٣م، وفي عام ١٩٨٦م أصدرا معاً دليلاً آخر عن الجرائم التي لها علاقة بالحاسوب ودور القانون في مختلف الدول تجاه هذا النوع المستحدث من الجرائم، وقد تم تطوير هذه القواعد عامي ١٩٨٩م، ١٩٩٢م، ثم أصدرت المفوضية الأوربية في عام ٢٠٠٢م قواعد التحقيق في الجرائم عبر الحاسوب [٢].

**ثالثاً: الطبيعة الخاصة لإثبات الجرائم الإلكترونية:**

إن الحقيقة تحتاج دائماً إلى دليل، وإذا كانت هذه الحقيقة قابلة للتطور فإن الدليل الذي تقوم به لابد أن يكون هو الآخر متطوراً لكي يقوى على إثباتها[٣].

وليس صحيحاً ما قاله الكثير من الإعلاميين الغربيين في المراحل الأولى لظاهرة الحاسوب أنها ليست أكثر من (نبيذ قديم في زجاجة جديدة)، بل إنها بحق، جرائم جديدة في محتواها ونطاقها ومخاطرها، ووسائلها، ومشكلاتها، وفي الغالب في طبائع وسمات مرتكبيها[٤].

---

(١) خالد عياد الحلبي،المرجع السابق، ص٢٢٩.

(٢) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص ١٢.

(٣) د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجريمة الإلكترونية، بحث منشور على شبكة الإنترنت على الموقع التالي:

www.f - law.net/law/showthread.php?t=2208. تاريخ الدخول في ٢٠١٨/٨/٢٢م.

(٤) د. عيسى مدالله المخول، المرجع السابق، ص٣١.

وإن الطبيعة الخاصة للجرائم الإلكترونية أو جرائم الحاسوب والإنترنت سوف ينعكس على طبيعة الإثبات الجزائي لهذه الجرائم[١]، ونظراً للطبيعة الخاصة للجرائم الإلكترونية فإن دليل إثباتها يختلف ويتميز عن الدليل الجزائي التقليدي[٢].

وكمثال على الطبيعة الخاصة للجرائم الإلكترونية في الإثبات هو أن الجرائم التي تقع على بطاقات الائتمان تتميز بطبيعة خاصة الأمر الذي يتطلب إتباع طرق مختلفة عن طرق إثبات الجرائم التقليدية[٣].

وبالتالي هناك صعوبة في إثبات الجرائم الإلكترونية بالأدلة التقليدية وذلك لحداثتها واختلاف قواعد إثباتها عن الجرائم التقليدية[٤].

ومن ثم أضحى إثبات الجرائم الإلكترونية يحتاج إلى أدلة تتميز بطبيعة خاصة عما ألفناه في الجرائم التقليدية[٥]، حيث أصبح الدليل الإلكتروني ضرورة لكشف أنماط الجرائم عبر الحاسوب [٦].

**ونحن نرى أن من أهم الحجج لملاءمة إثبات الجريمة الإلكترونية بالدليل الإلكتروني، هو الطبيعة الخاصة التي تتميز بها الجرائم الإلكترونية والمستمدة من ارتكاب هذه الجرائم في العالم الافتراضي وليس المادي مما استوجب أن يكون دليل إثباتها أي الدليل الإلكتروني من الطبيعة ذاتها.**

---

(١) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص٦٣.

(٢) سهى إبراهيم داود عريقات، المرجع السابق، ص١١.

(٣) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، المرجع السابق، ص ٥٢.

(٤) معمر علي إبراهيم محمد، المرجع السابق، ص٢٦.

(٥) د. محمد أحمد المنشاوي، المرجع السابق، ص٥١٧.

(٦) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص ٩.

# المطلب الثاني

# نطاق العمل بالدليل الإلكتروني في الجرائم التقليدية

**إن السؤال الذي يطرح نفسه هنا هو: هل الدليل الإلكتروني ينحصر مجاله كدليل إثبات فقط على الجرائم الإلكترونية أم يمتد ليشمل إثبات الجرائم التقليدية؟**

في الواقع لا بد لنا من التمييز بين نوعيين من الجرائم التقليدية (الجرائم التقليدية المختلطة والجرائم التقليدية الصرفة)، ولذلك سنقوم بتقسيم هذا المطلب إلى فرعين ندرس في:

**الفرع الأول: نطاق العمل بالدليل الإلكتروني في الجرائم التقليدية المختلطة.**

**الفرع الثاني: نطاق العمل بالدليل الإلكتروني في الجرائم التقليدية الصرفة.**

## الفرع الأول

## نطاق العمل بالدليل الإلكتروني في الجرائم التقليدية المختلطة

إن بحث نطاق العمل بالدليل الإلكتروني في الجرائم التقليدية المختلطة (المرتكبة بواسطة الآلة)، يقتضي منا، أولا، تحديد مفهوم الجرائم التقليدية المختلطة، وثانياً، البحث في ملاءمة الدليل الإلكتروني لإثبات الجرائم التقليدية المختلطة، كمايلي:

**أولا: مفهوم الجرائم التقليدية المختلطة:**

إذا كانت الجريمة مرتكبة من خلال النظام المعلوماتي بحيث يكون وسيلة تنفيذها وأداتها، فإننا نكون إزاء جرائم تقليدية أداة ارتكابها ووسيلة تنفيذها هي الحاسوب أو النظام المعلوماتي عامة[١].

---

(١) أ. د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، المرجع السابق، ص٤٤٣.

وكما سبق أن قلنا عندما عرَّفنا الدليل الإلكتروني أنه لا يستخرج من الحاسوب فقط، بل من أي جهاز تقني آخر، حيث أن حصر تعريف الدليل الإلكتروني على جهاز الحاسوب معناها أن الدليل الإلكتروني يثبت الجرائم الإلكترونية فقط، غير أنه يمكن أن ترتكب جرائم تقليدية باستخدام التكنولوجيا الحديثة وهذا للاستفادة من مزاياها(١). وهذا النوع من الجرائم لا يُعد استخدام الحاسوب أو الشبكة العالمية للمعلومات أو الإنترنت من طبيعة الفعل الجرمي أو ركناً من أركان الجريمة بمعناها القانوني، فهنا الحاسوب أو الإنترنت أو الشبكة هي وسيلة ارتكاب الجاني للجريمة والتي يمكن ارتكابها بأي وسيلة أخرى(٢).

ويمكن تحديد مفهوم الجرائم التقليدية التي ترتكب بواسطة نظم المعلومات وخاصة شبكة الإنترنيت بأنها: " تلك الجرائم التي كانت موجودة قبل عصر المعلومات، ولكن بعد ظهور هذه التقنية وانتشار الشبكات أصبحت ترتكب بواسطتها، فراحت تبدو وكأنها جرائم جديدة. ومن هذه الجرائم: جريمة التهديد بالقتل وجريمتي الذم والقدح التي ترتكب عبر البريد الإلكتروني، والجرائم المخلّة بالأخلاق والآداب العامة التي ترتكب عبر المواقع الإباحية وغير ذلك من الجرائم"(٣).

كما تُعرَّف بأنها: " الجرائم التي يكون الحاسب الآلي وسيلة لارتكابها كالاحتيال والتزوير بواسطة الحاسب"(٤).

ولقد كانت هذه الجريمة مندمجة في جرائم الحاسوب وتعد جزء منها، إذ كان مصطلح جرائم الحاسوب يستخدم للدلالة على كل صور جرائم الحاسوب سواء أكان الحاسوب هدفاً صريحاً للفعل الإجرامي أو وسيلة له، إلا أنه بعد اتساع جرائم

---

(١) د. هلال آمنة، المرجع السابق، ص٩.

(2) Brian Carrier. Defining Digital Forensics Examination and Analysis Tools. In Digital Research Workshop II, 2002, Available at: http://www.Dfrws.org/dfrws2002/papars/papars/Brian Carrier.pdf.

(٣) د. محمد طارق الخن، المرجع السابق، ص٢٤.

(٤) د. عيسى مدالله المخول، المرجع السابق، ص٣٤.

الحاسوب وولادة جرائم الإنترنت أصبح مصطلح الجرائم المتعلقة بالحاسوب يُعد من الجرائم التي يكون الحاسوب وسيلة لارتكابها، أي أنها كل فعل غير مشروع يستخدم الحاسوب في ارتكابه كأداة رئيسية[١].

إذاً هذا النوع من الجرائم يستخدم فيه الحاسوب الآلي والانترنت كوسيلة مساعدة لارتكاب الجريمة مثل استخدامه في الغش والاحتيال وغسل الأموال وتهريب المخدرات، وهذا النوع من الجرائم لا صلة له بالوسط الافتراضي إلا من حيث الوسيلة، وبكلمة أوضح فإن الجريمة في هذه الحالة هي جريمة تقليدية استعملت في ارتكابها أداة رقمية[٢].

فمثلاً الإرهاب الإلكتروني لا يختلف عن الإرهاب التقليدي إلا من حيث الوسيلة المستخدمة في ارتكابه، وهي شبكة المعلومات الدولية[٣].

وعلى الرغم من قلة النصوص التشريعية التي تعاقب من يرتكب جرائم بالوسائل الإلكترونية، ولكن نجد في بعض نصوص التشريعات نصوص قانونية مستحدثة تعاقب كل من يرتكب جريمة باستخدام الوسائل الإلكترونية، ومن هذه التشريعات التشريع الأردني والذي جاء بقانون المعاملات الإلكترونية المؤقت رقم (٨٥) لعام٢٠٠١م، حيث نصت المادة (٣٨) منه على أن: "يعاقب كل من يرتكب فعلاً يشكل جريمة بموجب التشريعات النافذة بواسطة استخدام الوسائل الإلكترونية بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على السنة أو بغرامة لا تقل عن (٣٠٠٠) ثلاثة آلاف دينار ولا تزيد على (١٠٠٠٠) عشرة آلاف دينار أو بكلتا هاتين العقوبتين ويعاقب بالعقوبة الأشد إذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذا القانون"[٤].

---

(١) د. عيسى مدالله المخول، المرجع السابق،ص٣٤-٣٥.

(٢) د. ميسون خلف حمد الحمداني، المرجع السابق، ٢٠٧.

(٣) عبد العزيز خنفوسي، المرجع السابق، ص١٤٤.

(٤) سهى ابراهيم داود عريقات، المرجع السابق، ص١٢.

وكذلك التشريع السوري حيث عاقب المشرع السوري على الجرائم التقليدية المرتكبة بواسطة نظم المعلومات وخاصة شبكة الإنترنيت في المادة (٢٨) من قانون مكافحة الجريمة المعلوماتية لسنة ٢٠١٢م على أنه: (أ- إذا انطبق نصّ في القوانين الجزائية النافذة على إحدى الجرائم المنصوص عليها في هذا القانون، تُطبَّق العقوبة التي هي أشد.

ب- يُضاعف الحدّ الأدنى للعقوبة المقرّرة لأي من الجرائم المنصوص عليها في القوانين الجزائية النافذة الأخرى في إحدى الحالتين التاليتين:

١- إذا ارتُكبت الجريمة باستخدام الشبكة أو وقعت على الشبكة.

٢- إذا وقعت الجريمة على جهاز حاسوبي أو منظومة معلوماتية، بقصد التأثير على عملها، أو على المعلومات أو البيانات المخزّنة عليها).

وسنتناول الأحكام التي جاءت بها هذه المادة على التتالي:

## أ-تطبيق النصوص الجزائية:

أشارت الفقرة (أ) من المادة ٢٨ من قانون مكافحة الجريمة المعلوماتية إلى أنه إذا انطبق نص في القوانين الجزائية النافذة على إحدى الجرائم المنصوص عليها في قانون مكافحة الجريمة المعلوماتية فيجب تطبيق النص ذو العقوبة الأشد، والغاية من هذا النص واضحة، وهي رغبة المشرع في تطبيق العقوبة الأشد في حالة انطباق نصين على واقعة ما تتعلق بجرائم المعلوماتية، والمثال على ذلك هو أن المادة (٢٩) من قانون مكافحة الجريمة المعلوماتية تعاقب بالحبس من ستة أشهر إلى ثلاث سنوات والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية على كل من يقوم بالترويج لأي جريمة باستخدام الشبكة، وقد جاءت المادة ٨ من قانون مكافحة الإرهاب الصادر بالقانون رقم ١٩ تاريخ ٢٠١٢/٧/٢ لتعاقب بالأشغال الشاقة المؤقتة جريمة ترويج الأعمال الإرهابية المرتكبة على موقع إلكتروني، ففي هذه الحالة يجب على المحكمة أن تطبق النص ذو العقوبة الأشد وهو نص المادة ٨ من قانون مكافحة الإرهاب.

**ب- ارتكاب الجرائم التقليدية باستخدام الشبكة أو عليها:**

نصت الفقرة (ب) من المادة ٢٨ على ما يلي: (يُضاعف الحدّ الأدنى للعقوبة المقرّرة لأي من الجرائم المنصوص عليها في القوانين الجزائية النافذة الأخرى في إحدى الحالتين التاليتين:

١- إذا ارتُكبت الجريمة باستخدام الشبكة أو وقعت على الشبكة.

٢- إذا وقعت الجريمة على جهاز حاسوبي أو منظومة معلوماتية، بقصد التأثير على عملها، أو على المعلومات أو البيانات المخزّنة عليها).

وقد تستخدم الشبكة وخاصة الانترنت لارتكاب الجرائم التقليدية المنصوص عليها في التشريعات النافذة، ومن أمثلة هذه الجرائم:

- جريمة الذم المنصوص عليها بالمادة ٥٦٨ من قانون العقوبات.
- جريمة القدح المنصوص عليها بالمادة ٥٧٠ من قانون العقوبات.
- جريمة التعرض للآداب العامة المنصوص عليها بالمادة ٥١٧ من قانون العقوبات.
- جريمة التعرض للأخلاق العامة المنصوص عليها بالمادة ٥١٨ من قانون العقوبات.
- جريمة توزيع الصور والأفلام المخلة بالحياء المنصوص عليها بالمادة ٥١٩ من قانون العقوبات.
- جريمة توجيه الكلام المخل بالحشمة المنصوص عليها بالمادة ٥٠٦ من قانون العقوبات.
- جريمة التهديد بجناية مثل القتل المنصوص عليها بالمادة ٥٦١ من قانون العقوبات.
- جريمة إثارة النعرات المذهبية التي ترتكب بالكتابة أو الخطاب المنصوص عليها بالمادة ٣٠٧ من قانون العقوبات.

– جريمة الاستحصال على أسرار تتعلق بأمن الدولة المنصوص عليها بالمادة ٢٧٢ من قانون العقوبات.

– جريمة إذاعة أنباء كاذبة في الخارج من شأنها أن تنال من هيبة الدولة المنصوص عليها بالمادة ٢٨٧ من قانون العقوبات.

فجميع هذه الجرائم وغيرها يمكن أن ترتكب باستخدام الشبكة وخاصة الانترنت، والحقيقة أنه لابد من أن يكون لاستخدام الشبكة **دور إيجابي** في ارتكاب الجريمة، كأن يرتكب النشاط الجرمي بواسطة الشبكة أو أن يكون للشبكة دور على قدر من الأهمية في ارتكاب الجريمة، كإرسال عبارات التهديد بالقتل إلى المجني عليه عبر البريد الإلكتروني، أو نشر العبارات التي تثير النعرات الطائفية على موقع إلكتروني، أما إذا كان دور الشبكة ثانوياً، فلا يمكن القول بأن الجريمة ارتكبت باستخدام الشبكة، كاستخدام الشبكة لمجرد التواصل، والمثال على ذلك إرسال بريد إلكتروني من الجاني إلى المجني عليه لترتيب لقاء بينهما في مكان ما، ثم قيام الجاني بقتل المجني عليه، أو إجراء اتصال بينهما عبر الشبكة لتحديد مكان اللقاء، ففي مثل هذه الحالة لا تُعد جريمة القتل بأنها ارتكبت باستخدام الشبكة، لأن الشبكة لم يكن لها أي دور إيجابي في ارتكاب الجريمة[١].

**وهكذا نرى أن المشرع السوري عد ارتكاب الجرائم التقليدية عبر الشبكة بمثابة ظرف تشديد يشدد عقوبة فاعل الجريمة وذلك بمضاعفة الحد الأدنى للعقوبة المنصوص عليها في القوانين الجزائية ذات الصلة، وبرأينا الشخصي نرى أن نص الفقرة (أ) من المادة (٢٨) من قانون مكافحة الجريمة المعلوماتية كافي وكفيل لمعاقبة الجرائم التقليدية المرتكبة عبر الانترنت أو بواسطتها، ويُعد ظرف تشديد لأن ارتكاب هذه الجرائم باستخدام الشبكة أو عليها يجعلها أكثر خطورة وضرراً.**

---

(١) د. محمد طارق الخن، المرجع السابق،ص٦٧-٦٨.

ومن الأمثلة الواقعية على الدور الإيجابي للإنترنت في جرائم القتل، أن رجلاً قتل زوجته التي كانت موضوعة تحت المراقبة في المستشفى، بأن دخل عبر الانترنت إلى شبكة المعلومات الخاصة بالمستشفى، ثم قام بتغيير المعلومات الطبية الخاصة بالمجني عليها المريضة[١] .

وغني عن البيان فإن **الركن المعنوي المطلوب في الجرائم التقليدية** التي ترتكب في العالم المادي لا يختلف فيما إذا ارتكبت هذه الجرائم عبر الشبكة، فالعلاقة الذهنية النفسية التي يكون عليها الفاعل ساعة ارتكاب الجريمة وهي جوهر الركن المعنوي لا تتأثر لكون الجريمة ارتكبت عبر الشبكة، فجميع القواعد المتعلقة بالقصد الجرمي وعناصره وأنواعه، والخطأ وعناصره وصوره يمكن تطبيقها على الركن المعنوي في الجرائم التقليدية التي ترتكب عبر الشبكة.

وفي الجرائم الإلكترونية عموماً يمكن إثبات القصد الجرمي من خلال القرائن، فتفتيش حاسوب المشتبه به مثلاً، ومعرفة المواقع التي قام بتصفحها والأشخاص الذين اتصل بهم، قد يفيد في إثبات قصده الجرمي. ومن الوقائع الحقيقية التي تمّ فيها اكتشاف نية المدعى عليه في إحدى جرائم القتل، بأنه لدى تفتيش حاسوب المدعى عليه تبين بأنه كان يبحث عن مصطلحات مثل "قتل، خنق، وفيات، حادث" قبل قيامه بقتل زوجته، فبفضل عملية البحث هذه تم إثبات نية العمد لديه، ورفع مستوى الجريمة إلى القتل من الدرجة الأولى[٢].

## جـ- ارتكاب الجريمة على جهاز حاسوبي أو منظومة معلوماتية بقصد التأثير على عملها أو على المعلومات أو البيانات المخزنة عليها:

والحقيقة أن غاية المشرع من هذه الفقرة هي وضع نص عقابي **احتياطي** يطال مختلف الجرائم التي تهدف إلى التأثير على عمل الأجهزة الحاسوبية أو

---

(١) مشار إلى هذه القضية عند: د. محمد طارق الخن، المرجع السابق، ص٦٨.

(2 ) . Eoghan Casey, op,cit, chapter 1, p4

المعلومات المخزنة بها في الحالات التي لم يفرض قانون مكافحة الجريمة الإلكترونية عقاب عليها[١].

**ثانياً: ملاءمة الدليل الإلكتروني لإثبات الجرائم التقليدية المختلطة:**

على الرغم من عدم اتصال هذه الجريمة بالنظام المعلوماتي فإن الدليل الإلكتروني يصلح كدليل لإثباتها[٢].

فالدليل الإلكتروني لا يقتصر مجال العمل به كدليل إثبات على الجرائم الإلكترونية فهو يصلح لإثبات كافة الجرائم التي ترتكب بواسطة الحاسوب والانترنت فكثيراً ما يتم استعمال الحاسوب في تزوير أو استعمال شبكة الانترنت في إرسال ذم وقدح وتشهير أو تهديد فالحاسوب في هذه الحالة وسيلة لارتكاب الجريمة ولا يغير من وصفها كجريمة تقليدية[٣].

وبالتالي يصلح الدليل الإلكتروني لأن يكون دليل إثبات في الجرائم التقليدية المرتكبة بواسطة الحاسوب مثل جرائم غسل الأموال أو تهريب المخدرات، وعلى الرغم من عدم اتصال الجريمة بالحاسوب إلا من حيث الوسيلة لارتكاب الجريمة في مثل هذه الحالات فإن الدليل الإلكتروني يصلح ليكون دليلاً لإثباتها[٤].

---

(١) د. محمد طارق الخن، المرجع السابق، ص٦٩.

(٢) د. ميسون خلف حمد الحمداني، المرجع السابق، ٢٠٧.

(٣) خالد عياد الحلبي، المرجع السابق، ص ٢٤٥ – ٢٤٦. د. ميسون خلف حمد الحمداني، المرجع السابق، ص ٢٣٩.

(٤) سهى إبراهيم داود عريقات، المرجع السابق، ص١٩.

## الفرع الثاني

## نطاق العمل بالدليل الإلكتروني في الجرائم التقليدية الصرفة

في الحقيقة لا يوجد تلازم بين نطاق العمل بالدليل الإلكتروني وشكله في إثبات الجريمة الإلكترونية، فمن ناحية فإن الدليل الإلكتروني مثلما يصلح لإثبات الجريمة الإلكترونية ويعتبر في نفس الوقت الدليل الأفضل لإثباتها، فإنه من ناحية أخرى يصلح لإثبات الجرائم التقليدية إن جاز التعبير[١]، بل هنالك من يرى[٢] أنه بالفعل أصبح للدليل الإلكتروني دوراً مهماً في الإثبات يتم الاعتماد عليه في إثبات ليس فقط الجرائم الإلكترونية وإنما أيضاً في كل أنواع الجرائم.

كما أن هناك من يرى[٣] أن الدليل الإلكتروني يصلح لإثبات بعض الجرائم التقليدية وإن لم تكن من ضمن النوعين المذكورين (الجرائم الإلكترونية – الجرائم التقليدية المختلطة المرتكبة بواسطة الآلة)، وذلك في حال استعملت الآلة الرقمية للتمهيد لارتكاب الجريمة أو لإخفاء معالمها، كالمراسلات التي يبعث بها الجاني لشريكه وتتضمن معلومات عن جريمة ينويان ارتكابها أو يطلب إخفاء معالم هذه الجريمة، فتلك المراسلة تصلح كدليل إثبات لهذه الجريمة حال وقوعها، رغم أنها لم ترتكب ضد الآلة الرقمية أو بواسطتها.

ومما لا ينبغي إغفاله فيما يخص الفرق بين الدليل الإلكتروني، وبرامج الحاسوب الآلي، أن الدليل الإلكتروني لا يقتصر دوره في إثبات الجرائم الإلكترونية فقط، كسرقة الملكية الفكرية، وإنما يمتد أيضاً إلى الجرائم التقليدية، كالقتل،

---

(١) د. ميسون خلف حمد الحمداني، المرجع السابق، ٢٠٧.

(٢) أمجد خليل حمودة، المرجع السابق، ص١١٨.

(٣) د. ميسون خلف حمد الحمداني، المرجع السابق، ٢٠٨. . وأ. طارق محمد الجملي، المرجع السابق، ص٤٩.

والاختطاف، وأيضاً الاتجار بالمخدرات، وغيرها من الجرائم التي تستخدم فيها التقنية الإلكترونية للتسهيل فيها[١].

**ونرى أن الدليل الإلكتروني يصلح ويمكن أن يُعول عليه في إثبات الجرائم التقليدية الصرفة، فمثلاً يمكن إثبات جرائم السرقة والاختلاس التقليدية عن طريق أدلة إلكترونية والتي تكون عبارة عن مستندات إلكترونية متعلقة بالمحاسبات أو مراسلات إلكترونية بين الجاني وشخص آخر.**

**وفي هذا المبحث، درسنا نطاق العمل في الجرائم الإلكترونية، حيث بحثنا في ماهية الجرائم الإلكترونية من حيث تعريفها ومحلها وأنواعها وأصنافها والخصوم فيها، وكذلك درسنا ملاءمة الدليل الإلكتروني لإثباتها، والحجج المبررة لإثبات هذه الجرائم بالدليل الإلكتروني، وأيضاً درسنا نطاق العمل بالدليل الإلكتروني في الجرائم التقليدية بنوعيها المختلطة والصرفة، فبحثنا ملائمة الدليل الإلكتروني لإثبات الجرائم التقليدية المختلطة المرتكبة بواسطة الحاسوب مثل جرائم غسل الأموال أو تهريب المخدرات، كما بحثنا ملاءمة الدليل الإلكتروني لإثبات الجرائم التقليدية الصرفة، مثل جرائم السرقة والاختلاس التقليدية.**

---

(١) هلال آمنة، المرجع السابق، ص٩.

# الفصل الثاني
# تقدير الدليل الإلكتروني في الإثبات الجزائي

لا تقف الصعوبات التي تواجه الدليل الإلكتروني عند حد كيفية الحصول عليه، وإجراءات حفظه، بل تمتد إلى مدى القوة الثبوتية التي يتمتع بها هذا الدليل، ومدى حرية قاضي الموضوع بالاقتناع به لبناء الحكم على أساسه بالبراءة أو الإدانة. لذلك حاول المشرع والقضاء والفقه المقارن التصدي لهذه المسألة، وذلك بتحديد الشروط التي يجب توافرها في الدليل الإلكتروني أو في مخرجات الحاسوب حتى يمكن قبوله من قبل القاضي الجزائي.

واستقر الفقه والقانون على أن للقاضي الجزائي سلطة واسعة في تقدير الأدلة واستنباط القرائن، وما تحمله الوقائع من دلالات شريطة أن يكون الدليل ثابتاً بيقين، مرتبطاً بالوقائع الرئيسية ومنسجماً مع التسلسل المنطقي للأحداث. ومن الطبيعي أن ينسحب هذا الرأي على الأدلة الإلكترونية باعتبارها محكمة بقواعد علمية وحسابية قاطعة لا تقبل التأويل، كما أنها في الوقت ذاته معالجة بوسائل التقنية المعلوماتية التي أصبحت تستغل في الجرائم المستحدثة[١].

وإن عمل القاضي محصور في حدود القانون وما ينص عليه، إلا أن المشرع منح القاضي الجزائي صلاحية الملاءمة بين جميع الظروف والملابسات التي وقعت في ظلها الجريمة حتى يتسنى له الوصول للحقيقة التي يسعى إليها[٢].

---

(١) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٥٧.

(٢) د.محمد أحمد المنشاوي، المرجع السابق، ص٥١٩.

لكن السؤال الذي يطرح نفسه هو: ما مدى إعمال هذه الصلاحية في ظل الدليل الإلكتروني؟

لذلك سنقوم بتقسيم هذا الفصل إلى مبحثين ندرس في:

**المبحث الأول: حرية القاضي الجزائي في تقدير الدليل الإلكتروني.**

**المبحث الثاني: تقدير القاضي الجزائي للدليل الإلكتروني في أنظمة الإثبات المختلفة.**

# المبحث الأول

# حرية القاضي الجزائي في تقدير الدليل الإلكتروني

إن دراسة حرية القاضي الجزائي في تقدير الدليل الإلكتروني، يقتضي منا بحث مفهوم السلطة التقديرية للقاضي الجزائي في تقدير الدليل الجزائي، وكذلك دراسة الشروط الواجب توافرها في الدليل الإلكتروني حتى يخضع للسلطة التقديرية للقاضي الجزائي.

لذلك سنقسم هذا المبحث إلى مطلبين ندرس في:

**المطلب الأول: مفهوم السلطة التقديرية للقاضي الجزائي.**

**المطلب الثاني: الشروط الواجب توافرها في الدليل الإلكتروني.**

## المطلب الأول

## مفهوم السلطة التقديرية للقاضي الجزائي

إن دراسة مفهوم السلطة التقديرية للقاضي الجزائي في تقدير الدليل الجزائي، يقتضي منا بيان تعريف مفهوم السلطة التقديرية للقاضي الجزائي في تقدير الدليل الجزائي، كما يقتضي منا دراسة ضوابط السلطة التقديرية للقاضي الجزائي في تقدير الدليل الجزائي، لذلك سنقسم هذا المطلب إلى فرعين ندرس في:

**الفرع الأول: تعريف السلطة التقديرية للقاضي الجزائي.**

**الفرع الثاني: ضوابط السلطة التقديرية للقاضي الجزائي في تقدير الدليل الجزائي.**

### الفرع الأول

### تعريف السلطة التقديرية للقاضي الجزائي

من أهم ما يقع على القاضي الجزائي عند نظر الدعوى، هو تقدير أدلة الإثبات والتحقق والتثبت منها والاقتناع بها، وذلك حتى لا يدان بريء ولا يفلت من العقاب مجرم، فالقاضي قبل أن يصدر حكمه يقوم بالبحث والتثبت حتى يتبين وجه الحق في الدعوى، وهو في سبيل ذلك يقوم بفحص الأدلة المختلفة ويطرحها

في مجلس القضاء ليتناولها الخصوم بالفحص والتفنيد[١]. سعياً للوصول إلى الحقيقة التي ترضي ضميره، وتكَّون اقتناعه الشخصي لتحقيق العدالة[٢].

وعلى هذا فإن الدور الذي يقوم به القاضي في سبيل تحقيق العدالة الاجتماعية يتفق مع العقل والمنطق، فهو يحقق مصلحة المجتمع بصفة عامة، وذلك عندما يشعر الناس بالعدل والمساواة، وهذا ما يتأتى بمنح القاضي سلطة في تقدير الأدلة بهدف الوصول إلى الحقيقة.

وقد تعددت محاولات تعريف موضوع السلطة التقديرية للقاضي، ولكن هذه المحاولات كانت لها نقطة التقاء واحدة، باعتبار هذا المبدأ حالة ذهنية نابعة من ضمير القاضي النقي وتفكيره المنطقي الذي يكشف عن الحقيقة من خلال تقييمه للأدلة المطروحة في الدعوى، وبناء الجزم واليقين على ما يقتنع به من الأدلة دون إلزامه بإصدار حكمه بناءً على دليل معين مقتنع به، ورفض ما لا يقتنع به دون رقيب عليه في ذلك، فالقاضي يبني يقينه على ضوء ما يمليه عليه ضميره وتفكيره المنطقي دون أدنى تحكم[٣].

وأهم ما يبرر مبدأ حرية القاضي الجزائي في تقدير الدليل، أنه يكفل ألا تبتعد الحقيقة القضائية عن الحقيقة الواقعية، فإذا وجد القاضي الجزائي نفسه طليقاً في تحري الواقع من أي مصدر غير ملزم بدليل معين يفرض عليه التسليم بما يخالف الواقع، فإنه يصل في النهاية إلى قضاء يطابق الحقيقة الواقعية قدر ما يسمح بذلك التفكير البشري، ويدعم هذا المبدأ أن الإثبات في الدعوى الجزائية يرد على وقائع ولا يرد على تصرفات قانونية، والوقائع الجزائية لا يمكن تحديدها مسبقاً، خلافاً لما عليه الأمر غالباً في المواد المدنية، كما أن المجرمين لا يرتكبون في الغالب أفعالهم في العلن ولا يعلنون عما ينون الإقدام عليه، وتقضي مصلحة

---

(١) د. عبد الرؤوف مهدي، المرجع السابق، ص١٢٤٥.

(٢) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٢٠.

(٣) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٢٠.

المجتمع مكافحة الإجرام بكل السبل، وهذا يتطلب أن يخول المشرع القاضي الجزائي سلطة إثبات الجريمة والخطورة الإجرامية بجميع الطرق، ومنحه قدراً واسعاً من الحرية في تقديره للأدلة التي يستقيها(١).

وإن الأدلة المتحصلة من الوسائل الإلكترونية تخضع للسلطة التقديرية للقاضي الجزائي، فإن استراح إليها ضميره، ووجدها كافية ومنطقية، أمكنه أن يستمد اقتناعه منها، ويعول عليها في الحكم الذي ينتهي إليه(٢).

## الفرع الثاني

## ضوابط السلطة التقديرية للقاضي الجزائي في تقدير الدليل الجزائي

هذه الضوابط لا تتعلق بالدليل، وإنما تتعلق بالاقتناع ذاته الذي يتولد لدى القاضي الجزائي من فحص الدليل، فإذا كان المعول عليه عند الاقتناع هو اليقين القضائي الذي يمكن أن يصل إليه الكافة لاستقامته على أدلة تحمل بذاتها معالم قوتها في الإقناع وليس اليقين الشخصي للقاضي فحسب – فإنه لابد من توافر ضوابط هذا الاقتناع(٣).

فحرية القاضي الجزائي في قبول الدليل الإلكتروني ليعمل سلطته في تقديره لا يمكن أن تكون مطلقة من كل قيد خاصة أن كلاً من الفقه والقضاء قد توجس منها خيفة نظراً لما يمكن أن تخضع له طرق الحصول عليها من التعرض للتزييف والتحريف، لذا كان من الضروري رسم ضوابط وأطر معينة يتعين أن تمارس هذه السلطة في نطاقها بحيث لا تنحرف عن الغرض الذي يبغيه المشرع من ورائها، وهو الوصول إلى الحقيقة الفعلية في الدعوى(٤).

---

(١) د.محمد أحمد المنشاوي، المرجع السابق،ص٥٢١.

(٢) د.محمد أحمد المنشاوي، المرجع السابق،ص٥٢٥.

(٣) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٥٥.

(٤) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٤٢.

وهذه الضوابط هي: الضابط الأول: بلوغ الاقتناع القضائي درجة اليقين، والضابط الثاني: مواءمة الاقتناع القضائي لمقتضيات العقل والمنطق، والضابط الثالث: تقيد القاضي الجزائي بسلامة التقدير والاستدلال.

**أولاً: بلوغ الاقتناع القضائي درجة اليقين:**

يلتزم القاضي أن يبني اقتناعه على سبيل الجزم واليقين، وهذا اليقين هو اليقين القضائي وليس اليقين الشخصي، واليقين القضائي يقوم على عنصرين:

الأول شخصي: ويعني ارتياح ضمير القاضي واطمئنانه إلى إدانة المتهم على سبيل الجزم واليقين.

الثاني: موضوعي: ويعني ارتياح ضمير القاضي واطمئنانه على أدلة من شأنها أن تفض لذلك وفقاً لمقتضيات العقل والمنطق.

والجزم بوقوع الجريمة الإلكترونية ونسبتها إلى المتهم المعلوماتي يتطلب نوعاً جديداً من المعرفة، وهو المعرفة العلمية للقاضي بالأمور المعلوماتية.

ولا سبيل له في ذلك إلا في الاستئناس برأي الخبير إذا ما اطمأن إليه واقتنع به[١].

**ثانياً: مواءمة الاقتناع القضائي لمقتضيات العقل والمنطق:**

يلتزم القاضي بأن يبني اقتناعه على عملية عقلية منطقية تقوم على الاستقراء والاستنباط ينتهي في ختامها إلى نتيجة معينة[٢].

فلابد أن يكون استخلاص القاضي الجزائي لواقعة الدعوى استخلاصاً معقولاً وسائغاً، بمعنى أن يكون الدليل الإلكتروني مؤدياً إلى ما رتبه الحكم دون تعسف في الاستنتاج، أو تنافر مع مقتضيات العقل والمنطق[٣]، وفي ذلك تقول محكمة النقض المصرية إنه: "وإن كان من حق محكمة الموضوع أن تستخلص الواقعة من

---

(١) د.محمد أحمد المنشاوي، المرجع السابق، ص ٥٥٥ – ٥٥٦.

(٢) د. أحمد فتحي سرور، الوسيط في قانون الإجراءت الجنائية، د.ط، دار النهضة العربية، القاهرة، مصر، ١٩٨٥م، ص٣٩٧.

(٣) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٥٦.

أدلتها وعناصرها المختلفة فإن شرط ذلك أن يكون هذا الاستخلاص سائغاً تؤدي إليه ظروف الواقعة وأدلتها وقرائن الأحوال فيها"[١].

**ثالثاً: تقيد القاضي الجزائي بسلامة التقدير والاستدلال:**

إن سلطة القاضي الجزائي في تكوين عقيدته مقيدة بسلامة التقدير والاستدلال حرصاً على صيانة الحقوق وحفاظاً على قدسية العدالة وحسن تطبيق القانون، وهو أمر مؤتمن عليه من قبل المشرع[٢].

ومن ثم، فلا يجوز للقاضي الجزائي الخروج عن القواعد القانونية في تكوين اقتناعه، ويجب أن تبنى عقيدته بعد تدقيق الوقائع وتمحيصها بصورة سليمة ومنطقية وتعليل الأخذ بها بشكل مقبول يتفق مع المنطق السليم بصورة توحي بالاطمئنان إلى صحة قضائه، بالإضافة إلى التزامه أن يدلل على صحة هذه العقيدة في أسباب حكمه بأدلة مؤدية إليها توافرت لها شروط معينة، بغير خطأ في الإسناد، ولا فساد في الاستدلال بها، ولا إبهام أو غموض أو تناقض[٣].

**ونجد مما تقدم أن هذه الضوابط ليست قيوداً على السلطة التقديرية للقاضي الجزائي، لأن هذه السلطة المعطاة له لا تعني التحكم، بل هي لضمان الوصول إلى اليقين القضائي.**

وأخيراً هناك من يرى[٤] أنه يعطى الدور الرئيسي في إثبات الجريمة للخبير بدلاً من القاضي، ويجعل أهم الأدلة القرائن التي تخضع للفحص العلمي الدقيق، ويستخرج منها ما يثبت الإدانة أو البراءة، ولقد لقي هذا الرأي رواجاً وتفضيلاً خاصة من قبل

---

(١) نقض مصري في ٣٠ نيسان، سنة ١٩٦٣، مجموعة القواعد القانونية، الجزء الرابع، رقم ٢٠٨، ص٣٨٥.

(٢) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٥٣.

(٣) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٥٤.

(٤) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٣٩.

أنصار المدرسة الوضعية الذين تنبؤوا له بمستقبل كبير من حيث أنه سوف يحل محل نظام الاقتناع القضائي.

والحقيقة أن من شأن ذلك أن يجعل الخبير هو قاضي الدعوى، ويتم حرمان المتهم من ضمانات الحرية الفردية والكرامة الإنسانية التي لا يحسن أن يقررها سوى القاضي، بالإضافة إلى أن مباشرة الخبير عمله تفترض تحديد عناصر مهمته وتقدير قيمة تقريره، وهما وظيفتان قضائيتان، أضف إلى ذلك أن الفصل في الدعوى الجزائية يثير مسائل قانونية وشرعية، لا يحسن الخبير التعامل معها والبت فيها برأي(١).

فالتطور والتقدم في العلم وإن أثبت جدوى الأساليب الفنية المستحدثة فيما يتعلق بالأدلة، كلا أن ذلك لا يعني استبعاد نظام الاقتناع القضائي، فإذا كانت الخبرة وسيلة إثبات تهدف إلى كشف بعض الدلائل والأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية، التي لا تتوافر لدى القاضي، حيث تتطلب بعض الحالات دراية ومعرفة خاصة لا يملك القاضي الأهلية اللازمة لها مما استلزم أن يكون الخبير دوراً في الدعوى الجزائية(٢).

وإذا كان الدليل الإلكتروني شأنه شأن باقي أدلة الإثبات، يخضع لتقدير القاضي الجزائي، ومدى تأثيره في الاقتناع الذاتي، فإنه لا يمكن للخبير مهما كانت دقة نتائجه وموضوعيتها أن يحتل مكانة القاضي، في إيجاد العدالة التي يستلزمها حس خاص يدركه القاضي بوجدانه من خلال تكوينه العلمي والقضائي، ليشكل أساساً رصيناً في التقدير السليم للأدلة، الذي من خلاله يصل إلى قرار عادل يكون عنواناً للحقيقة. وعلى الرغم من ذلك فإن الدليل الإلكتروني من شأنه أن يجعل القاضي الجزائي أكثر جزماً ويقيناً، حيث يساعده على التقليل من الأخطاء

---

(١) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٣٩.

(٢) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٣٩.

القضائية، والاقتراب إلى العدالة بخطوات أوسع والتوصل إلى درجة أكبر نحو الحقيقة، الأمر الذي نستطيع معه القول بتضاؤل دور القاضي الجزائي في تقدير الدليل الإلكتروني أمام نقص الخبرة الفنية للقاضي، وتعاظم دور الخبرة في هذا المجال نظراً لصعوبة فهم الدليل المتحصل من الوسائل الإلكترونية، فالدليل الفني قد يكون مضمونه مسائل فنية، لا يقوى على فهمها إلا الخبير، إذ أنه قد يتحصل من عمليات فنية معقدة، بعكس الدليل القولي فإن الكثيرين ممن يتصلون به يسهل عليهم فهم مضمونه، وإدراك حقيقته(١).

**ونحن نرى أن الدليل الإلكتروني شأنه شأن باقي أدلة الإثبات، يخضع لتقدير القاضي الجزائي، ومدى تأثيره في الاقتناع الذاتي، ولا يمكن للخبير مهما كانت دقة نتائجه وموضوعيتها أن يحتل مكانة القاضي.**

## المطلب الثاني
## الشروط الواجب توافرها في الدليل الإلكتروني

بما أن الدليل الإلكتروني عبارة عن محرر مأخوذ من أجهزة الحاسوب وغيرها من الأجهزة التقنية، ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات تكنولوجيا خاصة، وهو مكون رقمي لتقديم معلومات في اشكال متنوعة، مثل النصوص المكتوبة أو الصور أو الأصوات والاشكال والرسوم، وبالتالي ما يتم عرضه على القاضي الجزائي سيكون في نهاية الأمر صورة من صور تلك الدعامات، أو صورة منسوخة على الورق من المحرر الإلكتروني، ومن ثم إذا ثار نزاع حول صحة هذا

---

(١) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٤٠.

الدليل، فإن على القاضي الجزائي التثبت من توافر بعض الشروط في الدليل الإلكتروني[١].

فهناك شروط معينة تحكم الأدلة الناتجة عن الحاسوب الآلي يلتزم بها القضاء لتحاشي سوء التصرف ولدعم حقوق الأطراف أو غيرها من الحقوق محل الاحترام، وهذه الشروط مدارها أصل البراءة وما يتفرع عنها من نتائج وآثار وما يتمتع عن ذلك من وجوب توافر شروط معينة في المخرجات الكمبيوترية حتى يمكن الحكم بالإدانة. ذلك أنه لا محل لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين، فإذا كان القاضي لم ينته من المخرجات الكمبيوترية التي ذكرها إلى الجزم بنسبة الفعل أو الجريمة الإلكترونية إلى المتهم المعلوماتي، كان من المتعين عليه أن يقضي بالبراءة، كما يجب أن تكون عقيدة القاضي واقتناعه بالإدانة قد استمد من مخرجات كمبيوترية طرحت بالجلسة لأن القاعدة هي أن لا يحكم إلا بناء على التحقيقات التي تحصل بالطرق والشروط القانونية لا بناء على معلوماته الشخصية، أو على ما قد يكون قدر رآه بنفسه أو حققه في غير مجلس القضاء، كما ينبغي ألا يؤسس القاضي الجزائي حكمه على دليل ناتج عن الحاسوب لحقه سبب يبطله ويعدم أثره[٢].

لذلك لابد لنا من دراسة هذه الشروط وذلك عن طريق تقسيم هذا المبحث إلى ثلاثة فروع ندرس في:

**الفرع الأول: شرط يقينية الدليل الإلكتروني.**

**الفرع الثاني: شرط وجوب مناقشة الدليل الإلكتروني.**

**الفرع الثالث: شرط مشروعية الدليل الإلكتروني.**

---

(١) محمد نافع فالح رشدان العدواني، المرجع السابق، ص١٠٥.

(٢) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٣٧-٧٣٨.

## الفرع الأول
## شرط يقينية الدليل الإلكتروني

يُعرَّف اليقين في النظم الإجرائية بأنه: " عبارة عن حالة ذهنية أو عقلانية تؤكد وجود الحقيقة، ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة من خلال ما يعرض على القاضي من وقائع الدعوى، وما ينطبع في ذهنه من تصورات واحتمالات ذات درجة عالية من التوكيد"(١).

وإن دراسة شرط يقينية الدليل الإلكتروني، يقتضي منا بيان نطاق هذا الشرط ومدى شموله لإحكام الإدانة والبراءة، وذلك يقتضي أولاً، بحث شرط يقينية الدليل الإلكتروني في حكم الإدانة، وثانياً، بحث شرط يقينية الدليل الإلكتروني في حكم البراءة.

**أولاً: شرط يقينية الدليل الإلكتروني في حكم الإدانة:**

يُعرف دليل الإدانة (Inculpatory Evidence) بأنه: "هو الدليل الذي يؤيد ويثبت فكرة معينة لارتكاب الجريمة محل البحث"(٢).

فلا مجال لدحض أصل البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين(٣).

حيث إن شرط اليقين في أحكام الإدانة شرط عام سواء كانت الأدلة التي يستقى منها هذا اليقين تقليدية أو مستحدثة كالدليل الإلكتروني. واليقين الذي يُعول عليه في هذا الشأن هو ما يتولد لدى القاضي بأن ما وصل إليه هو الحقيقة عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال وقائع الدعوى، وما

---

(١) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٣٨-٧٣٩.

(٢) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص ١٢٥.

(٣) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٤٠.

يرتبه ذلك في ذهنه من تصورات ذات درجة عالية من التأكيد إلى أن يصل إلى اليقين، الذي تكون ثمرته الاقتناع[١].

وتقيد القاضي الجزائي بالأدلة اليقينية يستوجب أن تقترب الأدلة نحو الحقيقة الواقعية، بحيث لا تقبل الشك وأن تبتعد عن الظنون والتخمينات، ويترتب على ذلك أن جميع مخرجات الوسائل الإلكترونية[٢] تخضع لتقدير القاضي الجزائي، ويجب أن يستنتج منها الحقيقة بما يتفق مع اليقين ويبتعد عن الشك والاحتمال[٣].

وهكذا يستطيع القاضي – من خلال ما يعرض عليه من مخرجات إلكترونية، وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها – أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة الإلكترونية إلى شخص معين من عدمه[٤].

وأخذت التشريعات اللاتينية والإنكلوسكسونية بشرط يقينية الدليل الإلكتروني، ففي التشريعات اللاتينية، فإنه يشترط في المخرجات الكمبيوترية أن تكون يقينية حتى يمكن الحكم بالإدانة.

---

(١) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٤٣.

(٢) سواء كانت مخرجات ورقية تنتجها الطابعات أو الراسم، أم كانت مخرجات لا ورقية أو إلكترونية كالأشرطة المغناطيسية والأقراص المغناطيسية والمصغرات الفيلمية وغيرها من الاشكال الإلكترونية غير التقليدية للتكنولوجيا التي تتوافر عن طريق الوصول المباشر، أم كانت الأخيرة مجرد عرض لهذه المخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به أو على الطرفيات. أ. د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٤١-٧٤٢.

(٣) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٤٢.

(٤) د. علي حسن الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، المرجع السابق.

د. محمد أحمد المنشاوي، المرجع السابق، ص٥٤٣.

لكـن المشـرع السـوري لـم يـنظم شـرط يقينيـة الـدليل الإلكترونـي فـي قـانون أصـول المحاكمات الجزائية السوري بل نظمه في قانون مكافحة الجريمة الإلكترونية وتنظيم التواصل عبر الشبكة لعام ٢٠١٢م عندما نص في الفقرة (أ) من المادة (٢٥) من هذا القانون، على ما يلي:

"أ – يعود للمحكمة تقدير قيمة الدليل الرقمي، شريطة تحقُّق ما يلي:

١) أن تكون الأجهزة الحاسوبية أو المنظومات المعلوماتية المستمدّ منها هذا الدليل تعمل على نحو سليم".

وأيضاً في التشريعات الإنكلوسكسونية، ففي قانون البوليس والإثبات الجنائي في المملكة المتحدة، فإنه يشترط حتى تتحقق يقينية المخرجات الكمبيوترية أن تكون البيانات دقيقة وناتجة عن حاسوب يعمل بصورة سليمة[١]، وفي كندا فإن الرأي السائد هو اعتبار مخرجات الحاسوب من أفضل الأدلة ولذلك فإنها تحقق اليقين المنشود في الأحكام الجزائية.

وأيضاً في أمريكا نصت قوانين بعض الولايات، كما هو الحال في كاليفورنيا وإيوا على أن النسخ المستخرجة من البيانات التي يحويها الحاسوب تُعد أفضل الأدلة المتاحة لإثبات هذه الجرائم، وبالتالي يتحقق شرط يقينية المخرجات الكمبيوترية، بيد أن هذا لا يمنع القضاء الأمريكي من استبعاد هذه المخرجات إذا كانت ناتجة عن حاسوب لا يؤدي وظائفه بصورة سليمة، أو كان القائم عليه لا يتوافر فيه الثقة والطمأنينة[٢].

---

(١) وإن كان بعضاً من الفقه جرى على عدم ضرورة هذه الشروط حتى يتحقق اليقين، وذلك اسوة بما قررته اللجنة القانونية الاسكتلندية أن الشرائط المنصوص عليها في القسم (٦٩) بخصوص الدليل الناتج عن الحاسوب غير ضرورية. د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص ٧٤٤-٧٤٥.

(٢) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٤٤-٧٤٥.

ويمكن للقاضي الجزائي أن يصل إلى يقينية المخرجات الكمبيوترية المتقدم ذكرها عن طريق نوعين من المعرفة: أولهما المعرفة الحسية التي تدركها الحواس، من خلال معاينة هذه المخرجات وتفحصها، وثانيهما المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل والاستنتاج، من خلال الربط بين هذه المخرجات والملابسات التي أحاطت بها، فإذا لم ينته القاضي إلى الجزم بنسبة الفعل أو الجريمة الإلكترونية إلى المتهم المعلوماتي، كان من المتعين عليه أن يقضي بالبراءة، فالشك يجب أن يستفيد منه المتهم المعلوماتي(١).

لكن هذا الأمر على إطلاقه محل نظر، حيث إنه إذا توافر للبعض من القضاة هذا الحس اليقيني بما تكشفه حواسه الوجدانية، فالبعض الآخر ليست لديه هذه الملكة، الأمر الذي يصبح معه التشكيك في وجهة نظر القاضي الجزائي في يقينية الدليل الإلكتروني محل اعتبار(٢).

**ثانياً: شرط يقينية الدليل الإلكتروني في حكم البراءة:**

يُعرف دليل البراءة (Exculpatory Evidence ) بأنه: "هو الدليل الذي يناقض فكرة معينة لارتكاب الجريمة محل البحث"(٣).

إن عدم قدرة أدلة الإدانة على إحداث القطع واليقين يترتب عليه استمرار حالة البراءة التي يكفي لتأكيد وجودها حينئذ مجرد الشك في ثبوت تلك الإدانة وذلك إتباع لمبدأ البراءة المسلم بوجوده بدايةً، فإذا كان الحكم بالإدانة يستوجب اليقين بوجود هذه الإدانة وذلك لأنها إثبات على خلاف الأصل الذي لا يمكن إثبات عكسه إلا بمقتضى حالة اليقين تتساوى في نتائجها مع تلك المسلم بوجودها نتيجة لمبدأ افتراض البراءة، أما الحكم بالبراءة فهو مجرد تأكيد لمبدأ البراءة الذي

---

(١) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٤٢.

(٢) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٤٤.

(٣) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص ١٢٥.

يتمتع به الفرد منذ ميلاده[١]، ولذلك فإنه يكفي أن يتشكك القاضي في صحة إسناد التهمة إلى المتهم حتى يقضي بالبراءة، وذلك إعمالاً لمبدأ تفسير الشك لصالح المتهم[٢]، وهذا ما أكدته المادة (٣٠٤) من قانون الإجراءات الجنائية المصري، حيث نصت على أنه:

" إذا كانت الواقعة غير ثابتة تحكم المحكمة ببراءة المتهم".

غير أن محكمة النقض المصرية وضعت شرطاً لذلك، يتمثل في أنه يجب أن يتضمن الحكم ما يفيد أن المحكمة قد فحصت الدعوى وأحاطت بأدلتها عن بصر وبصيرة، ووازنت بين أدلة الثبوت وأدلة النفي، ولم تقتنع على وجه اليقين بإدانة المتهم[٣]، أو اقتنعت يقينياً ببراءته، لأنه إذا كان من حق محكمة الموضوع أن تستبعد أي دليل لا ترتاح إليه، فإنه لا يجوز لها بتر التحقيق وعدم استكمال عناصره مادام منتجاً ومؤثراً في الدعوى[٤].

**ونحن نرى أن ذلك يطبق على الدليل الإلكتروني أيضاً فإذا لم يصل القاضي الجزائي إلى مرحلة الاقتناع اليقيني بالدليل الإلكتروني المعروض أمامه بإدانة المتهم فإنه لا يستطيع أن يدحض براءته ويحكم بإدانته، وذلك لأن قرينة البراءة لا تدحض إلا باقتناع القاضي اليقيني.**

---

(١) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٤٠-٧٤١.

(٢) د. محمد أحمد المنشاوي، المرجع السابق،ص٥٤٧.

(٣) نقض١٠، يناير سنة ١٩٧٢، مجموعة أحكام النقض، س٢٣، رقم ١٧، ص٦٠. وأيضاً نقض ١٨، ديسمبر ١٩٩٣، مجموعة أحكام النقض، س٤٤، رقم ١٧٢، ص١١٠٣. د. محمد أحمد المنشاوي، المرجع السابق، ص٥٤٧.

(٤) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٤٧.

## الفرع الثاني

## شرط وجوب مناقشة الدليل الإلكتروني

يعني مبدأ وجوب مناقشة الدليل الجزائي بصفة عامة أن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى(١)، ولا يختلف الأمر بالنسبة للمخرجات الكمبيوترية بوصفها أدلة إثبات إذ ينبغي أن تطرح في الجلسة وأن يتم مناقشتها في مواجهة الأطراف(٢).

وهذا يعني أن المخرجات الكمبيوترية سواء كانت مطبوعات أم بيانات معروضة على شاشة الحاسوب أم كانت بيانات مدرجة في حاملات البيانات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية – كل ذلك سيكون محلاً للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة(٣).

فإذا كان القاضي الجزائي على اقتناع فإنه يجب عليه أن يعيد تحقيق جميع الأدلة القائمة في الأوراق، لكي يتمكن من تكوين اقتناع يقربه نحو الحقيقة الواقعية التي يصبو إليها كل قاضٍ عادل ومجتهد، ويترتب على هذا المبدأ أن القاضي لا يمكنه أن يحكم في الجرائم الإلكترونية استناداً إلى علم شخصي له أو استناداً إلى رأي الغير، إلا إذا كان الغير من الخبراء، وقد ارتاح ضميره إلى التقرير المحرر منه، فقرر الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة

---

(١) انظر: قرار محكمة النقض المصرية رقم ١٧٩، الصادر في ١٩٨٦/١١/٢٠، مجموعة المبادئ القانونية، ص ٩٤٣. مشار إليه لدى: د. محمد أحمد المنشاوي، المرجع السابق، ص٥٤٨.

(٢) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٤٧.

(٣) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٤٨.

عليه، بحيث أن الاقتناع الذي يكون قد أصدر حكمه بناء عليه يكون متولداً عن عقيدته هو وليس من تقرير الخبير[١].

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، بل بصفة مباشرة أمام القاضي، وهذه الأحكام تنطبق على جميع الأدلة المتولدة عن الحاسبات، وأيضاً بالنسبة لشهود الجرائم الإلكترونية الذين يكون قد سبق أن سمعت أقوالهم في التحقيق الابتدائي، فإنه يجب أن يعيدوا أقوالهم مرة أخرى من جديد أمام المحكمة، كذلك فإن خبراء الأنظمة المعلوماتية على اختلاف تخصصاتهم، ينبغي أن يمثلوا أمام المحاكم لمناقشتهم، أو مناقشة تقاريرهم التي خلصوا إليها لإظهار الحقيقة ولكشف الحق[٢]، وأخيراً فإن متحصلات الجريمة الإلكترونية التي يتم ضبطها يجب أن تعرض على القاضي شخصياً بكافة مفرداتها وعناصرها، وذلك لأن حيدة القاضي توجب عليه أن لا يقيم قضاءه إلا على ما يطرح أمامه وكان موضوع للفحص والتحقيق والمناقشة[٣].

ومن القواعد العامة المستقرة في القانون الجزائي عدم قبول البينة السماعية أمام المحاكم الجزائية، إلا في حالات استثنائية حصرها القانون بشروط مشددة[٤]، ويُعزى عدم قبول البينة السماعية إلى استحالة استجواب الشاهد الأصلي ومناقشته بوساطة المحكمة والدفاع، ولاستثناءات البينة السماعية علاقة بمناقشة حجية الأدلة الجزائية الإلكترونية، فعلى سبيل المثال، كما ذكرنا سابقاً في هذا البحث أنه تضمنت القواعد الفيدرالية الأمريكية نصاً يُعد السجلات والبيانات المنظمة بدقة

---

(١) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٤٨.

(٢) معمر علي إبراهيم محمد، المرجع السابق، ص١٦٣.

(٣) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٤٨.

(٤) وهناك استثناءات على هذه القاعدة نصت عليها بعض التشريعات، كالولايات المتحدة الأمريكية، وانكلترا، وكندا، وأستراليا.

بينة مقبولة أمام المحاكم الجزائية استثناء للبينة السماعية، وبناءً على تلك القواعد تُعد التقارير والمعلومات والبيانات المحفوظة في أي شكل، وكذلك الوقائع والأحداث والآراء ونتائج التحاليل المنقولة بوساطة أصحاب المعرفة والخبرة في نطاق الأنشطة والممارسات المنظمة بيّنة مقبولة أمام المحاكم الجزائية، لكونها بيانات أكثر دقة ومحفوظة بأسلوب علمي يختلف عن غيرها من الأدلة السماعية، والأدلة الجزائية الإلكترونية من هذا القبيل، لكونها معدة بعمليات حسابية دقيقة لا يتطرق إليها الشك ويتم حفظها آلياً بأسلوب علمي(١).

ويترتب على مناقشة الأدلة الإلكترونية نتيجتان:

**النتيجة الأولى:** عدم جواز أن يقضي القاضي في الجرائم الإلكترونية بناءً على معلوماته الشخصية.

**والنتيجة الثانية:** ضرورة التأهيل التقني والفني للقضاء لمواكبة المناقشة العلمية للأدلة الإلكترونية بشكل ينسجم مع التقارير التي تم تقديمها في المؤتمرات الخاصة بجرائم الحاسوب والإنترنت(٢).

وقد حرصت التشريعات الإجرائية في التشريعات اللاتينية على أن تنص على هذه القاعدة المهمة، ومن ذلك على سبيل المثال لا الحصر، الفقرة الثانية من المادة (٤٢٧) من قانون الإجراءات الجنائية الفرنسي التي تنص على أنه: " لا يجوز للقاضي أن يؤسس حكمه إلا على أدلة طرحت عليه أثناء المحاكمة ونوقشت أمامه في مواجهة الأطراف"(٣).

وكذلك نص المشرع السوري في قانون أصول المحاكمات الجزائية السوري

---

(١) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٤٩ – ٥٥٠.

(٢) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٥٠.

(3) Article 427 alinéa 2 :
''Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui''.

موقع التشريعات الفرنسية:

https://www.legifrance.gouv.fr. تاريخ الدخول في ٢٠١٩/٣/١٠م.

في المادة (١٧٦) والتي جاء فيها: "لا يجوز للقاضي أن يعتمد إلا البينات التي قدمت اثناء المحاكمة وتناقش فيها الخصوم بصورة علنية".

**إلا أن المشرع السوري لم ينص بشكل صريح على شرط مناقشة الدليل الإلكتروني وهذه ثغرة قانونية ينبغي عليه معالجتها.**

كذلك فإن قاعدة وجوب مناقشة الدليل الجزائي من القواعد الأساسية في التشريعات الإنكلوسكسونية، حيث إن كل عناصر الإثبات لا بد أن تكون موضوعاً للمناقشة والحضورية بين الأطراف عن طريق ممثليهم القانونيين بينما يكون القاضي – إلى حد ما– مستمعاً مصغياً لكل ما يمكن أن يقال في الجلسة ومن جميع الأطراف(١).

**ونحن نرى أن القاضي الجزائي ليس له أن يؤخذ بالدليل الإلكتروني سواء أكان دليل إدانة أو براءة إذا لم يكن قد عرض أثناء المرافعات ولم يناقشه الأطراف في الدعوى، ولا بد من أن يمثل الشهود المعلوماتيين ويعيدوا أقوالهم مرة ثانية أمام المحكمة، وكذلك ضرورة أن يمثل خبراء الأنظمة المعلوماتية – على اختلاف تخصصاتهم – أمام المحاكم لمناقشتهم أو مناقشة تقاريرهم التي خلصوا إليها لإظهار الحقيقة.**

## الفرع الثالث

## شرط مشروعية الدليل الإلكتروني

يعني مبدأ مشروعية الدليل الجزائي بما يتضمنه من مخرجات كمبيوترية ضرورة اتفاق الإجراء مع القواع القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر، أي أن قاعدة مشروعية الدليل الجزائي لا تقتصر فقط على مجرد المطابقة مع القاعدة القانونية التي ينص عليها المشرع، بل يجب أيضاً مراعاة

---

(١) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٤٨-٧٤٩.

إعلانات حقوق الإنسان والمواثيق والاتفاقيات الدولية، وقواعد النظام العام وحسن الآداب السائدة في المجتمع، بالإضافة إلى المبادئ التي استقرت عليها محكمة النقض(١).

فمشروعية الدليل تتطلب صدقه في مضمونه، وإن يكون هذا المضمون قد تم الحصول عليه بطرق مشروعة، تدل على الأمانة والنزاهة من حيث طرق الحصول عليه، ولا يعني ذلك حصر حالات المشروعية في نطاق مخالفة النصوص المقررة لضمانات الحرية الفردية، إذ يوصف الدليل بعدم المشروعية متى كانت طريقة الحصول عليه تتعارض مع القواعد العامة للأصول الجزائية والمبادئ القانونية العامة التي توجب احترام قيم العدالة وأخلاقياتها(٢).

فمن المقرر أن الأدلة في أي جريمة لا بد أن تكون مبنية على أسس مشروعة حصل عليها وفق قواعد الأخلاق والنزاهة واحترام القانون(٣).

ومعيار نزاهة مصادر الأدلة الجزائية أي مشروعيتها هو في احترام الضمانات التي أتى بها القانون لاحترام حرية المتهم بوصفه بريئاً إلى أن تثبت إدانته بحكم بات، فلا يمكن في نفس الدعوى أن يكون الإجراء مشروعاً وغير مشروع في آن واحد، فعدم المشروعية المبني على تجاهل الضمانات لا يمكن أن تصاحبه مشروعية الدليل المنبثق عنها(٤).

ومن الضروري التمييز بين نوعين من الأدلة، دليل الإدانة من ناحية، ودليل البراءة من ناحية أخرى، وبالتالي لابد لنا من التمييز بالنسبة لشرط مشروعية الدليل الإلكتروني بين أولاً شرط مشروعية الدليل الإلكتروني بالنسبة لدليل الإدانة، وثانياً شرط مشروعية الدليل الإلكتروني بالنسبة لدليل البراءة كما يلي:

---

(١) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٥١.

(٢) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٥٣.

(٣) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٥٢.

(٤) د. أحمد فتحي سرور، الوسيط في قانون الإجراءت الجنائية، د.ط، دار النهضة العربية، القاهرة، مصر، ١٩٨٥م، ص٣٩٦.

**أولاً: شرط مشروعية الدليل الإلكتروني بالنسبة لدليل الإدانة:**

فيما يتعلق بشرط مشروعية الدليل الإلكتروني بالنسبة لدليل الإدانة هنالك قاعدة واستثناء:

**أ- القاعدة:**

إن اقتناع القاضي القائم على الدليل الصحيح هو تطبيق للمبادئ العامة التي توجب على المحاكم عدم الاعتراف إلا بالإجراءات المشروعة، وإنه لا يكفي لسلامة الحكم أن يكون الدليل صادقاً متى كان وليد إجراء غير مشروع، لأن الإجراء غير المشروع يبطل الدليل المستمد منه، ويبطل كذلك الحكم الذي يبنى عليه حتى ولو كان الدليل في ذاته صادقاً[١].

فانطلاقاً من قاعدة أن الأصل في الإنسان البراءة، فإن المتهم من اللزوم أن يعامل على أساس أنه بريء في مختلف مراحل الدعوى العامة، إلى غاية صدور الحكم البات في حقه، مما يقتضي أن تكون الأدلة التي يؤسس عليها حكم الإدانة مشروعة، وبالتالي فإن أي دليل يتم الحصول عليه بطريقة غير مشروعة لا تكون له قيمة في الإثبات، باعتبار أنه لو تم قبول الأدلة التي تستمد من إجراءات باطلة فإن الضمانات التي كفلها القانون لحماية حقوق الأفراد تصبح بلا قيمة، وكذلك تصبح القواعد التي سنها المشرع بلا أهمية متى أصبح في الإمكان إهدارها، وعدم الالتزام بها، فمشروعية الإثبات الجزائي تستلزم عدم قبول أي دليل كان الحصول عليه قد تم بطريق غير مشروع، فمتى تم الحصول على هذا الدليل بإجراءات تخرج عن إطار الشرعية فإن هذه الإجراءات يطالها البطلان، وبالتالي فإنه إن تم بطلان إجراء ما يجب استبعاد ما ينتج عنه من أدلة، وهذا عملاً بقاعدة ما بني على باطل فهو باطل[٢].

---

(١) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٥٢.

(٢) هلال آمنة، المرجع السابق، ص٩٨.

فالأدلة التي يؤسس عليها حكم الإدانة يجب أن تكون مشروعة، سواء كانت هذه الأدلة أدلة تقليدية أو ناتجة عن الوسائل الإلكترونية بصفة عامة[١]، ولا يحول ذلك أن تكون الأدلة صارخة وواضحة على إدانة المتهم طالما كانت هذه الأدلة مشبوهة ولا يتسم مصدرها بالنزاهة واحترام القانون[٢].

وبالتالي فإن إجراءات جميع الأدلة المتحصلة من الوسائل الإلكترونية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها لا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجزائية[٣].

**ولم ينص المشرع السوري في قانون أصول المحاكمات الجزائية السوري وقانون مكافحة الجريمة الإلكترونية على ضرورة أن تكون الأدلة مشروعة سواء بالنسبة للأدلة التقليدية بشكل عام أم بالنسبة للدليل الإلكتروني بشكل خاص وهذه ثغرة قانونية ينبغي عليه معالجتها بأسرع وقت ممكن.**

**ب-الاستثناء:**

رأينا أنه لابد من خضوع الدليل الإلكتروني لمبدأ مشروعية الدليل الجزائي وألا ترتب عليه البطلان لكن قد يؤخذ الدليل الإلكتروني بإجراءات غير مشروعة ويؤكد الإدانة بطريقة لا يرتقي إليها أدنى شك ولا سيما إذا كان المجرم من ذوي السوابق العدلية. **فهل ندع المجرم يفلت من العقاب بحجة أن الإجراءات غير مشروعة أو باطلة؟**

---

(١) هلال آمنة، المرجع السابق، ص٩٨-٩٩.

(1) Bouzet ; La loyauté dans la recherche des preuves, (Problèmes contemporains de procédures pénale, en hommage à Hugueney, Paris, France, 1964, PP .155.

(٣) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٥٢.

وحددت محكمة النقض البلجيكية[١] ماهية الدليل غير المشروع بأنه: "ليس فقط الدليل المتحصل عليه بفعل محظور قانوناً بنص صريح وإنما كذلك بفعل لا يتسق مع القواعد الجوهرية للإجراءات الجنائية ولا مع المبادئ العامة للقانون".

ولقد أقر النظام القانوني البريطاني تشريعات تتيح الرقابة والملاحقة والقبض والتفتيش دون الخضوع للمبادئ والأحكام القانونية، التي استقرت بموجب الاتفاقية الأوربية لحقوق الإنسان ومبادئ وتوجيهات الاتحاد الأوربي[٢].

كما أصدر الكونجرس الأمريكي تشريعاً يرفع الكثير من القيود على عمليات التنصت والرقابة الهاتفية ومراقبة الإنترنت والبريد الإلكتروني، خاصة بعد ما أثاره المحققون من أن الإنترنت والبريد الإلكتروني، كانا الواسطة التي أتاحت للجهة التي نفذت الهجوم على مركز التجارة العالمي والبنتاغون، ويمثل السبب الرئيس الأول لقبول هذا التشريع رغم تعارضه مع حقوق وحريات الأفراد، أنه تشريع موجه لغير المواطنين الأمريكيين، مما يجعل الكثير من الأمريكيين مقتنعين أنه لا يطالهم من أحكامه ضرر مع أن الواقع العملي لن يكون كذلك[٣].

**ونحن نرى أن التمسك بمشروعية الدليل الإلكتروني بالنسبة لدليل الإدانة على إطلاقه لا يضمن أمن المجتمع واستقراره وبهذا يكون مبدأ المشروعية قاصراً ولا يكون فعالاً في حماية المجتمع أمام هذا الدليل العلمي الحديث، وبالتالي نقترح قبول الدليل الإلكتروني غير المشروع في أحكام الإدانة في الجرائم التي تهدد الدولة في كيانها ووجودها كالجرائم الإرهابية وجرائم أمن الدولة الداخلي والخارجي حفاظاً على المصلحة العامة.**

---

(١) Cour de cassation (Belgique), 13 Mai 1986, R.D.P.C.1986, J, PP. 905.
و د. جميل عبد الباقي الصغير، المرجع السابق، ص١١٠.

(٢) خالد عياد الحلبي، المرجع السابق، ص ١٦٦.

(٣) خالد عياد الحلبي، المرجع السابق، ص ١٦٦-١٦٧.

**ثانياً: شرط مشروعية الدليل الإلكتروني بالنسبة لدليل البراءة:**

لا بد من الإشارة إلى أنه لا يشترط في دليل البراءة أن يكون ثمرة إجراء مشروع، وذلك لأن الأصل في المتهم البراءة، ولا حاجة للمحكمة في أن تثبت براءته وكل ما تحتاج إليه هو أن تشكك في إدانته(١)، وقد تأكد ذلك في اجتهادات محكمة النقض المصرية(٢).

**ونحن نرى أن ذلك يطبق على الدليل الإلكتروني فيمكن أن يكون هذا الدليل غير مشروع وذلك لتقرير براءة المدعى عليه لأن شرط مشروعية الدليل لا يتطلب في دليل البراءة بل يقتصر على دليل الإدانة نظراً لخطورته فكان لا بد أن يكون هذا الدليل مشروع.**

**وفي هذا المبحث، درسنا حرية القاضي الجزائي في تقدير الدليل الإلكتروني، فدرسنا مفهوم السلطة التقديرية للقاضي الجزائي، كما درسنا ضوابط السلطة التقديرية للقاضي الجزائي في تقدير الدليل الإلكتروني وهذه الضوابط هي بلوغ الاقتناع القضائي درجة اليقين، ومواءمة الاقتناع القضائي لمقتضيات العقل والمنطق، وتقيد القاضي الجزائي بسلامة التقدير والاستدلال.**

**كما درسنا الشروط الواجب توافرها في الدليل الإلكتروني لكي يخضع للسلطة التقديرية للقاضي الجزائي وأهم الشروط الواجب توافرها في الدليل الإلكتروني هي شرط يقينية الدليل الإلكتروني وشرط وجوب مناقشة الدليل الإلكتروني وشرط مشروعية الدليل الإلكتروني حيث ميزنا بين دليل الإدانة ودليل البراءة.**

---

(١) د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، د.ط، دار النهضة العربية، القاهرة، مصر، ١٩٨٥م، ص ٣٩٧.

(٢) نقض مصري، ٢٥ يناير، سنة ١٩٦٥م، مجموعة الأحكام، س١٦، رقم ٢١، ص٨٧. ونقض مصري ٣١ يناير، سنة ١٩٦٧م، مجموعة الأحكام، س١٨، رقم٢٤، ص١٢٨.

# المبحث الثاني

# تقدير القاضي الجزائي للدليل الإلكتروني في أنظمة الإثبات المختلفة

تختلف حرية القاضي الجزائي في تقدير الدليل الإلكتروني باختلاف نظم الإثبات الجزائي، حيث إن نظم الأدلة الجزائية في الإثبات الجزائي تتنوع، بين التي تأخذ بنظام الإثبات الحر في الإثبات الجزائي القائم على حرية القاضي الجزائي في الاقتناع، وأخرى تعتنق نظام الإثبات المقيد.

وسنبين حرية القاضي الجزائي في تقدير هذا الدليل المستحدث في ظل نظام الإثبات الحر، وكذلك في نظام الإثبات المقيد، وأخيراً سنبحث النظام المقترح لتقدير الدليل الإلكتروني، لذلك سنقوم بتقسيم هذا المبحث إلى ثلاثة مطالب ندرس في:

**المطلب الأول: تقدير القاضي الجزائي للدليل الإلكتروني في نظام الإثبات الحر.**

**المطلب الثاني: تقدير القاضي الجزائي للدليل الإلكتروني في نظام الإثبات المقيد.**

**المطلب الثالث: النظام المقترح لتقدير الدليل الإلكتروني.**

## المطلب الأول

## تقدير القاضي الجزائي للدليل الإلكتروني في نظام الإثبات الحر

إن دراسة تقدير الدليل الإلكتروني في نظام الإثبات الحر، تقتضي منا بيان الأسس العامة لتقدير الدليل الإلكتروني في نظام الإثبات الحر، ومن ثم سنعرض موقف بعض التشريعات اللاتينية التي تتبنى هذا النظام من تقدير الدليل الإلكتروني، ولابد لنا من تقسيم هذا المطلب إلى فرعين ندرس في:

**الفرع الأول: الأسس العامة لتقدير الدليل الإلكتروني في نظام الإثبات الحر.**

**الفرع الثاني: موقف بعض التشريعات اللاتينية من تقدير الدليل الإلكتروني.**

## الفرع الأول

## الأسس العامة لتقدير الدليل الإلكتروني في نظام الإثبات الحر

إن بحث تقدير القاضي الجزائي للدليل الإلكتروني في نظام الإثبات الحر، يقتضي أولاً، بيان مفهوم السلطة التقديرية للقاضي الجزائي في نظام الإثبات الحر، وثانياً، مدى حرية القاضي الجزائي في تقدير الدليل الإلكتروني في نظام الإثبات الحر.

**أولاً: مفهوم السلطة التقديرية للقاضي الجزائي في نظام الإثبات الحر:**

يقوم هذا النظام على مبدأ القناعة القضائية، وبمقتضاه يباشر القضاء دور إيجابي في كشف الحقيقة، ويبدو هذا الدور من جانبين هما: الأول، حرية القاضي في أن يستمد قناعته من أي دليل يطمئن إليه، والثاني، حرية القاضي في تقديره للأدلة المطروحة عليه، فمن جهة للقاضي حرية قبول أي دليل، يمكن أن تتولد منه قناعته، فجميع أدلة الإثبات أمام القاضي سواء، ومن جهة أخرى، فإنه يتمتع بالحرية نفسها في تقدير قيمتها، فهو الذي يستقل بتقدير القيمة الحقيقية لكل دليل فليس هناك دليلاً له قوة ذاتية قانونية يلزم بها، ونتيجة لذلك، فإنه يحظر على المشرع، إضفاء قوة معينة لأي دليل من شأنه أن يقيد سلطة القاضي في تكوين قناعته، أو يسبغ على بعضها شكاً أو عدم ثقة كي يستبعدها القاضي من تقديره الحر[١].

لكن لا يعني هذا النظام تحَّكم القاضي، فلا يجوز لهذا الأخير أن يحكم وفقاً لهواه، أو يحتكم في قضائه لمحض عاطفته، وإنما هو ملتزم بأن يتحرى المنطق الدقيق في تفكيره الذي قاده إلى اقتناعه[٢].

---

(١) د. فاضل زيدان محمد، المرجع السابق، ص٥٩-٦٠.

(2) MERLE (R) et VITU (A), Traité de droit criminel, Procédure pénale, 4 ème éd, Cujas, Paris, France, 1989, N 133, p. 169.

ونظام الإثبات الحر يطبق أمام جميع أنواع القضاء الجزائي وسواء في المخالفات أو الجنح أو الجنايات[١].

وهذا النظام يسري على قضاة التحقيق والإحالة أسوة بقضاة الحكم، على أنه في هذه الحالة ينحصر تقدير قضاة التحقيق أو الإحالة في مدى قيمة الأدلة لتقديم المتهم للمحاكمة ويكفي لذلك مجرد ترجيح إدانته[٢].

وهذا يعني أن للقاضي أن يقبل جميع الأدلة التي يقدمها إليه أطراف الدعوى، فلا وجود لأدلة يحظر عليه القانون مقدماً قبولها، وله أن يستبعد أي دليل لا يطمئن إليه فلا وجود لأدلة مفروضة عليه، وله بعد ذلك السلطة التقديرية الكاملة في وزن كل دليل على حدة، وله في النهاية السلطة التقديرية الكاملة – وفق القانون – والتنسيق بين الأدلة التي قدمت إليه واستخلاص نتيجة منطقية من هذه الأدلة مجتمعة ومتساندة، وتتمثل في تقرير البراءة أو الإدانة، وهذا المبدأ يقوم على التقدير الحر المسبب لعناصر الإثبات في الدعوى، فلا يتدخل المشرع إلا من زاوية تنظيم وسائل الحصول على الأدلة وتقديمها وتحقيقها بوساطة القاضي للوقوف على مدى قانونيتها واستنادها إلى إجراءات صحيحة، ويبقى بعد ذلك أمر تقديره وتحديد قوتها الإقناعية للقاضي في حرية تامة، فالبحث عن أن المتهم بريء أو مذنب يعتمد – في حقيقة الأمر – على عاملين أساسيين، هما البحث عن الحقيقة واقتناع القاضي بدليل الإدانة، أو مجرد شكه في البراءة دون أن يكون هناك قيد على حريته في الاقتناع[٣].

---

(1) STEFANI (Gaston), LEVASSEUR (Georges) et BOULOC (Bernard), Procédure pénale, Précis Dalloz, 16ème éd, Paris, France, 1996, N30, P 26.

(٢) د. أحمد فتحي سرور، أصول الإجراءات الجنائية، الطبعة الأولى، دار النهضة العربية، ١٩٦٩، ص ٣٤٣ – ٣٤٤.

(٣) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٣٥ – ٥٣٦.

وهنالك أسباب عديدة تبرر الأخذ بنظام الإثبات الحر والاقتناع القضائي ومنها ظهور الأدلة العلمية وتقدمها، مثل تلك المستمدة من تحليل الحامض النووي (DNA) وتحقيق الشخصية، وهي لا تقبل بطبيعتها إخضاع القاضي لأي قيود بشأنها، بل ينبغي أن يترك الأمر في تقديرها لمحض اقتناعه، خاصة وأنها كثيراً ما تتضارب مع باقي أدلة الدعوى، فضلاً عن احتمال تضارب آراء المختصين في شأنها[١].

ويجب التفرقة بين حرية الإثبات، وحرية القاضي في الاقتناع، حيث يقصد بحرية الإثبات، الطريق الإثباتي المرسوم لكل أطراف الدعوى، بمن فيهم القاضي في اختيار أدلة الإثبات الملائمة للواقعة محل الإثبات، بينما تتعلق حرية القاضي الجزائي في الاقتناع بنطاق سلطة القاضي في تقدير الدليل وتقييمه، بحيث يمثل هذا المبدأ الأساس الذي يسيطر على آخر مرحلة من مراحل تقدير الدليل الجزائي[٢].

ومن ناحية أخرى تجب التفرقة بين حرية القاضي في قبول الأدلة، وحرية القاضي في تقدير الأدلة.

فحرية القاضي الجزائي في قبول الأدلة مسألة قانونية لا مجال لإعمال سلطة القاضي التقديرية فيها، حيث إن المشرع حسم هذه المسألة بتحديده النموذج القانوني للدليل الخاضع لتقدير القاضي، فمتى ما توافرت شروط هذا النموذج طبقاً لمبدأ المشروعية الإجرائية وجب على القاضي إخضاعه لعملية تقديره، أما حرية القاضي الجزائي في تقدير الأدلة فمسألة تتعلق بقيمة الدليل لإثبات الحقيقة، وهي مسألة موضوعية محضة، وللقاضي أن يمارس سلطته التقديرية فيها، بل هي

---

(١) د. جميل عبد الباقي الصغير، المرجع السابق، ص١٣.

(٢) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٣٦ – ٥٣٧.

المجال الطبيعي لهذه السلطة، حيث إنها تتعلق بقيمة الدليل في الإثبات وصولاً للحقيقة[١].

ومن ثم فالحرية التي يتمتع بها القاضي الجزائي في هذا المجال ليست مقررة لكي تتسع سلطته من حيث الإدانة أو البراءة، وإنما هي مقررة له بالنظر إلى صعوبة الحصول على الدليل في المواد الجزائية، فاستنباط الحقيقة من هذا الدليل إنما يتم بمعرفة القاضي وقدرته على الوصول إلى الحقيقة، وما حباه الله من علم ومدى توافر حاسة القضاء لديه، ولذلك نجد أن القاضي الجزائي يتمتع بدور إيجابي في الدعوى الجزائية[٢].

وهذا النظام هو السائد في التشريعات الجزائية المعاصرة، كالتشريع المصري الذي أكد هذا المبدأ في المادة (٣٠٢) من قانون الإجراءات الجنائية المصري، بقولها: "يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته". وكذلك نص قانون أصول المحاكمات الجزائية السوري في المادة (١٧٥) فقرة (١) على أنه: " تقام البينة في الجنايات والجنح والمخالفات بجميع طرق الإثبات، ويحكم القاضي حسب قناعته الشخصية".

ونستنتج من النص السابق أنه للقاضي الجزائي حرية مطلقة في الكشف عن الحقيقة واستثباتها و ويحق له اللجوء إلى جميع وسائل الإثبات من بينات خطية وشخصية وقرائن واعترافات وكشوف وخبرة ومعاينات وغيرها، بشرط واحد هو الحصول عليها وفقاً للأحكام المقررة في القانون.

وأيضاً المشرع اليمني في المادة (٣٦٧) إجراءات بقولها: "يحكم القاضي في الدعوى بمقتضى العقيدة التي تكونت لديه بكامل حريته". وكذلك المشرع الأردني في المادة (٢/١٤٧) من قانون أصول المحاكمات الجزائية بقولها: "تقام البينة في الجنايات والجنح والمخالفات بجميع طرق الإثبات ويحكم القاضي حسب قناعته

---

(١) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٣٧.

(٢) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٣٧.

الشخصية"، وكذلك المادة (١/٢٧٣) من قانون الإجراءات الفلسطيني الصادر برقم ٣ لسنة ٢٠٠١م بقولها: "تحكم المحكمة في الدعوى حسب قناعتها التي تكونت لديها بكامل حريتها، ولا يجوز لها أن تبني حكمها على أي دليل لم يطرح أمامها في الجلسة أو تم التوصل إليه بطريق غير مشروع"، وكذلك المشرع الليبي في المادة (٢٧٥) إجراءات الصادر في ١٩٥٣/١١/٢٨م، وكذلك المشرع العراقي في المادة (١/٢١٣) من قانون أصول المحاكمات الجزائية العراقي الصادر برقم (١٢٣) لسنة ١٩٧١م، وكذلك التشريع الجزائري في المادة (١٥٠) إجراءات الصادر في ١٩٦٦/٦/٨م.

وكذلك المشرع الفرنسي في المادة (٤٢٧) إجراءات، وكذلك الحال بالنسبة إلى كل من ألمانيا وتركيا ولوكسمبورج واليونان والبرازيل.

## ثانياً: مدى حرية القاضي الجزائي في تقدير الدليل الإلكتروني في نظام الإثبات الحر:

وفقاً لهذا النظام في الإثبات، فإن القاضي يملك سلطة واسعة في تقييم الدليل من حيث قيمته الإثباتية، فللقاضي قبول الدليل ورفضه وهو يعتمد في ذلك على مدى اقتناعه الشخصي بذلك الدليل[١].

**والسؤال الذي يطرح نفسه هو: هل يمكن للقاضي الجزائي وفقاً لهذا النظام أن يُعمل سلطته التقديرية لقبول هذا الدليل أو رفضه بما يمكنه من استبعاد الدليل الإلكتروني لعدم الاقتناع به أو للشك في مصداقيته؟**

إن سلطة القاضي الجزائي في تقدير الدليل لا يمكن أن تتوسع في شأنها بحيث يقال إن هذه السلطة تمتد لتشمل الأدلة العلمية، فالقاضي بثقافته القانونية لا يمكنه إدراك الحقائق المتعلقة بأصالة الدليل الإلكتروني، فضلاً عن ذلك فإن هذا الدليل يتمتع من حيث قوته الإثباتية بقيمة إثباتية قد تصل إلى حد اليقين، فهذا هو

---

(١) خالد عياد الحلبي، المرجع السابق، ص٢٤٦.

شأن الأدلة العلمية عموماً، فالدليل الإلكتروني من حيث إثباته على الواقع تتوافر فيه شروط اليقين، مما لا يمكن معه القبول بممارسة القاضي لسلطته في التأكد من ثبوت تلك الوقائع التي يعبر عنها ذلك الدليل[١]. ولكن هذا لا يناقض من أن الدليل الإلكتروني هو موضع شك من حيث سلامته من العبث من ناحية وصحة الإجراءات المتبعة في الحصول عليه من ناحية أخرى، حيث يشكك في سلامة الدليل الإلكتروني من ناحيتين:

**الأولى:** الدليل الإلكتروني من الممكن خضوعه للعبث للخروج به على نحو يخالف الحقيقة، ومن ثم فقد يقدم هذا الدليل معبراً عن واقعة معينة صنع أساساً لأجل التعبير عنها خلافاً للحقيقة، وذلك دون أن يكون في استطاعة الشخص غير المتخصص إدراك ذلك العبث، على نحو يمكن معه القول إن ذلك قد أصبح هو الشأن في النظر لسائر الأدلة الإلكترونية التي قد تقدم للقضاء، فالتقنية الحديثة تمكن من العبث بالدليل الإلكتروني بسهولة ويسر بحيث يظهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة[٢].

**الثانية:** إن كانت نسبة الخطأ الفني في الحصول على الدليل الإلكتروني نادرة للغاية، إلا أنها تظل ممكنة، ويرجع الخطأ في الحصول على الدليل الإلكتروني لسببين:

١ – الخطأ في استخدام الأداة المناسبة في الحصول على الدليل الإلكتروني، ويرجع ذلك للخلل في الشفرة المستخدمة أو بسبب استخدام مواصفات خاطئة.

٢ – الخطأ في استخلاص الدليل، ويرجع ذلك إلى اتخاذ قرارات لاستخدام الأداة تقل نسبة صوابها عن ١٠% ويحدث هذا غالباً بسبب وسائل

---

(١) خالد عياد الحلبي، المرجع السابق، ص ٢٤٧.

(٢) خالد عياد الحلبي، المرجع السابق، ص ٢٤٧.

اختزال البيانات أو بسبب معالجة البيانات بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها[١].

ومن خلال ذلك فإن الشك في الدليل الإلكتروني لا يتعلق بمضمونه كدليل، وإنما بعوامل مستقلة عنه، ولكنها تؤثر في حجيته[٢].

إذاً يمكننا أن نميز بالنسبة لسلطة القاضي التقديرية في نظام الإثبات الحر بين أمرين:

- القيمة العلمية القاطعة للدليل الإلكتروني.
- والظروف والملابسات التي وجد فيها الدليل الإلكتروني.

**الأمر الأول: القيمة العلمية القاطعة للدليل الإلكتروني:**

فسلطة القاضي التقديرية للدليل لا تتناول الدليل العلمي، ذلك أن قيمة الدليل تقوم على أسس وأصول وحقائق علمية دقيقة تتميز بالثبات والاستقرار والثقة في مصادرها العلمية، الأمر الذي يصعب معه بل قد يستحيل على القاضي أن يتناولها بالفحص والتقدير[٣].

**الأمر الثاني: الظروف والملابسات التي وجد فيها الدليل الإلكتروني:**

إن الظروف التي وجد فيها الدليل تدخل بطبيعتها في نطاق التقدير الذاتي للقاضي الجزائي، - ومن ثم فللقاضي الجزائي أن يطرح الدليل المستخرج من الحاسوب عندما يجد أن وجوده لا يتفق منطقياً مع ظروف الواقعة على الرغم من اقتناعه بقطعيته - إذا تبين له أنه لا يتفق مع ظروف الواقعة وملابساتها، وعلى ذلك فالقاضي ينظر إليه على ضوء الظروف والملابسات المحيطة به[٤].

---

(١) أ. طارق محمد الجملي، المرجع السابق، ص ٦٧ - ٦٨.

(٢) خالد عياد الحلبي، المرجع السابق، ص ٢٤٨.

(٣) د. محمد طارق الخن، المرجع السابق، ص١٢٢ - ١٢٣.

(٤) د. جميل عبد الباقي الصغير، المرجع السابق، ص٢٣.

وبالتالي فإن سلطة تقدير إنفاذ وتطبيق القانون في نظام الإثبات الحر لا تتناول القيمة العلمية القاطعة للدليل الإلكتروني باعتبار علميته وموضوعيته وحياده وكفاءته، لكن يمكنها أن تناقش الظروف والملابسات التي وجد فيها الدليل الإلكتروني[١].

وينتج عن ذلك أنه في هذا النظام والدول التي تأخذ به، تخضع الأدلة الإلكترونية لحرية القاضي في الاقتناع الذاتي، بحيث يكون بمقدوره أن يطرح مثل هذه الأدلة – على الرغم من قطعيتها من الناحية العملية – ذلك عندما يجد أن الدليل الإلكتروني لا يتسق منطقياً مع ظروف الواقعة وملابساتها[٢].

**ونرى أن الدليل الإلكتروني في نظام الإثبات الحر يخضع لتقدير القاضي وفقاً لقناعته القضائية كباقي الأدلة حيث أنه لو سلمنا بأن الدليل الإلكتروني يُعد حجة قطعية فما محل الاقتناع الشخصي للقاضي الجزائي وبالتالي فإن نظام الإثبات المقيد سيحل محل الإثبات الحر في هذا المجال ويصبح دليل قانوني يحدد المشرع قيمته الإثباتية مسبقاً،**

**لكن سلطة القاضي التقديرية للدليل الإلكتروني في ظل نظام الإثبات الحر لا تتناول قيمة هذا الدليل العلمي، ذلك أن قيمته تقوم على أسس وأصول وحقائق علمية تتميز بالثبات والاستقرار والثقة في مصادرها العلمية، الأمر الذي يصعب معه، بل قد يستحيل – على القاضي – أن يتناولها بالفحص والتقدير. وذلك بخلاف الظروف والملابسات التي وجد فيها الدليل الإلكتروني، فإنها تدخل بطبيعتها في نطاق التقدير الذاتي للقاضي الجزائي، بحيث يكون في استطاعته أن يطرحه – على الرغم من اقتناعه بقطعيته – إذا تبين له أنه لا يتفق مع ظروف الواقعة وملابساتها.**

---

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٢٦٧ – ٢٦٨.

(٢) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٣٨ – ٥٣٩.

## الفرع الثاني

## موقف بعض التشريعات اللاتينية من تقدير الدليل الإلكتروني

من التشريعات اللاتينية التي سنقوم بدراستها التشريع الفرنسي والمصري والسوري.

**أولاً: موقف التشريع الفرنسي:**

أخذ قانون الإجراءات الجزائية الفرنسي بمبدأ القناعة القضائية حيث نص عليه في المادة (٤٢٧) الفقرة الأولى والتي نصت على: " باستثناء الحالات التي ينص فيها القانون على خلاف ذلك، يجوز إثبات الجرائم بأية وسيلة إثبات، ويقرر القاضي وفقًا لقناعته الخاصة" [١] .

وبالرجوع إلى قانون الإجراءات والعقوبات الفرنسي نجد أن المادة (٣٥٣) الفقرة (١) نصت على تطبيق مبدأ (القناعة القضائية) أمام محكمة الجنايات، والمادة (٥٣٦) نصت على تطبيقه أمام محاكم المخالفات.

أما بالنسبة إلى قناعة القاضي الجزائي، فإن الدليل الإلكتروني يخضع لحرية القاضي في الاقتناع الذاتي، بحيث يمكن أن يطرح مثل هذه الأدلة – رغم قطعيتها من الناحية العلمية – عندما يجد أن الدليل الإلكتروني لا يتسق منطقياً مع ظروف الواقعة وملابساتها[٢].

ولقد أثيرت في فرنسا مشكلة الإثبات لمحاضر المخالفات التي تتم عن طريق جهاز السينموتر، وانتهى القضاء هناك إلى عدم اعتبار محاضر المخالفات المحررة بإثبات المخالفة حجة بذاتها في الإثبات، وإنما ذهب كل من الفقه والقضاء

---

(1) Article 427 alinéa 1:
"Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction. ".

موقع التشريعات الفرنسية:

https://www.legifrance.gouv.fr تاريخ الدخول في ٢٠١٩/٤/٢٢م.

(٢) د. محمد طارق الخن، المرجع السابق، ص١٢١.

إلى أن المحضر لا تكون له قوة إثباتية إلا إذا أثبت فيه محرره وقائع تدخل في اختصاصه، وأن يكون قد شاهدها أو سمعها أو تحقق منها بنفسه[١].

**ثانياً: التشريع المصري:**

أخذ المشرع المصري صراحة بمبدأ القناعة القضائية في قانون الإجراءات الجنائية المصري وذلك في المادة (٣٠٢) من قانون الإجراءات المصري رقم ١٥٠ لسنة ١٩٥٠م، المعدل بالقانون رقم ١٤٥ لسنة ٢٠٠٦م، والتي نصت على أن: "يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته". كما أقرت محكمة النقض المصرية[٢] مبدأ حرية القاضي الجزائي في قبول الأدلة عملاً بمبدأ حرية الإثبات، فأعلنت أن القانون الجزائي "قد فتح – فيما عدا ما استلزمه من وسائل خاصة في الإثبات – بابه أمام القاضي الجنائي على مصرعيه يختار من كل ما يراه موصلاً إلى الكشف عن الحقيقة".

**نستنتج من ذلك أن الدليل الإلكتروني في التشريع المصري يخضع للسلطة التقديرية للقاضي الجزائي شأنه شأن باقي أدلة الإثبات الجزائية، وللقاضي أن يحكم في الدعوى بناء على اقتناعه الذي تكون لديه.**

**ثالثاً: موقف التشريع السوري:**

المبدأ العام هو أن القاضي الجزائي السوري يستمد قناعته من أي دليل يطمئن إليه من الأدلة التي تقدم في الدعوى دون التقيد بدليل معين، ما لم ينص القانون على غير ذلك؛ فلا يوجد أدلة يحظر القانون عليه قبولها. فالقانون أمدّ القاضي الجزائي بسلطة واسعة وحرية كاملة في مجال الإثبات، فله أن يأخذ من الأدلة ما تطمئن له عقيدته، ويطرح ما لا يرتاح إليه. وهذا

---

(١) د. محمد أحمد المنشاوي، المرجع السابق، ص٥٢٥.

(٢) نقض ٢٠ يناير سنة ١٩٦٩، مجموعة أحكام محكمة النقض، س٢٠، رقم ٣٥، ص١٦٤. كذلك د. جميل عبد الباقي الصغير، المرجع السابق، ص١٣.

ما نصت عليه الفقرة الأولى من المادة (١٧٥) من قانون أصول المحاكمات الجزائية السوري بقولها: " تقام البينة في الجنايات والجنح والمخالفات بجميع طرق الإثبات، ويحكم القاضي حسب قناعته الشخصية".

وبالنسبة للدليل الإلكتروني، فقد نصت المادة (٢٥) من قانون مكافحة الجريمة المعلوماتية السوري الصادر بالمرسوم التشريعي رقم (١٧) لعام ٢٠١٢م، على ما يلي:

((أ – يعود للمحكمة تقدير قيمة الدليل الرقمي، شريطة تحقُّق ما يلي:

١) أن تكون الأجهزة الحاسوبية أو المنظومات المعلوماتية المستمدّ منها هذا الدليل تعمل على نحو سليم.

٢) ألاّ يطرأ على الدليل المقدَّم إلى المحكمة أي تغيير خلال مدة حفظه.

ب – يعدّ الدليل الرقمي المقدَّم إلى المحكمة مستجمعاً للشرطين الواردين في الفقرة (أ) من هذه المادة، ما لم يثبت العكس)).

فالدليل الإلكتروني يندرج تحت طائفة **القرائن القضائية** إذا تم الحصول عليه **بطريقة مشروعة**، ويمكن للقاضي الجزائي الأخذ به سواء في إطار الإدانة أم البراءة، **إذا توافرت في هذا الدليل الشرطين التاليين:**

١ – **السلامة:** أي أن تكون الأجهزة الحاسوبية أو المنظومات المعلوماتية المستمدّ منها هذا الدليل تعمل على نحو سليم، بحيث لا يتطرق الشك في دقته.

٢ – **المطابقة:** ألا يطرأ على هذا الدليل أي تغيير خلال فترة حفظه، أي أن يكون الدليل الرقمي المقدم إلى المحكمة هو نفس الدليل الذي تم جمعه وحفظه.

وقد وضع المشرع **قرينة قانونية بسيطة** في الفقرة (ب) من المادة ٢٥، تتضمن أن الدليل الرقمي المقدَّم إلى المحكمة يعدّ مستجمعاً لشرطّي السلامة والمطابقة المشار إليهما ما لم يثبت العكس.

أما بالنسبة إلى **الدفوع** المتعلقة بهذين الشرطّين، فإن هذه الدفوع يجب ألا تنقص من قيمة الدليل الإلكتروني إذا جاءت على شكل تخمين دون أن يوجد دليل يدعمها.

## المطلب الثاني

## تقدير القاضي الجزائي للدليل الإلكتروني في نظام الإثبات المقيد

إن دراسة تقدير الدليل الإلكتروني في نظام الإثبات المقيد، تقتضي منا بيان الأسس العامة لتقدير الدليل الإلكتروني في نظام الإثبات المقيد، ومن ثم سندرس موقف بعض التشريعات الأنكلوسكسونية التي تتبنى نظام الإثبات المقيد من تقدير الدليل الإلكتروني، وبناء على ذلك سنقسم هذا المطلب في فرعين ندرس في:

**الفرع الأول: لأسس العامة لتقدير الدليل الإلكتروني في نظام الإثبات المقيد.**

**الفرع الثاني: موقف بعض التشريعات الأنكلوسكسونية من تقدير الدليل الإلكتروني.**

### الفرع الأول

### الأسس العامة لتقدير الدليل الإلكتروني في نظام الإثبات المقيد

إن بحث تقدير القاضي الجزائي للدليل الإلكتروني في نظام الإثبات المقيد، يقتضي أولاً، بيان مفهوم السلطة التقديرية للقاضي الجزائي في نظام الإثبات المقيد، وثانياً، مدى حرية القاضي الجزائي في تقدير الدليل الإلكتروني في نظام الإثبات المقيد.

**أولاً: مفهوم السلطة التقديرية للقاضي الجزائي في نظام الإثبات المقيد:**

نظام الإثبات المقيد أو المحدد، ويسمى أيضاً بنظام الأدلة القانونية، وفي هذا النظام يقوم المشرع نفسه بتنظيم القناعة واليقين القضائي، طبقاً لقواعد قانونية ينص عليها بهذا الشأن، وذلك أما بتحديده دليلاً معيناً أو يسلزم شروطاً للدليل لإثبات الإدانة، ويترتب على هذا النظام، أن القاضي لا يمكنه أن يصل إلى قناعته بإثبات الواقعة إلا إذا توافر هذا الدليل، أو اجتمعت تلك الشروط اللازمة

له، متى توافرت أوجبة الحكم بالإدانة، مهما كانت قناعته بشأن حقيقتها، فالمشرع في نظام الأدلة القانونية،هو الذي يحدد حجية الأدلة مسبقاً ويضع ما يسمى ( بنسعيرة الأدلة) حيث يحدد القيمة المقنعة لها، وذلك وفق معايير خاصة به، فإذا توافرت منحها حجية كاملة أو نسبية حسبما يضعه من معيار[١].

ففي هذا النظام يختص المشرع بتحديد القيمة القانونية للدليل إذا توافرت له شروط معينة، فيلتزم القاضي بالأخذ به، ولا تكون له سلطة تقديرية في رفضه. ويترتب على ذلك أنه إذا توافرت أدلة الإدانة بشروطها التي حددها القانون التزم القاضي أن يدين المتهم، ولو كان غير مقتنع بإدانته[٢].

وبالتالي تكون الأدلة محصورة ومحددة سلفاً من قبل المشرع، بل إن قوتها التدليلية محددة ولا يجوز للقاضي أن يخرج عليها أو يبني حكمه على خلافها، ولا يستطيع تكوين عقيدته إلا بهذا الدليل الذي حدده القانون، فلا يحكم بعلمه الشخصي، ولا يجعل للدليل قيمة أكثر مما هو محدد له بالقانون، وهذا يعني أن القاضي يقبلها في حالة معينة، ويحظر عليه أن يقبل أدلة سواها، وإن كان يجوز له هذه الأخيرة في حالات مختلفة[٣].

ففي نظام الأدلة القانونية يتم الاقتناع اليقيني للقاضي وفقاً للشروط القانونية التي يحددها المشرع سلفاً، فالقاضي لا يكون سيد الموقف في تقدير قيمتها في الإثبات بل دوره يتمثل في مجرد التحقق من قيامها ومراقبة توافر شروطها القانونية لكي يقرر بعد ذلك اقتناعه أو عدم اقتناعه أي عمله هو مجرد عملية حساب رياضية لا دخل فيها لاقتناعه الشخصي[4].

---

(١) د. فاضل زيدان محمد، المرجع السابق، ص٦٣.

(٢) د. محمود نجيب حسني،المرجع السابق، ص٧٧٠ – ٧٧١.

(٣) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٣٣.

(٤) د. أحمد فتحي سرور، أصول الإجراءات الجنائية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، ١٩٦٩م، ص ٣٤٣ – ٣٤٤.

بالإضافة إلى ذلك يحدد الشارع القيمة القانونية للدليل إذا توافرت شروط معينة، وعندها يلتزم القاضي الجزائي بالأخذ به، وليس له رفضه، فيبني اقتناعه عليه، ويؤسس حكمه على أساسه، حتى وإن لم يكن مقتنعاً به شخصياً، وإذا لم تتوافر تلك العناصر، فالقاضي يكون على العكس ملزماً ببناء اقتناعه وتأسيس حكمه على أساس عدم قيام الدليل على الادعاء، حتى وإن كان بداخله مقتنعاً تماماً بثبوت الادعاء[١].

فالدليل القانوني وفقاً لهذا النظام هو الدليل الذي حدد القانون نوعه وقيمته مسبقاً، ويجد هذا النظام له مجالاً واسعاً في الإثبات المدني، وساد قديماً في بعض أنظمة الإثبات الجزائية، كما هو الحال في الإمبراطورية الرومانية، وفي أوربا في القرون الوسطى وما بعدها[٢].

ويُعاب على نظام الإثبات المقيد أن من شأنه تقييد القاضي على نحو يفقده سلطته في الحكم بما يتفق مع الواقع فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام، فيصبح القاضي كالآلة في إطاعته لنصوص القانون، ولذلك فإن النظام بدأ ينحسر نطاقه حتى في الدول التي تعد الأكثر اعتناقاً له[٣].

---

(١) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٣٣.

(٢) د.محمد أحمد المنشاوي، المرجع السابق، ص٥٣٥.

(٣) حيث أن بريطانيا مثلاً بدأت تخفف من غلوه حيث ظهر ما يعرف بقاعدة الإدانة دون أدنى شك، والتي مفادها أن القاضي يستطيع أن يكون عقيدته من أي دليل وإن لم يكن من ضمن الأدلة المنصوص عليها متى كان هذا الدليل قاطعاً في دلالته. د. هلالي عبد الله أحمد، المرجع السابق، ص٩١، وأيضاً خالد عياد الحلبي، المرجع السابق، ص٢٣٧.
ميسون خلف حمد الحمداني، المرجع السابق، ص٢٢٩.

**ثانياً: مدى حرية القاضي الجزائي في تقدير الدليل الإلكتروني في نظام الإثبات المقيد:**

تشترط المحاكم ذات النظام الأنكلوسكسوني بصفة عامة أن يكون الدليل متعلقاً بالقضية التي يجري نظرها وأن يكون محل ثقة ومعتمد كشرط لقبول جميع أنواع الأدلة الفنية التي تقدم في جرائم الكومبيوتر ويقوم القضاء بتحديد درجة مصداقية وفاعلية الدليل العلمي للوصول إلى النتيجة النهائية التي تم الحصول عليها باستخدام أحد أدوات الأدلة التناظرية الرقمية(١).

ويتم ذلك عادة في مرحلة ما قبل إجراءات المحكمة باستخدام موجهات أو "اختبارات داوبورت"(٢)، وتنحصر مسؤولية القاضي أثناء جلسة اختبار داوبورت في تحديد سلامة المنهجية المتبعة والطرق الفنية المتخذة في تحديد الدليل العلمي والقيام بذلك وفقاً لدرجة التوثيق المعتمدة(٣).

ويُعد اختبار داوبورت طريقة أكثر توسعاً للأسلوب الذي تبنته المحاكم سابقاً لقبول الدليل العلمي، إذ كانت المحاكم سابقاً إبان استخدامها للاختبار ( Frye Test) تضع مسؤولية تحديد الإجراءات المقبولة على المجتمع العلمي باستخدام المجلات والإصدارات العلمية المحققة، ولكن نسبة لعدم وجود مجلات علمية مراجعة في جميع المجالات تم استخدام اختبار داوبورت الذي يوفر وسائل وطرقاً إضافية لاختبار نوعية الدليل(٤).

وتحدد طريقة اختبار داوبورت (Daubert Test) أربع فئات عامة يجب استخدامها كموجهات عند تقييم الإجراءات أو المنهجية المتبعة:

---

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١٣٠.

(٢) ترجع أصول هذه الاختبارات للحكم الذي أصدرته المحكمة العليا الأمريكية في قضية داوبورت ضد ميريل دو للصناعات الدوائية عام ١٩٩٣م.

(3) Open source. Open source Case for Business. Available at: http://www.opensource.org/advocacy/case for business.php. Date 11/8/2018.

(4) Linux - NTFS Project.NTFS, Documentation Available at: http://linux - ntfssourceforgenet/ntfs. Date: 12/7/2018

١ – التجربة والاختبار: هل من الممكن تجربة واختبار الطريقة المتبعة أو هل سبق اختبار الطريقة المتبعة؟

٢ – نسبة الخطأ: هل هناك نسبة خطأ محتملة ترافق استخدام هذه الطريقة.

٣ – النشر: هل جرى نشر الطريقة المتبعة وخضع للمراجعة من قبل الآخرين؟

٤ – القبول: هل الطريقة المتبعة مقبولة بصورة عامة في المجتمع العلمي المعني؟[١].

وفي هذا الصدد لا يتم قبول الدليل الإلكتروني كدليل إذا لم يستكمل باختبارات الثقة للتأكد من صحته ودقته وصحة وكفاءة الكومبيوتر المستخرج منه وكان القائم عليه تتوافر فيه الثقة والاطمئنان[٢].

وسنشرح ذلك كالتالي:

**أ- التجربة والاختبار (Testing):**

تقوم الموجهات المعنية بالتجربة والاختبار على قابلية إخضاع الإجراءات المستخدمة للتجربة والاختبار للتأكد من أنها تقدم نتائج دقيقة، وإذا كان ذلك صحيحاً فهل معرفة النتيجة التي تم الحصول عليها تُعد نتيجة دقيقة؟ وتُعد هذه المشكلة معقدة جداً فيما يتعلق بالأدلة التناظرية الرقمية وذلك بالنظر لصعوبة وتعقد أجهزة الكومبيوتر. وتخضع نتيجة أو محصلة الأدوات المستخدمة إلى اختبارين رئيسيين هما اختبار السلبيات الزائفة (False Negatives) واختبار الإيجابيات الزائفة (False Positives)[٣].

**١- اختبار السلبيات الزائفة (False Negatives):**

يهدف إجراء اختبار السلبيات الزائفة إلى التأكد من أن الأدوات المستخدمة في الحصول على الدليل تقدم كافة البيانات المتاحة في هذا الدليل وتعرض

---

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١٣٠ – ١٣١.

(٢) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٢٦٨.

(3) NIST. Computer Forensics Toll Testing. Available at: http://www.cftt.nist.gov. Date:13/7/2018.

النتيجة أو المحصلة النهائية التي تم التوصل إليها. فعلى سبيل المثال يجب أن تظهر جميع الملفات إذا قمنا بعرض محتويات دليل ما بداخل الحاسوب.

وبنفس القدر يجب أن تكون الأداة قادرة على عرض أسماء الملفات المحذوفة فيجب أن تكون الأداة المستخدمة في الحصول على البيانات قادرة على نسخ كافة البيانات إلى الجهة المرغوب بنسخ البيانات فيها، ويُعد هذا النوع من الأدوات فيما يتعلق بالأدلة التناظرية الرقمية من أسمى الأنواع التي يمكن اختيارها والأكثر خضوعاً للتجربة والاختبار. إذ يتم نقل بيانات معروفة إلى نظام ما وبعد ذلك يجري تحليلها والتحقق من إمكانية العثور على هذه البيانات في الجهة التي تم النقل إليها[١].

**٢- اختبار الإيجابيات الزائفة (False Positives):**

تهدف اختبارات وتجارب الإيجابيات الزائفة إلى التأكد من عدم إضافة بيانات جديدة نتيجة لاستخدام الأدوات المعنية، فعلى سبيل المثال ضمان عدم إضافة أسماء ملفات جديدة عندما تستخدم الأدوات في عرض محتويات دليل ما. ويُعد هذا الاختبار من أصعب أنواع الاختبارات، وأكثر الطرق الفنية استخداماً للتحقق من أن الأداة المستخدمة لا تؤدي إلى إضافة أو إدخال بيانات جديدة، فهي طريقة للتحقق من النتائج باستخدام أداة ثانية، وعلى الرغم من أن هذه الطريقة تُعد طريقة جيدة إلا أنها لا تغني عن الحاجة إلى وجود منهجية ثابتة لإجراء تجارب واختبارات رسمية[٢].

لذلك قام المعهد الوطني للمقاييس والتكنولوجيا ( The National Institute Of Standards and Technology) بتخصيص مجموعة تركز كل جهودها على طرق تجربة واختبار أدوات الأدلة التناظرية الرقمية، وقامت بصياغة وتطوير منهجيات متعددة لكيفية إجراء التجارب والاختبارات لنوعية الأدوات المستخدمة وإجراء التجارب

---

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص ١٣٢ - ١٣٣.

(٢) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١٣٣.

باستخدام طرق معينة لإدخال البيانات. كما قامت هذه المجموعة بنشر مواصفات أدوات نسخ محتويات الأقراص كما قامت أيضاً بإجراء هذه الاختبارات على مختلف أنواع الأدوات، غير أنه لم يتم حتى الآن الكشف بصورة رسمية عن النتائج التي تم التوصل إليها. وبالإضافة إلى ذلك توصلت هذه المجموعة إلى منهجية اختبار تتعلق بالأدوات المستخدمة في التحليل[1].

وقبل الوصول إلى نتائج معهد المواصفات والتكنولوجيا وطرق اختبار أدوات الأدلة الرقمية جرت العادة على نشر تجربة واحدة من تجارب مقارنة أدوات الأدلة الرقمية، تقوم التجربة بنسخ أو زرع بيانات في مواقع متعددة تستخدم مختلف أنواع الأقراص ومن ثم تقوم بمحاولة العثور على البيانات التي تم نسخها أو نقلها إليه.

وعلى الرغم من أهمية وفائدة هذه التقييمات عند القيام بدراسة أي نوع من الأدوات فينبغي شراؤها (بغض النظر عن مواضع الخلل والأخطاء المتواجدة) إلا أنه من الضرورة بمكان إلا تكون هذه التقييمات هي الخيارات الوحيدة المتاحة أمام الإجراءات القانونية.

لذلك فإن أمثل طريقة لاختيار أدوات الأدلة الرقمية تتمثل في استخدام برامج المصادر الحرة أو المفتوحة، وبالإضافة إلى ذلك ينبغي صياغة وإعداد شروط ومتطلبات كل أداة من أنواع الأدوات كما يجب صياغة نوعية الاختبارات لكل أداة التي تطبق هذه الشروط والمتطلبات.

ويؤدي استخدام شروط محددة بإجراء التجربة والاختبار لكافة أنواع الأدلة إلى اكتشاف المزيد من مواضع الخلل والأخطاء وذلك بالنظر للعدد الكبير من الاختبارات التي بالإمكان إجراءها، فعلى سبيل المثال، فإن إعداد مجموعة شاملة لمتطلبات وشروط التجارب والاختبارات لكافة أدوات تحليل نظام الملفات يُعد مهماً

(1) NIST CETT. Disk Imaging Tool Specification, 3,1,6 Edition, October 2001, Available at:
http://www.cftt.nist.gov/DI - spec - 3 - 6/doc. Date 11/9/2018.

وواجباً متعدد الاتجاهات، ويعود السبب وراء ذلك بصورة خاصة إلى أن تنظيم أو تركيب نظام الملفات ليس تركيباً عاماً[١].

واستناداً إلى المتطلبات والشروط الزمنية، فمن غير المحتمل تطوير مجموعة اختبارات بإمكانها إثبات صحة وسلامة كافة المكونات المحتملة لنظم الملفات، وفي واقع الأمر فمن المحتمل جداً أن تكون متطلبات وشروط الاختبار أكثر دقة وحداثة فيما يتعلق بالأدوات التحليلية للأدلة التناظرية الرقمية ومن ثم التطبيق الرئيسي وتجارب نظام التشغيل وبالإضافة إلى ذلك يجب أن تكون أداة التحليل قادرة على التعامل مع كافة الظروف والأوضاع المحتملة.

لكن إذا كانت خلاف ذلك فقد يتيح ذلك للمتهم التشكيك في مصداقية وموضوعية الدليل كما يعمل على خلق وإيجاد حالة قد تؤدي إلى اختفاء البيانات في مرحلة إجراء التحقيقات. وبصورة عامة يجب أن يكون برنامج التطبيق الأصلي قادراً على اختبار وتجربة مقدرته في التعامل مع أي حالة أو ظروف يستطيع خلقها وإيجادها.

ولكن على الرغم من ذلك لم يتم التوصل إلى منهجية اختبار قياسية، لذلك يتم اكتشاف مواضع الخلل والعيوب في تطبيقات المصادر المفتوحة والمصادر المغلقة في وقتنا الراهن بواسطة المحققين أو خبراء الأدلة الرقمية أو مستهلكي هذه البرامج في نفس المجال والذين يقومون بدورهم بإخطار البائع بمواضع الخلل.

ولعل الحجة التي توجه ضد برامج تطبيقات المصادر المفتوحة تتمثل في أن بعض الأفراد من ذوي النوايا الإجرامية قد يكتشفوا بعض الخلل والعيوب في شفرة المصدر ويقومون باستغلالها لتحقيق نواياهم الإجرامية دون نشر أي معلومات أو تفاصيل عن موضع الخلل والضعف التي اكتشفوها.

---

(1) Scientific Working Group on Imaging Technologies. Definitions and Guidelines for the use of Imaging Technologies in the criminal justice system. Forensic Communications, 1(3) October 1999, Available at: http://www.fbi.gov/hq/lab/fsc/backissu/oct1999/swgit.htm. Date 10/9/2018.

وعلى كل حال، توجد مواضع الضعف والخلل في تطبيقات المصادر المفتوحة كما توجد أيضاً في برامج تطبيقات المصادر المغلقة، وبذلك تتساوى احتمالية قيام أحد الأفراد من ذوي النوايا السيئة باستغلال أماكن الضعف والخلل الموجودة في أي من التطبيقين، ويتمثل الحل الدائم لهذه المشكلة في إيجاد منهجية اختبار شامل تؤدي إلى تقليل عدد الأخطاء ومواضع الخلل وبذلك تقل فرص استغلال هذه التطبيقات بواسطة الأشخاص من ذوي النوايا السيئة.

ويؤدي امتلاك وسيلة الدخول إلى شفرة مصدر الأداة المستخدمة إلى تحسين نوعي في كيفية إجراء التجربة وذلك نظراً لإمكانية تحديد مواقع الأخطاء والخلل عبر دراسة ومراجعة الشفرة المستخدمة وعير تصميم بعض الاختبارات والتجارب اعتماداً على تصميم وانسياب البرامج.

وأخيراً، يجب أن يتم إجراء هذه التجارب بواسطة خبراء محايدين من ذوي الخبرة والدراسة، كما يجب أن يتم نشر نتائج هذه التجارب والاختبارات، كما يجب على أقل تقدير أن يتم نشر مواصفات تصميم أدوات المصادر المفتوحة حتى يتمكن الطرف الثالث مثل فريق المعهد الوطني للمواصفات والتكنولوجيا المعني بتجربة واختبار أدوات الأدلة التناظرية الرقمية من اختبار الإجراءات المستخدمة أو منهج المعالجة الخاص بالأداة المستخدمة بصورة وفاعلية أكثر[١].

**وهكذا نرى أن الهدف من استخدام موجه التجربة والاختبار للطريقة المتبعة في الحصول على الأدلة الإلكترونية هو تجنب الأخطاء والخلل، والتأكد من صحة ودقة النتائج التي تم التوصل إليها.**

**ب- نسبة الخطأ (Error Rates):**

تهدف موجهات نسبة الخطأ إلى تحديد نسبة الخطأ المعروفة في الإجراءات أو منهج المعالجة التي تقوم بها أدوات الأدلة التناظرية الرقمية بمعالجة البيانات

---

(١) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص١٣٦ - ١٣٧.

عبر سلسلة من القواعد والضوابط، وفي العادة يتم تعميم وإعداد مثل هذه القواعد والضوابط بواسطة مصنعي برنامج التطبيق الأصلي الذي يجري تحليله.

فعلى سبيل المثال تستخدم أدلة تحليل الملفات مواصفات نظام الملفات في عملية إجراء التحليل، لذلك تنعدم نسبة الخطأ تماماً في الأداة المستخدمة باستثناء أخطاء البرمجة إذا كانت هذه المواصفات متاحة للجميع. أما إذا لم تتوفر مثل هذه المواصفات لفريق المعهد الوطني للمواصفات والتكنولوجيا على سبيل المثال – فإن ذلك يؤدي إلى حدوث أخطاء نسبة لعدم فهم واستيعاب المواصفات المطلوبة.

وتشابه هذه المواصفات الطرق الفنية لإجراء التجارب والتي يتم استخدامها مع النظم الطبيعية مثل فحص واختبار الحمض النووي أو البصمات والتي ترافقها نسبة خطأ اعتماداً على كيفية إجراء التجربة والاختبار[1].

ووفقاً لما ورد أعلاه يوجد نوعان من الأخطاء في أدوات علم الأدلة التناظرية الرقمية وهما تحديد الخطأ في استخدام الأداة وخطأ استخلاص الدليل ويحدث الخطأ في استخدام الأداة المناسبة بسبب مواضع الخلل والخطأ في الشفرة المستخدمة أو بفعل استخدام مواصفات خاطئة. أما خطأ استخلاص الدليل فيرجع إلى اتخاذ قرارات لاستخدام الأداة تقل نسبة التأكد من صوابها عن ١٠٠% ويحدث هذا غالباً بسبب وسائل اختزال البيانات بطريقة تختلف عن الطريقة الأصلية التي تم تصميمها. وإن إعطاء نسبة الخطأ في كافة الإجراءات المستخدمة لاستخلاص الدليل – كما هو الحال في مختلف فروع العلم – يُعد أمراً يسيراً – إذ أن البحوث التي يتم القيام بها ستؤدي إلى تقليل نسبة الخطأ التي تم تحديدها، ومن الجانب الآخر فمن الصعوبة بمكان تحديد قيمة معينة لهامش

(1) Daved Wheeler. Is Open Source Good for Security? Secure Programming for Linux and Unix HOWTO 13 july 2002. Available at: http://www.dwheeler.com/secure - programs/Secure - Programs - HO//w/tO/open - source - security.html. Date 21/9/2018.

الخطأ في الأداة المستخدمة، ووفقاً لما سبق بالإمكان حساب نسبة الخطأ لكل أداة اعتماداً على عدد وخطورة مواضع الخلل والأخطاء.

وللمحافظة على قيمة أو نسبة الخطأ التي تم تحديدها يجب علينا امتلاك الوسيلة التي تمكننا من معرفة حالات الخطأ ومواضع الخلل التي ظلت ترافق الأداة المستخدمة، ويُعد هذا الجانب سهلاً بدرجة نسبية فيما يتعلق بأدوات المصادر المفتوحة نسبة لإمكانية مقارنة آخر إصدار من المصدر مع الإصدار السابق لاكتشاف الشفرة التي تم تغييرها حتى وإن لم يتم توثيق وتسجيل مواقع الخلل والأخطاء.

ولكن من الصعوبة بمكان المحافظة على نسبة الخطأ في برامج تطبيقات الموارد المغلقة وذلك بالنظر لإمكانية معالجة الخلل أو تصحيح الخطأ بكل هدوء إذا لم يتم نشر ذلك الخطأ للجميع. بالإضافة إلى أنه سيصبح من الصعوبة بمكان البدء في حساب نسبة الخطأ وذلك لأن الأدوات التجارية تركز على مقدار العوائد وحجم المبيعات، لذلك فإن نشر الخطأ يُعد أمراً محصوراً بالنسبة لما ينطوي عليه من خسائر بسبب انخفاض المبيعات.

ونسبة لعدم وجود معادلة محددة لحساب نسبة الخطأ يجري الاعتماد بصورة رئيسية على حصة السوق من الأدوات المعينة باعتبارها مقياساً على اعتبار أن الناس سيحجمون عن شراء الأدوات ذات نسبة الأخطاء المرتفعة.

وعلى الرغم من أن هذا الاتجاه قد يكون صحيحاً إلى حد ما إلا أن هناك ضرورة لإيجاد طريقة أكثر عملية لتحديد نسبة الخطأ بصورة ميدانية، فأرقام أو حجم المبيعات لا توضح عدد مرات استخدام أداة ما أو درجة صعوبة وتعقد البيانات التي تقوم بمعالجتها، لذلك فيجب علينا عند تحديد نسبة الخطأ أن نأخذ بالحسبان مخطط عمليات التحليل البسيطة ومخطط عمليات التحليل البالغة الصعوبة والتعقيد وهي الأماكن التي بها حاول المشتبه فيه إخفاء البيانات من الأداة المستخدمة.

وبغرض خفض نسبة الخطأ يجب علينا تطوير منهجية التجارب والاختبارات التي تتطلبها أدوات المصادر المفتوحة من أجل صياغة منهجية اختبارات بصورة أكثر سهولة وإضافة إلى ذلك من الصعوبة بمكان أن ينجح أحد التطبيقات المفتوحة في إخفاء حالات الأخطاء ومواضع الخلل التي ترافقه، لذلك يجب أن نولي عناية خاصة في مثل هذه الأدوات والإجراءات المستخدمة في نسخ البيانات من إحدى وسائل التخزين إلى وسيلة أخرى وإلى استخلاص الملفات والبيانات الأخرى من نسخة نظام الملفات[١].

**جـ- النشر (Publication):**

توضح موجهات النشر في "اختبارات داوبورت"، أن الإجراءات المتبعة للحصول على الدليل الإلكتروني إجراءات موثقة في مكان عام وأنها خضعت للبحث والتحقيق من ذوي الاختصاص ووفقاً لاختبار (Fry Test) الذي كان يجري سابقاً فإن الشرط الوحيد لقبول الدليل العلمي كان يتمثل في البحث والتحقيق عن الإجراءات المتبعة بواسطة ذوي الاختصاص، أما فيما يتعلق بالأدلة التناظرية الرقمية فلم تظهر إلا حديثاً منشورات علمية تتناول بالبحث والدراسة الأدلة الرقمية التناظرية ومع ذلك لم تشمل هذه المجلات الإجراءات التي تتبعها أدوات استخلاص الأدلة الرقمية.

وفي إصدار المجلة الدولية لعلم الأدلة الجزائية الرقمية " The International Journal of Digital Evidence" جرت العادة على استغلال مقالات مجلات التكنولوجيا في نشر ومناقشة أدوات الأدلة الجزائية الرقمية، وقد أشارت إحدى هذه المقالات إلى الاستخدام الواسع لهذه الأدوات كما قامت بسرد بعض ملامح هذه الأدوات وفي الغالب يتناول هذا النوع من النشر الإجراءات ذات المستوى المتقدم

---

١ د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص ١٣٨ – ١٣٩.

للحصول على القرص المستخدم وكيفية تحليل مواضيعه ألا أنه لا تناقش الإجراءات الفنية المستخدمة في استخلاص الدليل.

وفيما يتعلق بتحليل نظام الملفات فإن الإجراءات التي يجب نشرها تتمثل في الإجراءات المستخدمة في تقسيم ملف ضخم الحجم والمحتويات إلى آلاف الملفات التي يكونها المستخدمون في حافظات الملفات والدلائل(١).

وبالإضافة إلى ذلك توضح معظم أدوات علم الأدلة التناظرية الرقمية المستخدمة في تحليل نظم الملفات حافظة الملفات والدلائل التي تم حذفها من القرص كما أنها تستطيع في بعض الأحيان استرجاعها مرة أخرى، ولأن هذه الوظائف والواجبات لا تمثل جزءاً من مواصفات نظام الملفات الأصلي لذلك لا توجد طريقة قياسية لكيفية إجرائها والقيام بها حيث يتم استرجاع أسماء الملفات المحذوفة عبر معالجة المساحات غير المستخدمة في القرص لإيجاد البيانات التي تجتاز شروط ومتطلبات خاصة للفحص والتدقيق.

فإذا كانت اختبارات الفحص شديدة الدقة يؤدي ذلك إلى عدم ظهور بعض الملفات وبالتالي عدم العثور على الدليل، أما إذا كانت شروط ومتطلبات الفحص والتدقيق شديدة الضعف يؤدي ذلك إلى ظهور بيانات خاطئة، لذلك يجب أن يتم نشر إجراءات هذه الطريقة حتى يتمكن المحقق من معرفة كيفية تطبيق واستخدام هذه الإجراءات(٢).

هذا وقد نشرت مجلة مكتب التحقيقات الفيدرالية الأمريكية ( The FPI, s Forensic Journal) في عام ١٩٩٩م، وثيقة حول استخدام الصورة الرقمية وقد أرفق مع قسم موجهات البرنامج المستخدم الواردة في هذه الوثيقة التحذير القانوني

---

(1) Brian Carrier, "Open Source Digital Forensic Tolls, the Legal Arguments, October 2002", Available at:
http://www.atstak.com Date 22/9/2018.

(2) Eoghan Casey; "Digital Evidence and Computer Crime" February 2002. ISBN:012162885 X, Available at:
http://www.apcatalog.com Date 22/9/2018.

التالي: "قد يتحتم على مصنعي البرنامج المستخدم لمعالجة الصور إتاحة أو تمكين الخصوم من معرفة شفرة مصدر البرنامج ويخضع ذلك لأمر حماية مناسبة تمت صياغته بغرض حماية حقوق ملكية المصنع، ويترتب على عدم قيام المصنع بتقديم هذه المعلومات إلى الخصوم استبعاد الصورة كدليل في إجراءات المحاكمة، ويجب أن يؤخذ هذا الجانب بالحسبان عند اختبار البرنامج الذي ينوي استخدامه"(١).

توضح الفقرة الواردة أعلاه وجوب توفر الرغبة والاستعداد لدى مصنعي البرامج على كشف شفرة المصدر الخاصة بهم إذا كان ذلك لغرض الحصول على الدليل المطلوب، أما إذا كانت جهة الصنع غير راغبة في الكشف عن الشفرة فيجب أن يتم الإعلان عن ذلك قبل وقت كاف حتى يتم التحوط أو وضعه في الاعتبار عند شراء أداة تحليل.

أما إذا سمحت المحكمة بدراسة شفرة المصدر بواسطة أحد الشهود الخبراء في هذا مجال على ألا يتم الكشف عن الشفرة المستخدمة فقد يكون هذا التوجه مقبولاً إذا كانت هناك طريقة فنية لمعالجة البيانات مقبولة بصورة عامة إذ باستطاعة الخبير مقارنة رمز المصدر مع الإجراءات المقبولة والتحقق من أنها استخدمت على النحو المطلوب.

ويُعد النشر جانباً بالغ الأهمية كما يُعد أيضاً الجانب الذي يفقده علم الأدلة التناظرية الرقمية، فإذا لم تنشر أي معلومات ضئيلة عن استرجاع الملفات المحذوفة وعن تحليل نظم الملفات، يجب على الأقل أن تنشر أدوات المصدر المقفول وكذلك مواصفات التصميم التي توثق إجراءات ومعلومات وتفاصيل التحليل الذي تقوم بإجرائه.

---

(1) Eoghan Casey; Computer Crime Investigation" October 2001 ISBN:012631036, Available at: http://www.apcatalog.com Date 22/9/2018.

كما يجب على أدوات المصادر المفتوحة أن تكشف كل الإجراءات المتعلقة بها عبر شفرة المصدر بغرض تمكين الشخص من التحقق بأن الأداة تتبع الطريقة التي تم نشرها وتتحاشى نشر الحد الأدنى فقط من المعلومات المطلوبة، وبالإضافة إلى ذلك على أدوات المصادر المفتوحة نشر كافة التفاصيل المتعلقة بالإجراءات المستخدمة بلغة أخرى وليس بشفرة المصدر فقط(١).

**رابعاً: القبول (Acceptance):**

يمثل القبول الإطار التوجيهي للمجتمع العلمي لتقييم الإجراءات التي تم نشرها، واستجابت أدوات المصدر المغلق سابقاً إلى هذا الموجه عبر الإشارة إلى الأعداد الضخمة من المستخدمين إذ يختلف قبول الأداة عن القبول بإجراء بعض الإجراءات المستخدمة.

فإذا كانت هنالك خيارات محدودة من الأدوات التي باستطاعتها تنفيذ إجراء ما وكانت جميع هذه الأدوات تفتقد إلى المعلومات المنشورة عن تفاصيل الإجراءات أو الأخطاء ومواضع الخلل الرئيسية ما يعتمد اختيار الأداة المناسبة من بين هذه الأدوات عن العوامل اللإجرائية مثل مقدار الدعم الذي توفره مجموعة الأدوات المستندة عليه.

فإلى أن يتم نشر التفاصيل الإجرائية وتصبح عاملاً أساسياً يجب أن يؤخذ بالحسبان عند شراء أدوات تحليل الأدلة الرقمية التناظرية أنه لا يمكن اعتبار حجم مستخدمي الأداة كمقياس صحيح لدرجة القبول بالإجراءات المستخدمة وإنما يمكن الاعتماد على توثيق أدوات المصدر المفتوح وكذلك الإجراءات التي تستخدمها عبر إتاحة شفرة المصدر للجميع ويتيح ذلك للمستخدمين قبولها أو رفضها(٢).

---

(1) Eoghan Casey; Computer Crime Investigation" October 2001 ISBN:012631036, Available at: http://www.apcatalog.com Date 22/9/2018.

(2) Eoghan Casey; "Computer Crime Investigation" October 2001 ISBN:012631036, Available at: http://www.apcatalog.com Date 22/9/2018.

**ونحن نرى أن الدليل الإلكتروني يجب أن يخضع لموجهات اختبارات داوبورت وذلك باعتباره دليل علمي، وبالتالي تسري موجهات اختبارات داوبورت على الدليل الإلكتروني وذلك من أجل فحص وإثبات صحة الإجراءات المستخدمة للحصول على الدليل الإلكتروني وبالتالي الحصول على دليل صحيح دون أي خلل وخالي من الأخطاء.**

وبعد دراسة الأسس العامة لتقدير الدليل الإلكتروني في النظام الأنكلوسكسوني، سنقوم بعرض موقف بعض التشريعات الأنكلوسكسونية من تقدير الدليل الإلكتروني.

## الفرع الثاني

## موقف بعض التشريعات الأنكلوسكسونية من تقدير الدليل الإلكتروني

أن التشريعات الانكلوسكسونية تتمثل بتشريع الولايات المتحدة الأمريكية وإنكلترا وكندا، وبناء على ما تقدم، سنتناول بحث تقدير الدليل الإلكتروني أولاً، في الولايات المتحدة الأمريكية وثانياً، في إنكلترا، وثالثاً، في كندا.

**أولاً: الولايات المتحدة الأمريكية:**

سنقوم بدراسة موقف الفقه الأمريكي، ومن ثم موقف القضاء الأمريكي، وأخيراً موقف التشريع الأمريكي.

**أ- موقف الفقه الأمريكي:**

يلخص الفقيه الأمريكي أدوار وايز (Edward WISE) الوضع بالنسبة لمدى قبول الأدلة الناتجة عن الحاسوب بقوله إن الصعوبات الحقيقة في الولايات المتحدة الأمريكية نابعة من عدم الالفة مع تكنولوجيا الحاسوب أكثر من كونها صعوبات قانونية، ولذلك فمن غير المعتقد، على وجه العموم، أن تكون هنالك

حاجة ماسة إلى سن تشريعات بخصوص التعامل مع مدى قبولية السجلات المعالجة بواسطة الحاسوب[١].

وإن الفقه في أمريكا يرى بأنه حتى يكون الدليل الإلكتروني مقبولاً أمام المحكمة، يجب أن يتوفر فيه الشروط التالية:

١- أن لا يطرأ على محتويات السجل الإلكتروني أي تغيير، أي أن يكون الدليل المقدم إلى المحكمة هو نفس الدليل الذي تمّ جمعه، ويمكن للشخص الذي قام بجمع الدليل أن يشهد بذلك أمام المحكمة، وهذا ما يطلق عليه مفهوم "**سلسلة الرعاية**" Chain of Custody، ويقصد بذلك أن الدليل الإلكتروني منذ لحظة جمعه وحتى لحظة تقديمه إلى المحكمة لم يطرأ عليه أي تغيير، ولا يوجد أي احتمال للعبث به، وأنه تمّت مراعاة سلامته حتى يبقى بنفس الحالة التي وجد عليها[٢].

٢- أن تكون المعلومات الموجودة في السجل، قد صدرت فعلاً عن المصدر المزعوم، سواء كان هذا المصدر الإنسان أم الآلة.

٣- أن تكون المعلومات الموجودة في السجل، والمتعلقة بالوقت والتاريخ، معلومات دقيقة[٣].

**ب- موقف القضاء الأمريكي:**

قرر القضاء الأمريكي في أحكامه المختلفة، أن المخرجات الكومبيوترية يجب أن تكون مقبولة كأدلة إثبات، طالما كان الحاسوب المتولدة عنه يؤدي وظائفه بصورة سليمة، وكان القائم عليه تتوافر فيه الثقة الطمأنينة[٤].

---

(1) WISE (Edward M), "Computer crimes and other crimes against information Technology in the United States, R. I. D. P, 1993, P.667.

(2) Dr. Henry B. wolfe, Forensics and the emerging importance of electronic Evidence gathering, OTAGO university, 2001, P - 4, available on line. www.e - evidence.info.

(٣) د. محمد طارق الخن، المرجع السابق،ص١١٩.

(٤) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٢٩.

كما تعرض القضاء الأمريكي في العديد من القضايا إلى مسألتي الأصالة والصحة، ففي إحدى القضايا، قررت المحكمة: "إن عضو مكتب التحقيقات الفيدرالي FBI الذي كان حاضراً عندما تمّ ضبط الحاسوب الخاص بالمتهم، يمكن أن يقرر صحة الملفات المضبوطة". وفي قضية أخرى قبلت المحكمة سجلات الهاتف بعد أن أكّدت موظفة الفواتير في الشركة أصالة هذه السجلات. كما قبلت إحدى المحاكم الدليل الإلكتروني رغم الدفوع المتعلقة بالعبث بهذا الدليل، لأن هذه الدفوع جاءت على شكل تخمين، دون أن يوجد أي دليل يدعمها. وفي إحدى القضايا قررت المحكمة: "إن حقيقة وجود احتمال بتعديل البيانات الموجودة في الحاسوب غير كافية للقول بعدم جدارة الدليل." كما ذكرت وزارة العدل الأمريكية في المرشد الفيدرالي لتفتيش وضبط الحواسيب، وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية: "إن غياب دليل واضح على حدوث العبث في الدليل، لا يؤثر على أصالة ودقة سجلات الحاسوب"(١).

**جـ- موقف التشريع الأمريكي:**

يشترط المشرع الأمريكي لقبول الدليل الإلكتروني ثبوت صحة وأصالة (Authentication) كل الملفات الموجودة في النظام الحاسوبي وذلك بعد تقرير كفاية الدليل لدعم صحة ثبوت الواقعة محل النزاع بالإضافة إلى أنه فيما يتعلق بالدليل المخزن (Stored Records) فإنه يجب ثبوت أن الدليل المستمد منه ليس شهادة سماع (Hearsay) التي هي غير مقبولة وفق النظام الأمريكي(٢).

حيث تبنّى قانون الإثبات الفيدرالي في المادة /١٠٠٢/ منه قاعدة **الدليل الأفضل**، ويقصد بهذه القاعدة أنه عند إثبات مضمون كتابات أو سجلات أو صور، فإن أصل هذه الكتابات أو السجلات أو الصور يجب أن يكون متوفراً، أي

---

(١) د. محمد طارق الخن، المرجع السابق،ص١١٩ - ١٢٠.

(٢) د. عمر محمد بن يونس، ورقة بحثية بعنوان" الدليل الرقمي"، المرجع السابق، ص٦.

يجب تقديمه إلى المحكمة[1].

وقاعدة الدليل الأفضل التي تعبر عن أصالة الدليل تقف حائلاً أمام الدليل الإلكتروني، لأن ما يتم تقديمه إلى المحكمة ليس الملفات الإلكترونية المخزنة في الحاسوب، وإنما نسخ عن هذه الملفات. ولذلك فقد حسم المشرع الأمريكي هذه المسألة لصالح الدليل الإلكتروني في المادة 1001/3 من قانون الإثبات الأمريكي والتي نصت على ما يلي:

"إذا كانت البيانات مخزنة في حاسوب أو آلة مشابهة، فإن أي مخرجات مطبوعة منها أو مخرجات يمكن قراءتها بالنظر إليها وتعكس دقّة البيانات، تعدّ بيانات أصلية".

ووفقا لهذه المادة، فإن البيانات أو المعلومات التي تمّ الحصول عليها من الإنترنت، والتي تمّ استخراجها بواسطة الطابعة، تعدّ دليلاً أصلياً كاملاً، ولا حاجة لجلب الحاسوب إلى قاعة المحكمة.

أما فيما يخص القوة الإثباتية للسجلات الإلكترونية، فإن المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب الصادر في عام ٢٠٠٢ يميز بين نوعين من السجلات، وهما:

**النوع الأول: السجلات المخزنة في الحاسوب:** وهي الوثائق الإلكترونية التي تحتوي على كتابات عائدة لشخص ما، ومن أمثلتها رسائل البريد الإلكتروني، وملفات الورد Word، ورسائل غرف الدردشة على الإنترنت.

---

(1) The Federal Rules of Evidence

يتضمن هذا القانون القواعد المقبولة في الإثبات أمام المحاكم الاتحادية في الولايات المتحدة الأمريكية، في حين أن محاكم الولايات تتبع قواعدها الخاصة مثل "كاليفورنيا" و"واشنطن". وقد وُضِعَ هذا القانون بناء على اقتراح المحكمة العليا في الولايات المتحدة الأمريكية أول مرة عام ١٩٧٥، وجرى تعديله عدة مرات، وهو متوفر على الإنترنت مع تعديلاته حتى ٢٠٠٨/١٢/١ على الموقع www.wikipedia.org أو www.lawsource.com.

وهذه الوثائق تتضمن إفادات بشرية، وتعدّ كالشهادة على السماع في مجال الإثبات[١].

**النوع الثاني: السجلات المأخوذة من الحاسوب:** وهي عبارة عن نتائج برامج الحاسوب التي لا تمسها الأيدي البشرية، ومن أمثلتها سجلات الدخول إلى الإنترنت، وسجلات الهاتف، وإيصالات الصراف الآلي وغيرها. فهذه السجلات لا تتضمن إفادات بشرية، وإنما هي عبارة عن نتائج البرامج الحاسوبية. فالصراف الآلي مثلاً يمكن أن يعطي إيصالاً يتضمن أن /١٠٠/ دولار أمريكي قد تم إيداعها في الحساب عند الساعة ٢.٢٥ مساءً، وهذا النوع من السجلات يمكن للمحاكم أن تأخذ به، إذا كان برنامج الحاسوب يؤدي عمله على نحو جيد وسليم[٢].

وأخيراً يشترط المشرع الأمريكي لقبول الدليل الإلكتروني أن تكون له صلة بالوقائع المراد إثباتها، وهو ما يعرف بالعلاقة الكاشفة[٣].

## ثانياً: في انكلترا:

إذا نظرنا إلى القسم (٦٩) من قانون الشرطة والإثبات الجنائي البريطاني (Pace)[٤] لعام ١٩٨٤م، الذي تم تعديله في ١٤ تشرين الأول عام ٢٠٠٢م، لوجدنا أن المستند الناتج عن الحاسوب الآلي لا يقبل كدليل إذا لم يستكمل باختبارات الثقة (The Tests of reliabilit) المنصوص عليها في هذا القسم من

---

(١) الشهادة على السماع وفق قواعد الإثبات الفيدرالية تقبل على سبيل الاستثناء في المجالات التالية: الأعمال، المذاكرات اليومية، التقارير، السجلات، الأحداث، الشروط، الآراء، التشخيص. فإذا تمّ حفظ هذه الأشكال في الحاسوب بالأسلوب المعتاد ووفق نظام العمل السائد، فإنها تُعد كالشهادة على السماع. د. محمد طارق الخن، المرجع السابق، ص١١٨.

(٢) د. محمد طارق الخن، المرجع السابق، ص١١٨ – ١١٩.

(٣) المادة (٤٠١) من قانون الإثبات الفيدرالي الأمريكي.

(٤) وهو اختصار The Police Criminal Evidence Act ومتوفر على الإنترنت على موقع القوانين البريطانية www.briTishlaw.org.uk.

هذا القانون، ويمكن بلورة هذه الاختبارات أو الشروط الواجب توفرها في المستند الناتج عن الحاسوب، حتى يُقبل كدليل في الإثبات، فيمايلي:

أ- عدم وجود أسس معقولة للاعتقاد بأن البيان يفقد الدقة بسبب الاستخدام غير المناسب أو الخاطئ للحاسوب.

ب- أن الحاسوب كان يعمل في جميع الأحوال بصورة سليمة، وإذا لم يكن كذلك، فإن أي جزء لم يكن يعمل فيه بصورة سليمة، أو كان معطلاً عن العمل، لم يكن ليؤثر في إخراج المستند أو دقة محتوياته(١).

وقد علق مجلس اللوردات على القسم (٦٩) المشار إليه، بأنه: "يمكن للشهادة الشخصية الصادرة عن شخص على علم بطريقة تشغيل الحاسوب، أن تعطي الثقة بالدليل، وليس بالضروري أن يكون هذا الشخص خبيراً بالحاسوب". وبناءً على ذلك قبلت المحاكم الإنكليزية – فيما يتعلق بسلامة نظام الحاسوب – بشهادة أشخاص لديهم علم بطريقة عمل نظام الحاسوب(٢).

بيد أن الأحكام الأخيرة للمحاكم البريطانية تشير إلى أن شروط القسم رقم (٦٩) لا تنطبق إذا كانت مطبوعات الحاسوب دليلاً حقيقاً أو أصلياً وليس مجرد نقل عن الغير(٣).

وقد أشار بعض المتخصصين في مجال الحاسوب إلى استحالة إثبات دقة هذا الحاسوب بالطريقة الموضحة في القانون، ويتضمن ذلك أنه إذا بدأ المحامون جدال في الأدلة الناتجة عن الحاسوب بطريقة معينة، فإنه يستحيل غالباً إثبات الدقة بالمستوى المقبول.

---

(١) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٢٨.

(٢) د. محمد طارق الخن، المرجع السابق،ص١٢٠.

(٣) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص ٧٢٨.

كما اقترح الفقه الإنكليزي أنه في حالة ما إذا كان الحاسوب موضوعاً لاستخدام غير مصرح به فإن أي أدلة مستندية ناتجة عن الحاسوب بخصوص أصل ومدة هذه الاستعمال، لن يكون مقبولاً، لأن سوء استخدام الحاسوب في حد ذاته أدى إلى أن الجهاز لا يعمل كما ينبغي، ولذلك فإن عدداً من المعلقين ناقش مسألة إلغاء القسم (٦٩)، أسوة بما قررته اللجنة القانونية الاسكتلندية بالنسبة لاختبارات الثقة المنصوص عليها في هذا القسم بخصوص الدليل الناتج عن الحاسوب بأنها غير ضرورية في القضايا الجزائية في اسكتلندا[١].

**ثالثاً: في كندا:**

تنص المادة (٢٩) من قانون الإثبات الكندي عام ١٩٨٢م، والخاصة بسجلات المؤسسات المالية على عدد من الشروط التي يجب توافرها قبل عمل صورة (Copy) من السجل الذي يضاف إلى الأدلة، ومن هذه الشروط أن تكون الصورة حقيقية من المدخل الأصلي، وقد قضت محكمة استئناف أونتاريو الكندية في قضية مكميلان (MC Mullen) بأنه:

يشترط لكي تكون سجلات الحاسوب مقبولة بوصفها نسخاً حقيقية من السجلات الإلكترونية، أن تكون محتوية على وصف كامل لنظام حفظ السجلات السائد في المؤسسات المالية، كما يمكن أن يتضمن ذلك وصفاً للإجراءات والعمليات المتعلقة بإدخال البيانات وتخزينها واسترجاعها، حتى يتبين أن المخرج المتحصل من الحاسوب موثوق به بشكل كاف[٢].

كما تعرضت نفس المحكمة السابقة – في قضية بيل وبيروس– لواقعة كانت فيها البيانات الإلكترونية الأصلية قد محيت وكل ما تبقى منها هو مخرجات الطابعة، وقد استخدم البنك هذه المخرجات المطبوعة على أنها الأصل وليس مجرد صورة،

---

(١) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، المرجع السابق، ص٧٢٨.

(2) PIRAGOFF (Donald K), "Computer crimes and other crimes against information Technology in Canda, R I D P, 1993, P. 245.

فأيدت المحكمة ذلك وقالت إن الصورة في هذه الظروف التي كان يستخدمها البنك تنزل منزلة الأصل، وتصبح هذه الصورة هي السجل الأصلي حسبما جاء في المادة (٢٩) [١].

**وهكذا نرى أن التشريعات الأنكلوسكسونية اعترفت بحجية الدليل الإلكتروني أمام القضاء ولكن بعد خضوعه لاختبارات معينة أو توافر شروط معينة فيه للتأكد من سلامته من العبث، ومن مصداقيته، والتأكد من توافر الثقة والطمأنينة في الأشخاص الذين يحصلون عليه.**

## المطلب الثالث

## النظام المقترح لتقدير الدليل الإلكتروني

إن السؤال الذي يمكن طرحه هو: هل من الممكن التثبت من سلامة الدليل الإلكتروني من حيث العيوب؟ وبمعنى آخر هل من الممكن أن يُضفى على الدليل الإلكتروني اليقين من خلال إخضاعه للتقييم الفني الذي يُمكنه من تفادي تلك العيوب التي تشوبه، وما موقف القاضي الجزائي من هذا الدليل إذا ما خضع لمثل ذلك التقييم؟

مثلما يخضع الدليل الإلكتروني لقواعد معينة تحكم طرق الحصول عليه، فإنه يخضع لقواعد أخرى للحكم على حجيته الإثباتية، وذلك يرجع للطبيعة الفنية لهذا الدليل، فهناك وسائل فنية من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته وصحة الإجراءات المتبعة في الحصول عليه[٢].

لذلك سنقوم بدراسة هذا المطلب في فرعين:

**الفرع الأول: القواعد الواجبة لتقييم القيمة العلمية للدليل الإلكتروني.**

**الفرع الثاني: تقدير القاضي الجزائي للدليل الإلكتروني الخاضع لإجراءات التقييم.**

---

(1) PIRAGOFF (Donald K), op, cit, P. 245.

(٢) خالد عياد الحلبي، المرجع السابق، ص ٢٤٨ – ٢٤٩.

## الفرع الأول

## القواعد الواجبة لتقييم القيمة العلمية للدليل الإلكتروني

إن مجرد الحصول على الدليل الإلكتروني وتقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة، إذ الطبيعة الفنية الخاصة للدليل الإلكتروني، تمكن من العبث بمضمونه على نحو يُحرف الحقيقة دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث، فضلاً عن ذلك فإن نسبة الخطأ في إجراءات الحصول على دليل صادق في الأخبار عن الحقيقة تبدو عالية في مثل هذا النوع من الأدلة، لذلك تثور فكرة الشك في مصداقيته كدليل للإثبات الجزائي(١).

وفي الواقع، توجد عدة وسائل يتم بها تقييم الدليل الإلكتروني، وسوف نتناول أولاً، وسائل تقييم الدليل الإلكتروني من حيث سلامته من العبث، وثانياً، من ثم وسائل تقييمه من حيث سلامة الإجراءات المتبعة للحصول عليه من الناحية الفنية.

**أولاً: تقييم الدليل الإلكتروني من حيث سلامته من العبث:**

يمكن التأكد من سلامة الدليل الإلكتروني من العبث بعدة طرق نذكر منها:

أ – يلعب علم المعلوماتية دوراً مهماً في تقديم المعلومات الفنية التي تساهم في فهم مضمون وشكل الدليل الإلكتروني، وهذه العلوم يستعان بها في كشف مدى التلاعب بمضمون هذا الدليل، وتبدو فكرة التحليل التناظري الإلكتروني من الوسائل المهمة للكشف عن مصداقية الدليل الإلكتروني، ومن خلالها تتم مقارنة الدليل الإلكتروني المقدم للقضاء، ومن خلال ذلك يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا.

---

(١) محمد نافع فالح رشدان العدواني، المرجع السابق، ص١٠٢. أ. طارق محمد الجملي، المرجع السابق، ص٦٦.

ب – في حالة عدم الحصول على النسخة الأصلية للدليل الإلكتروني أو في حالة أن العبث قد وقع على النسخة الأصلية، ففي الإمكان التأكد من سلامة الدليل الإلكتروني من التبديل أو العبث من خلال استخدام عمليات حسابية خاصة تسمى بالخوارزميات.

ج – هناك نوع من الأدلة الإلكترونية تسمى بالدليل المحايد، وهو دليل لا علاقة له بوضوح الجريمة، ولكنه يساهم في التأكد من مدى سلامة الدليل الإلكتروني المقصود من حيث عدم حصول تعديل أو تغيير في النظم المعلوماتية[١].

**ونرى أنه بهذه الطرق السالفة الذكر يمكن التأكد من سلامة الدليل الإلكتروني من العبث، والتحقق من مطابقته للواقع.**

## ثانياً: تقييم الدليل الإلكتروني من حيث السلامة الفنية للإجراءات المتبعة في الحصول على الدليل الإلكتروني:

من المعتاد بأن تتبع جملة من الإجراءات الفنية للحصول على الدليل الإلكتروني، وقد بينا بأن هذه الإجراءات من الممكن أن يعتريها خطأ قد يشكك في سلامة نتائجها، ولذا فإنه يمكن في هذا الشأن اعتماد ما يعرف باختبارات (داوبورت) كوسيلة للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل الإلكتروني من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات، ولذلك فإن أهم الخطوات الواجب إتباعها للتأكد من سلامة هذه الإجراءات من الناحية الفنية، هي:

**أ – إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج المبتغاة:**

وذلك بإتباع اختبارين رئيسين هما:

---

(١) خالد عياد الحلبي، المرجع السابق، ص ٢٤٩ – ٢٥٠. و أ. طارق محمد الجملي، المرجع السابق، ص٦٨ – ٦٩.

**١ – اختبار السلبيات الزائفة:**

ومفاد هذا الاختبار أن تخضع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الإلكتروني، وأن لا يتم إغفال بيانات مهمة عنه(١).

**٢ – اختبار الإيجابيات الزائفة:**

ومفادها أن تخضع الأداة المستخدمة في الحصول على الدليل الإلكتروني لاختبار فني يمكن من التأكد من أن هذه الأداة لا تعرض بيانات إضافية جديدة.

وبذلك يتم من خلال هذين الاختبارين التأكد من أن الأداة المستخدمة عرضت كل البيانات المتعلقة بالدليل الإلكتروني وفي ذات الوقت لم تضف إليها أي بيان جديد، وهذا يعطي للنتائج المقدمة عن طريق جهاز الحاسوب مصداقية في التدليل على الواقع(٢).

**ب – الاعتماد على الأدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم نتائج أفضل:**

تبين الدراسات العلمية في مجال تقنية المعلومات على الطرق السليمة التي يجب إتباعها في الحصول على الدليل الإلكتروني، وفي المقابل أوضحت الدراسات الأدوات المشكوك في كفاءتها، وهذا يساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات(٣).

---

(١) خالد عياد الحلبي، المرجع السابق، ص ٢٥٠.

(٢) خالد عياد الحلبي، المرجع السابق، ص ٢٥١. وأ. طارق محمد الجملي، المرجع السابق، ص ٦٩.

(٣) خالد عياد الحلبي، المرجع السابق، ص ٢٥١.

## الفرع الثاني

## تقدير القاضي الجزائي للدليل الإلكتروني الخاضع لإجراءات التقييم

إذا توافرت في الدليل الإلكتروني الشروط العامة لما يمكن أن يمثل أساساً لتأكيد الثقة فيه، فإنه من غير المعقول أن يعيد القاضي تقييم هذا الدليل وطرحه من جديد على بساط البحث، فالدليل الإلكتروني بوصفه دليلاً علمياً فإن دلالته قاطعة بشأن الواقعة المستشهد به عنها، فإذا سلمنا سابقاً بإمكانية التشكيك في سلامة الدليل الإلكتروني بسبب قابليته للعبث ونسبة الخطأ في إجراءات الحصول عليه، فتلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنهما برأي حاسم وإن لم يقطع به أهل الاختصاص، ولذلك فإذا ما توافرت في الدليل الإلكتروني الشروط السابقة بخصوص سلامته من العبث والخطأ، فإن هذا الدليل لا يمكن رده استناداً لسلطة القاضي التقديرية، إذ أن سلطة القاضي في رد الدليل استناداً لفكرة الشك يلزم لإعمالها أن يكون هناك ما يرقى لمستوى التشكيك في الدليل، وهو ما لا يستطيع القاضي الجزم به متى توافرت في هذا الدليل شروط السلامة، بحيث يقتصر دور القاضي على بحث صلة الدليل بالجريمة، ولا شك أن الخبرة تحتل في هذه الحالة دوراً مهماً في التأكد من صلاحية هذا الدليل كأساس لتكوين عقيدة القاضي، فبحث مصداقية هذا الدليل هي من صميم فن الخبير لا القاضي. وتجدر الإشارة إلى عدم الخلط بين الشك الذي يشوب الدليل الإلكتروني بسبب إمكانية العبث به أو لوجود خطأ في الحصول عليه وبين القيمة الاقناعية لهذا الدليل، فالحالة الأولى لا يملك القاضي الفصل فيها لأنها مسألة فنية فالقول فيها هو قول أهل الخبرة، فإن سلم الدليل الإلكتروني من العبث والخطأ، فإنه لا يكون للقاضي سوى القبول بهذا الدليل ولا يمكنه التشكيك في حجيته الإثباتية لكونه وبحكم

طبيعته الفنية يمثل إخباراً صادقاً عن الواقع، مالم يثبت عدم صلة الدليل بالجريمة المراد إثباتها[١].

**ونرى إنه بعد خضوع الدليل الإلكتروني لجميع الاختبارات والشروط التي تهدف إلى التأكد من سلامته من العبث وكذلك من الخطأ في الحصول عليه فإنه يصبح ذو قيمة إثباتية قاطعة وينحصر دور القاضي الجزائي في إثبات صلة هذا الدليل الإلكتروني بالجريمة المرتكبة أو عدم صلته بها.**

**وفي هذا المبحث، درسنا تقدير الدليل الإلكتروني في نظم الإثبات المختلفة، فبحثنا تقدير هذ الدليل في نظام الإثبات الحر وذلك ببحث الأسس العامة لتقدير الدليل الإلكتروني في هذا النظام ومن ثم بحثنا في موقف بعض التشريعات اللاتينية التي تتبنى هذا النظام، وكما بحثنا في تقدير الدليل الإلكتروني في نظام الإثبات المقيد ببحث الأسس العامة لتقدير هذا الدليل في هذا النظام، ومن ثم دراسة موقف التشريعات الأنكلوسكسونية التي تتبنى هذا النظام من تقدير هذا الدليل، وأخيراً بحثنا في النظام المقترح لتقدير الدليل الإلكتروني من حيث القواعد الواجبة لتقييم القيمة العلمية للدليل الإلكتروني، ومن ثم تقدير القاضي الجزائي للدليل الإلكتروني الخاضع لإجراءات التقييم.**

---

(١) خالد عياد الحلبي، المرجع السابق، ص ٢٥١ – ٢٥٢.

# خلاصة الباب الثاني

في هذا الباب الذي كان بعنوان الأحكام المترتبة على مشروعية الدليل الإلكتروني في الإثبات الجزائي، وقد قسمناه لفصلين، وبحثنا في الفصل الأول آثار مشروعية الدليل الإلكتروني في الإثبات الجزائي، فدرسنا في المبحث الأول مؤيدات عدم مشروعية الدليل الإلكتروني التي هي نوعين مؤيدات إجرائية بالنسبة للدليل الإلكتروني غير المشروع، ومن ثم المؤيدات العقابية والمدنية والتأديبية، وفي المبحث الثاني درسنا نطاق العمل بالدليل الإلكتروني، فعرضنا مفهوم الجرائم الإلكترونية بتعريفها وخصائصها وأنواعها وكما بحثنا ملاءمة الدليل الإلكتروني لإثبات الجرائم الإلكترونية والحجج التي تستند عليها هذه الملاءمة والتي تجعله هو الدليل الأفضل لإثباتها، وكذلك درسنا نطاق العمل بالدليل الإلكتروني في إثبات الجرائم التقليدية والتي هي نوعين تقليدية مختلطة وتقليدية صرفة وتوصلنا إلى أنه يمكن الاعتماد على هذا الدليل الإلكتروني لإثبات هذه الجرائم.

وفي الفصل الثاني الذي كان بعنوان تقدير الدليل الإلكتروني في الإثبات الجزائي، قسمناه لمبحثين، درسنا في المبحث الأول السلطة التقديرية للقاضي الجزائي في تقدير الدليل الإلكتروني، فدرسنا مفهوم هذه السلطة وذلك بتعريفها والضوابط التي تحكم هذه السلطة، ومن ثم بحثنا في الشروط الواجب توافرها في الدليل الإلكتروني لتقديره، وفي المبحث الثاني درسنا تقدير الدليل الإلكتروني في نظم الإثبات المختلفة، فبحثنا تقدير هذ الدليل في نظام الإثبات الحر وذلك ببحث الأسس العامة لتقدير الدليل الإلكتروني في هذا النظام ومن ثم بحثنا في موقف بعض التشريعات اللاتينية التي تتبنى هذا النظام، وكما بحثنا في تقدير الدليل الإلكتروني في نظام الإثبات المقيد ببحث الأسس العامة لتقدير هذا الدليل في هذا النظام، ومن ثم دراسة موقف التشريعات الأنكلوسكسونية التي تتبنى هذا النظام من

تقدير هذا الدليل، وأخيراً اقترحنا نظام للوصول إلى الدليل الإلكتروني بصورة مشروعة ويقينية أمام القضاء، وذلك ببحث القواعد الواجبة لتقييم القيمة العلمية للدليل الإلكتروني، ومن ثم تقدير القاضي الجزائي للدليل الإلكتروني الخاضع لإجراءات التقييم.

# الخاتمة

# *Conclusion*

تطرَّقنا في بحثنا هذا إلى مشروعية الدليل الإلكتروني في الإثبات الجزائي، وخلصنا إلى مجموعة من النتائج والمقترحات نوردها تباعاً:

**أولاً: النتائج:**

١- إن جميع التعريفات الفقهية كانت قاصرة ولا تفي بالغرض في تعريف الدليل الإلكتروني وذلك باعتبارها أنها ضيقت من نطاق الدليل الإلكتروني حيث أنها حصرت استخراج هذا الدليل من جهاز الحاسوب فقط، في حين أن الدليل الإلكتروني لا يقتصر على الدليل المستخرج من الحاسوب، بل يمتد إلى ما يستخرج من مختلف الآلات والأجهزة الرقمية.

٢- أن البيئة الإلكترونية التي نشأ فيها الدليل الإلكتروني أضفت عليه عدد من الخصائص التي تميزه عن باقي الأدلة التقليدية، وأهمها أنه دليل علمي يتميز بالموضوعية والحياد في إقناع أجهزة العدالة الجزائية.

٣- أن الدليل الإلكتروني ذو طبيعة معنوية وليست مادية لأنه دليل غير ملموس يتجسد بالمجالات المغناطيسية أو الكهربائية، ولا يغير من هذه الطبيعة المعنوية تحويله بطباعته على أوراق مادية ملموسة.

٤- أن الدليل الإلكتروني له طبيعته الخاصة التي تميزه عن غيره من أنواع الأدلة الجزائية الأخرى، ومن ثم يُعد الدليل الإلكتروني إضافة جديدة لأنواع الأدلة الجزائية الأخرى، وما يؤهله ليكون كنوع جديد يضاف إلى باقي الأدلة الجزائية، هو أن الأدلة الإلكترونية تتمتع بمجموعة من الخصائص جعلتها مختلفة عن باقي الأدلة التقليدية، والتي جعلت من غير الممكن اعتبار هذه الأدلة كطائفة من الأدلة

التقليدية، خاصة ميزة العالم الافتراضي التي يوجد فيها الدليل الإلكتروني والتي تُعد من أهم ما يميز الدليل الإلكتروني عن باقي الأدلة الجزائية.

٥- أن الأنظمة القانونية المختلفة ( المقيد والحر) قد قبلت واعترفت بالدليل الإلكتروني كدليل إثبات في المواد الجزائية، حيث لا مانع مع الاعتراف بالدليل الإلكتروني في ظل نظام الإثبات المقيد وذلك مواكبة للتطور العلمي في الإثبات الجزائي، طالما أن القاضي الجزائي هو الذي يقدر في النهاية قيمة هذا الدليل المستحدث، كما يصلح الأخذ بالدليل الإلكتروني في نظام الإثبات الحر دون وجود أي عائق في الغالب، لأن كل دليل يمكن أن يتولد منه اقتناع القاضي الجزائي يكون – من حيث المبدأ – مقبولاً أمامه، وبالتالي فليس ثمة ما يمنع من قبول الأدلة الناشئة عن الحاسوب (الدليل الإلكتروني) باعتبارها من الأساليب العلمية الحديثة في الإثبات الجزائي.

٦- هنالك صعوبات كثيرة لاستخلاص الدليل الإلكتروني منها ما يتعلق بالدليل الإلكتروني ذاته مثل عدم رؤيته، ومنها ما يتعلق بالجريمة الإلكترونية التي هي في الغالب لا تترك آثاراً مادية، ومنها ما يتعلق بالأشخاص المرتكبين لهذه الجرائم وقدرتهم الفائقة في إخفاء هويتهم من جهة، وإخفاء المعلومات من جهة أخرى، وأخيراً فإن أجهزة العدالة الجنائية سواء ما يتعلق بجمع الاستدلالات أو التحقيق الجنائي قد تعيق الحصول على الدليل الإلكتروني متى انعدمت أو نقصت خبرتها بشأن كيفية استخلاص الدليل الإلكتروني.

٧- ليس هناك صعوبة مادية لتقرير صلاحية مسرح الجريمة الذي يضم مكونات مادية لمعاينته من قبل أعضاء الضابطة العدلية والتحفظ على الأشياء التي تُعد أدلة مادية على ارتكاب الجريمة ونسبتها إلى شخص معين، والسبب في سهولة المعاينة في هذه الحالة، أنها تتم على مكونات مادية محسوسة كانت محلاً للجريمة أو تخلفت عنها، بينما هنالك صعوبة تحَّول دون فاعلية المعاينة

للمكونات المعنوية في مسرح الجريمة الإلكترونية تتمثل في ندرة الآثار المادية التي تتخلف عن الجرائم التي تقع على أدوات المعلوماتية بصفة عامة، وبرامج الحاسوب وبياناته بصفة خاصة. وكذلك تتمثل في الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال الفترة من زمان وقوع الجريمة وحتى اكتشافها أو التحقيق فيها، وأخيراً تتمثل في مشكلة زوال الدليل الإلكتروني الذي يمكن تعديله أو تغييره أو محوه في بضع ثواني.

٨- هنالك اختلاف كبير بين معاينة الجرائم التقليدية الذي يتم في العالم المادي عنه في معاينة الجرائم الإلكترونية الذي يتم في العالم الافتراضي حيث يقتضي ذلك السرعة في إجراء هذه المعاينة خشية زوال الدليل الإلكتروني والتخصص الدقيق فيمن يقومون بإجراء هذه المعاينة.

٩- لا ضير من انتقال عضو الضابطة العدلية غير المادي للاطلاع على المعلومات ومعاينتها للحصول على الدليل الإلكتروني حيث يبقى هذا الدليل مشروع ويجوز الاعتماد عليه بالحكم.

١٠- من أهم ضمانات مشروعية المعاينة الإلكترونية للحصول على الدليل الإلكتروني هي وقوع جريمة ووجود مشتبه به وإجراء المعاينة من الجهات المختصة والمؤهلة وإبلاغ المتهم بإجراء المعاينة.

١١- أن محل التفتيش الإلكتروني هو كل مكونات الحاسوب سواء أكانت مادية أو معنوية، وشبكات الاتصال الخاصة به، بالإضافة إلى الأشخاص الذين يستخدمون الحاسوب محل التفتيش وتشمل برامج النظام وبرامج التطبيقات سابقة التجهيز طبقاً لاحتياجات العميل.

١٢- أن التفتيش المتعلق بمكونات الحاسوب، يسهل إجراءه على المكونات المادية، وتأتي سهولة هذا التفتيش لأنه يقع على أشياء مادية منصوص عليها في

أغلب القوانين الإجرائية، حيث أنه لا مشكلة في تفتيش الحاسوب، متى كان التفتيش ينصب على المكونات المادية، أي على معدات الحاسوب وشاشة العرض ولوحة المفاتيح وغيرها، وفي هذا الفرض تطبق القواعد التقليدية للتفتيش.

١٣- يمكن تفتيش المكونات المعنوية أو الوسط الافتراضي وذلك لأن كلمة شيء تشمل الأشياء المادية والمعنوية وذلك حسب التفسير الغائي للنص دون التفسير الحرفي له، وبالتالي فإن تفتيش الوسط الافتراضي يُعد صحيحاً وفقاً للقانون كما أن البيانات بذلك الوسط يصح ضبطها.

١٤-لا يجوز قانوناً إجبار المتهم على طباعة ملفات بيانات مخزنة داخل نظام المعالجة الآلية للمعلومات، أو إلزامه بالكشف عن الشفرات أو كلمات السر الخاصة بالدخول إلى هذه المعلومات، ذلك أن القاعدة الأساسية أنه لا يجوز إلزام الشخص باتهام نفسه، سواء عن طريق الشهادة، أو عن طريق تقديم عناصر الإثبات، كما أنه من حق المتهم الامتناع عن الإجابة أو الاعتصام بالصمت دون أن يؤخذ ذلك على أنه إقرار بصحة الاتهام والتسليم بأدلته، إلا أنه يجوز إجباره على تسليم مفتاح الخزينة التي يوجد فيها النظام المعلوماتي.

١٥- أن الشاهد أو القائم على تشغيل النظام المعلوماتي يلتزم بالكشف عن الشفرات أو كلمات السر التي يكون على علم بها، ولا يعفيه من هذا الالتزام سوى الاعتصام باحترام السر المهني.

١٦- أخذت أغلب التشريعات ومنها التشريع السوري بجواز امتداد تفتيش حاسوب المتهم المتصل بحاسوب أو مُخدّم موجود داخل الدولة إذا كان هناك أساس يدعو إلى الاعتقاد بأن البيانات المطلوبة قد تمّ تخزينها في نظام ذاك الحاسوب.

١٧- أن في حضور المشتبه به أو صاحب المحل أو المسكن أو من ينوب عنهما أو الشهود إجراء التفتيش فيه ضمانة أكيدة لنتائج التفتيش الواقعة على نظم

الحاسوب والإنترنت، لأنه يتيح للمشتبه به فرص مواجهة الدليل المستمد منه، وذلك في سبيل تحقيق التوازن المنشود بين مصلحة المشتبه به ومصلحة العدالة.

١٨- إن ضبط المكونات المادية للحاسوب والممثلة بمعدات الحاسوب والإنترنت وكابلات الشاشة وشاشة العرض ومفاتيح تشغيله، يمكن أن يطبق بصددها ذات القواعد التقليدية للضبط دون أدنى صعوبة.

١٩- عدم كفاية الإجراءات التقليدية للحصول على الدليل الإلكتروني، وضرورة إتباع إجراءات حديثة تتماشى مع طبيعة كل من الدليل الإلكتروني، والجرائم الإلكترونية.

٢٠- إن المراقبة الإلكترونية تُعد اعتداء على حرية الحديث الذي هو حق من الحقوق اللصيقة بالشخصية الإنسانية وتدخل في حياته الخاصة، ودون خصوصية الحديث يصبح الفرد متردداً خائفاً من ممارسة حقه والحديث عبر وسائل الاتصال الحديث، وذلك فيه مساس بأهم الحقوق اللصيقة بالإنسان تكمن في أنها تكشف أدق أسرار الأشخاص دون علمهم، وتمتد إلى كشف أسرار كل شخص يتصل بالشخص المراقب. ألا أنه يمكن السماح به في أحوال ضيقة، وأن يكون في نطاق ضيق، لأن إجراء المراقبة الإلكترونية مهم ويقوم بدور فعال للحصول على الدليل الإلكتروني، وذلك لعدم كفاية الإجراءات التقليدية للحصول على هذا الدليل والتي لا تتناسب مع طبيعته، ولكن لابد من إحاطة هذا الإجراء بضمانات عدة ولا سيما تحديد نوع الحديث المراد التقاطه، والجريمة المتعلقة بها، والجهة المصرح لها بذلك، وتحديد مدة المراقبة، وكل هذه الضمانات تكفل مشروعية الحصول عل الدليل الإلكتروني.

٢١- أن التشريعات قد رتبت على الإجراء غير المشروع بطلانه وكذلك بطلان الدليل الإلكتروني أي استبعاد هذا الدليل المتحصل بطريقة غير مشروعة.

٢٢-لا يترتب على بطلان الإجراءات أي أثر على الإجراءات السابقة لها، وبالتالي تبقى منتجة جميع آثارها، كما أنه لا يترتب على بطلان الإجراءات أي أثر على الإجراءات اللاحقة لها، إلا إذا كانت هذه الإجراءات ترتبت عليها مباشرة.

٢٣- يترتب على مخالفة الضمانات القانونية في الحصول على الدليل الإلكتروني قيام المسؤولية العقابية والمدنية والتأديبية للجهات المختصة المكلفة بالقيام بإجراءات الحصول على الدليل الإلكتروني.

٢٤- أن قاعدة استبعاد الأدلة الإلكترونية المتحصلة بطرق غير مشروعة أي تقرير بطلانها هو الوسيلة المثلى لاحترام حقوق الإنسان وحرياته المنصوص عليها في جميع الدساتير والقوانين، وذلك لأن الوسائل الأخرى لا تحول دون قيام رجال السلطة العامة من انتهاك حقوق الأفراد وحرمة حياتهم الخاصة، إذ من النادر من الناحية العملية أن يُقدم أحدهم إلى القضاء، وأن يوقع عليه جزاء، سواء أكان عقابياً أم مدنياً أم إدارياً، ولهذا كان استبعاد الأدلة الباطلة أكثر جدوى، لأن علم رجال السلطة العامة سلفاً بنتيجة الإجراء الباطل الذي يقوم به وهو طرح القضاء للدليل وعدم الأخذ به كفيل بحمله على الكف عن مخالفة القانون حتى لا يذهب جهده سدى.

٢٥- على الرغم من المحاولات الفقهية لوضع تعريف للجرائم الإلكترونية إلا أنها جميعها كانت قاصرة لأنها تعتمد على معيار واحد، ولم تستطع من وضع تعريف جامع مانع، وهذا مرده إلى أن هذا النوع من الجرائم معقد وصعب وفي تطور دائم.

٢٦- أن الدليل الإلكتروني هو الأكثر ملاءمة والأفضل لإثبات الجرائم المستحدثة وعلى رأسها الجرائم الإلكترونية، لكنه ليس الدليل الوحيد لإثبات هذه الجرائم، فيمكن التعويل على اعتراف المتهم بارتكابه جريمة إلكترونية والذي أدلى به عقب القبض عليه واستجوابه من قبل سلطة التحقيق ومواجهته، كما أن الخبرة يمكن أن

تكون دليل لإثبات الجرائم الإلكترونية بالاستعانة بخبير معلوماتي، كما يعترف الفقه وخاصة الفقه الفرنسي والمصري مثال على ذلك الشاهد المعلوماتي، فيمكن لجهة التحقيق أن تستمع إلى الشاهد المعلوماتي والشهادة دليل إثبات تقليدي يمكن أن يعول عليه لإثبات الجرائم الإلكترونية، والصحيح أن بعض الجرائم الإلكترونية قد لا يتوافر فيها أدلة تقليدية، إلا إنه لا يمكن بأي حال من الأحوال تعميم الفكرة ورفض الأدلة التقليدية في مجال الجرائم الإلكترونية.

٢٧- من أهم الحجج لملاءمة إثبات الجريمة الإلكترونية بالدليل الإلكتروني، هو الطبيعة الخاصة التي تتميز بها الجرائم الإلكترونية والمستمدة من ارتكاب هذه الجرائم في العالم الافتراضي وليس المادي مما يمكن أن يكون دليل إثباتها أي الدليل الإلكتروني من الطبيعة ذاتها.

٢٨- لا تلازم بين نطاق العمل بالدليل الإلكتروني ومشكلة إثبات الجريمة الإلكترونية، فمن ناحية فإن الدليل الإلكتروني مثلما يصلح لإثبات الجريمة الإلكترونية ويُعد في ذات الوقت الدليل الأفضل لإثباتها، فإنه من ناحية أخرى لا يقتصر دور الدليل الإلكتروني في الإثبات على الجريمة الإلكترونية بالمفهوم الضيق، فهو يصلح لإثبات الجرائم التقليدية المختلطة المرتكبة بواسطة الحاسوب مثل جرائم غسل الأموال أو تهريب المخدرات، وعلى الرغم من عدم اتصال الجريمة بالحاسوب إلا من حيث الوسيلة لارتكاب الجريمة في مثل هذه الحالات فإن الدليل الإلكتروني يصلح ليكون دليلاً لإثباتها، كما أن الدليل الإلكتروني يصلح ويمكن أن يُعول عليه في إثبات الجرائم التقليدية الصرفة، فمثلاً يمكن إثبات جرائم السرقة والاختلاس التقليدية عن طريق أدلة إلكترونية والتي تكون عبارة عن مستندات إلكترونية متعلقة بالمحاسبات أو مراسلات إلكترونية بين الجاني وشخص آخر.

٢٩- أن الدليل الإلكتروني يخضع للسلطة التقديرية للقاضي الجزائي، فإن استراح إليه ضميره، ووجده كافي ومنطقي، أمكنه أن يستمد اقتناعه منه، ويعول عليه في الحكم الذي ينتهي إليه شأنه شأن باقي أدلة الإثبات، ولا يمكن للخبير مهما كانت دقة نتائجه وموضوعيتها أن يحتل مكانة القاضي، ألا أن السلطة التقديرية للقاضي الجزائي لا يمكن أن تكون مطلقة بل هنالك ضوابط وأطر معينة يتعين أن تمارس هذه السلطة في نطاقها وهذه الضوابط هي: الضابط الأول: بلوغ الاقتناع القضائي درجة اليقين، والضابط الثاني: مواءمة الاقتناع القضائي لمقتضيات العقل والمنطق، والضابط الثالث: تقيد القاضي الجزائي بسلامة التقدير والاستدلال.

٣٠- من أهم الشروط الواجب توافرها في الدليل الإلكتروني ليخضع للسلطة التقديرية للقاضي الجزائي هي شرط يقينية الدليل الإلكتروني وشرط وجوب مناقشة الدليل الإلكتروني وشرط مشروعية الدليل الإلكتروني.

٣١- إذا لم يصل القاضي الجزائي إلى مرحلة الاقتناع اليقيني بالدليل الإلكتروني المعروض أمامه بإدانة المتهم فإنه لا يستطيع أن يدحض براءته ويحكم بإدانته، وذلك لأن قرينة البراءة لا تدحض إلا باقتناع القاضي اليقيني.

٣٢- أن القاضي الجزائي ليس له أن يأخذ بالدليل الإلكتروني سواء أكان دليل إدانة أو براءة إذا لم يكن قد عرض أثناء المرافعات ولم يناقشه الأطراف في الدعوى، ولا بد من أن يمثل الشهود المعلوماتيين ويعيدوا أقوالهم مرة ثانية أمام المحكمة، وكذلك ضرورة أن يمثل خبراء الأنظمة المعلوماتية – على اختلاف تخصصاتهم – أمام المحاكم لمناقشتهم أو مناقشة تقاريرهم التي خلصوا إليها لإظهار الحقيقة.

٣٣- يترتب على مناقشة الأدلة الإلكترونية نتيجتان:

النتيجة الأولى: عدم جواز أن يقضي القاضي في الجرائم الإلكترونية بناءً على معلوماته الشخصية.

والنتيجة الثانية: ضرورة التأهيل التقني والفني للقضاء لمواكبة المناقشة العلمية للأدلة الإلكترونية بشكل ينسجم مع التقارير التي تم تقديمها في المؤتمرات الخاصة بجرائم الحاسوب والإنترنت.

٣٤- يمكن أن يكون الدليل الإلكتروني غير مشروع وذلك لتقرير براءة المدعى عليه لأن شرط مشروعية الدليل لا يتطلب في دليل البراءة بل يقتصر على دليل الإدانة نظراً لخطورته فكان لا بد أن يكون هذا الدليل مشروع.

٣٥- لم ينظم المشرع السوري في قانون أصول المحاكمات الجزائية السوري شرط يقينية الدليل الإلكتروني وإن كان نظمه في قانون مكافحة الجريمة الإلكترونية وكذلك لم ينظم شرط مناقشة الدليل الإلكتروني وأيضاً شرط مشروعة الأدلة سواء بالنسبة للأدلة التقليدية بشكل عام أم بالنسبة للدليل الإلكتروني بشكل خاص.

٣٦- أن الدليل الإلكتروني في نظام الإثبات الحر يخضع لتقدير القاضي وفقاً لقناعته القضائية كباقي الأدلة، لكن سلطة القاضي التقديرية للدليل الإلكتروني في ظل نظام الإثبات الحر لا تتناول قيمة هذا الدليل العلمي، ذلك أن قيمته تقوم على أسس وأصول وحقائق علمية تتميز بالثبات والاستقرار والثقة في مصادرها العلمية، الأمر الذي يصعب معه، بل قد يستحيل – على القاضي – أن يتناولها بالفحص والتقدير. وذلك بخلاف الظروف والملابسات التي وجد فيها الدليل الإلكتروني، فإنها تدخل بطبيعتها في نطاق التقدير الذاتي للقاضي الجزائي، بحيث يكون في استطاعته أن يطرحه – على الرغم من اقتناعه بقطعيته – إذا تبين له أنه لا يتفق مع ظروف الواقعة وملابساتها.

٣٧- لا يتم قبول الدليل الإلكتروني في نظام الإثبات المقيد كدليل إذا لم يستكمل باختبارات الثقة للتأكد من صحته ودقته وصحة وكفاءة الحاسوب المستخرج منه وكان القائم عليه تتوافر فيه الثقة والاطمئنان.

٣٨- أن التشريعات الأنكلوسكسونية (الأمريكي والبريطاني والكندي) اعترفت بحجية الدليل الإلكتروني أمام القضاء ولكن بعد خضوعه لاختبارات معينة أو توافر شروط فيه للتأكد من سلامته من العبث، ومن مصداقيته، والتأكد من توافر الثقة والطمأنينة في الأشخاص الذين يحصلون عليه.

**ثانياً: المقترحات:**

بناءً على ما تقدَّم من نتائج فإنّنا نورد عدة مقترحات في محاولة منا لتقديم بعض الحلول التي تسهم في تعزيز الضمانات التي يتوجب أن يتمتع بها المُدَّعى عليه تجاه إجراءات الحصول على الدليل الإلكتروني، وكذلك معالجة كل الأحكام التي تنشأ عن استخدام الدليل الإلكتروني في الإثبات الجزائي ولاسيما مؤيدات عدم مشروعيته أن كان بالنسبة للدليل الإلكتروني غير المشروع أو بالنسبة للأشخاص الذين يحصلون عليه بطرق غير مشروعة، وكذلك نطاق العمل به، وأخيراً تقديره أمام القضاء الجزائي، وهذه المقترحات:

١- ضرورة تعديل قانون أصول المحاكمات الجزائية السوري بحيث يضاف له موضوع الأخذ بالدليل الإلكتروني كدليل إثبات في جميع الجرائم، والأخذ به بطبيعته المعنوية أي بدون وضع هذا الدليل أو استخراجه بشكل مطبوع مادياً، وكذلك إجراء تعديل في القوانين التي لا تأخذ بالدليل الإلكتروني في الإثبات الجزائي والنص عليه بشكل صريح.

٢- على التشريعات الجزائية ولا سيما التشريع السوري وضع نصوص قانونية تجرم التخلص من الأدلة الإلكترونية، وفي حال وجودها نطالب باعتبار أن

التخلص من هذه الأدلة ظرف تشديد وذلك نظراً لإمكانية التخلص منها بشكل أكبر وأكثر شيوعاً من الأدلة التقليدية.

٣- من أجل التصدي لصعوبات نقص الخبرة في الحصول على الدليل الإلكتروني، نقترح ضرورة إقامة دورات تدريبية لتأهيل أعضاء الضابطة العدلية وقضاة التحقيق والحكم، وإمدادهم بالخبرة المطلوبة اللازمة بكيفية استخلاص الدليل الإلكتروني، وحفظه، وكيفية تحليل الدليل الإلكتروني، وإعادة بناء الأدلة المهمشة، وكيفية إعداد التقارير الجنائية، وكيفية تقديمها في قالب إثبات تعتمده أجهزة العدالة الجزائية، ومن الممكن أن يتم ذلك التدريب من خلال عقد دورات تدريبية أو مؤتمرات أو ابتعاث العاملين في أجهزة إنفاذ القانون بعثات علمية للحصول على درجات علمية متخصصة في البحث والتحقيق الجنائي الإلكتروني.

٤- ضرورة عُد الإقدام على التشفير بدون ترخيص جريمة يعاقب عليها القانون، وأيضاً نقترح بمعاقبة الشخص الذي أعد برنامج التشفير بدون ترخيص.

٥- من أجل تفعيل عملية الإبلاغ عن الجريمة الإلكترونية، ومن ثم المساهمة بطريقة إيجابية في منع وقوع الجريمة أو سرعة تحصيل الدليل المتعلق بها، فلا بد من تشجيع المجني عليهم في هذه الجرائم على الإبلاغ عنها فور وقوعها، وذلك بإبلاغ جهة خاصة، أو إبلاغ سلطات إشرافية، وتشكيل أجهزة خاصة لتبادل المعلومات، وكذلك إصدار شهادة "أمن خاصة" تمنح بعد عمل مراجعة وتدقيق من قبل هيئة خاصة من المراجعين، ويتعين على هذه الهيئة إبلاغ الشرطة بما تكشفه من جرائم.

٦-لحل مشكلة الاختصاص في داخل إقليم الدولة فإنها تحل على أساس مكان القبض على المتهم أو محل إقامته أو مكان وقوع الجريمة، فأي مكان من الأماكن المذكورة، ينعقد الاختصاص القضائي لسلطات التحقيق والمحاكمة فيه بالجريمة الإلكترونية، ولكن على المستوى الدولي فإن الأمر في حاجة لعقد اتفاقيات دولية

ثنائية أو جماعية وتفعيل الإنابات القضائية. ولحل مشكلة ضعف التعاون الدولي في مجال الجريمة الإلكترونية ولا سيما في مجال تبادل الأدلة الإلكترونية، فإن الحاجة ماسة إلى إصدار تشريعات جزائية أكثر مرونة تسمح بسرعة التعاون المثمر في تبادل الأدلة الإلكترونية.

٧- ضرورة جعل ندب الخبرة في الجريمة الإلكترونية وجوبياً من أجل الحصول على الدليل الإلكتروني نظراً لأن طبيعة هذه الجريمة تستلزم التعامل معها بطريقة حرَّفية أو فنية تفوق قدرات فريق التحقيق غير المؤهل، وذلك عن طريق تعديل قوانين الأصول الجزائية التي تجعل من ندب الخبراء أمراً جوازياً.

٨- ضرورة تقديم الإخبار أو الشكوى عبر الإنترنت لأنه يسّهل عملية إعلام السلطات المختصة بوقوع الجريمة، كما يؤمّن الحماية لمقدم الإخبار الذي يظلّ مجهولاً في أغلب الأحيان، ونظراً لعدم معالجة المشرع السوري مسألة الإخبار عن الجرائم الإلكترونية عبر الإنترنت، نقترح على أجهزة العدالة السورية أن تنشأ مواقع إلكترونية متخصصة في تلقي الإخبارات والشكاوى المتعلقة بالجرائم الإلكترونية.

٩- ضرورة تأهيل رجال الضابطة العدلية على التعامل مع مسرح الجريمة الإلكتروني، كما له أثر كبير في سهولة الحصول على الدليل الإلكتروني وكذلك في عدم اتلافه، ونقترح بجواز أن يلتمس المشتبه به في المعاينة من القاضي أن يصرح له بتعيين خبير فني متخصص في الانترنت ليكون بصحبة المحقق في حال كان غير مؤهلاً، ذلك حتى يمنع أي تشكيك في صحة الدليل المستمد من المعاينة.

١٠-ضرورة تدخل قوانين الأصول الجزائية بشكل واضح لأجل تطبيق الإجراءات الخاصة بالوثائق التقليدية وتطبيقها على المعلومات الموجودة في أجهزة الكومبيوتر والنص صراحة على جواز تفتيش المكونات المعنوية.

١١- ضرورة امتداد تفتيش حاسوب المتهم المتصل بحاسوب أو مُخدّم موجود في مكان آخر داخل الدولة، لكن بشرط أن يكون الدخول للنهاية الطرفية الخاصة بغير المتهم لا يحتاج لكلمة مرور خاصة لا يستعملها غيره (شفرة)، وأن يكون نظام الحاسوب الآخر ضمن النطاق الإقليمي للدولة وأن يكون ذلك التفتيش ضرورياً لإظهار الحقيقة، ولا بد أن يكون أمر هذا التفتيش مسبب بإيراد الأسباب الذي دعت له.

١٢- ضرورة السماح بتفتيش الحاسوب أو المُخدّم الموجود في مكان آخر خارج الدولة فيما إذا لم يكن النظام المعلوماتي محمي بنظام شفرة للدخول للمعلومات، حيث أن النظام المعلوماتي لا يعرف الحدود والوحدة التي يتميز بها، هي التي تعطي للجهة القائمة بالتفتيش سلطة الولوج وتتبع المعلومات ولو امتد نشاطها لطرف نظام معلوماتي في دولة أخرى وذلك لا ينتهك سيادة الدولة، أما في حال وجود نظام شفرة للدخول للمعلومات، فنرى أنه لا يجوز تفتيش هذا النظام المعلوماتي لتلك الدولة، ولذلك نرى أن السبيل لحل تلك المشكلة هو تعزيز التعاون الدولي وذلك من خلال تعزيز دور الإنابة المتبادلة بين الدولة المحققة والدولة التي يراد التفتيش فيها.

١٣- ضرورة عدم تحديد مدة لتنفيذ التفتيش الواقع على نظم الحاسوب والإنترنت، فمن جهة أولى، هذا النوع من التفتيش يختلف في محله عن التفتيش التقليدي، حيث يقع هذا التفتيش على مكونات الحاسوب المادية والمعنوية ولاسيما إذا ما كان هنالك كم هائل من البيانات التي يتطلب تفتيشها وقت طويل، ومن جهة ثانية، يستلزم هذا التفتيش بعض الإجراءات المعقدة فيما إذا كانت العناصر المكونة للجريمة موجودة في بلد آخر الأمر الذي يقتضي الحصول على إذن من هذه الدولة بالتفتيش أو إعطائها إنابة قضائية وهذا كله يتطلب وقت طويل جداً.

١٤- نقترح بجواز أن يقع التفتيش في إطار تفتيش نظم الحاسوب والإنترنت على غير المتهم لكن بشرط أن يكون إجراء التفتيش قد تم بناء على أدلة قوية ولا يكفي أن تشير الدلائل إلى أن في حوزته أشياء تظهر الكشف عن الحقيقة.

١٥- ضرورة توسيع سلطات الجهة المعنية بإجراء التفتيش، ولو استلزم الأمر ولوج النظام المعلوماتي دون الحصول على إذن عند الضرورة، إذا كان من شأن انتظار صدور الإذن أن يفوت فرصة الحصول على الدليل الإلكتروني.

١٦- وضع استثناء على ضمانة حضور المشتبه به أو صاحب المحل أو المسكن أو من ينوب عنهما أو الشهود لإجراء التفتيش في حالة الخشية من العبث بالدليل أو للإفلات من الاتهام أو تهديد أحد الشهود أو الإضرار بسير التحقيق أو تأخير المحاكمة.

١٧- عدم تحديد وقت معين لتنفيذ التفتيش في إطار تفتيش نظم الحاسوب والإنترنت فقط، وذلك لأجل الحصول على الدليل الإلكتروني قبل التلاعب فيه أو إتلافه من قبل المجرمين.

١٨- بالرغم من أن كل من المعاينة والتفتيش من إجراءات التحقيق، والهدف منهما جمع الأدلة التي تثبت وقوع الجريمة ونسبتها إلى المتهم، إلا أن المعاينة بطبيعتها لا تشكل مساساً بأسرار وحقوق الأفراد وحرمتهم، سواء تعلقت بالأشخاص أو الأشياء أو الأماكن بالقدر الذي يمثله التفتيش الذي هو إجراء يمس بمستودع أسرار المتهم وحرمته سواء انصب على شخصه، أو مسكنه أو أمتعته لذلك يتوجب إحاطة التفتيش بضمانات قانونية بشكل أكبر من المعاينة لضمان مشروعية الحصول على الدليل الإلكتروني.

١٩- لابد من تطوير النصوص القانونية المتعلقة بالضبط، لتشمل إمكانية ضبط معطيات الحاسوب والبيانات المعالجة إلكترونياً.

٢٠- ضرورة تطوير قواعد الضبط لتتلاءم مع طبيعة البريد الإلكتروني وتخصيص إجراءات تتصف بالمرونة والسرعة تفوق الإجراءات الخاصة بالبريد العادي لضبط هذا البريد وذلك نظراً لسهولة التخلص من الأدلة الإلكترونية الموجودة فيه.

٢١- ضرورة الاستغناء عن طلب الإذن لضبط الأدلة الإلكترونية في الجرائم الإلكترونية استثناءاً وذلك خشية محو وطمس الدليل بسهولة، ومن ثم يكون من الصعب ملاحقة المجرم أو كشف شخصيته.

٢٢- يجب تحديث الأساليب الإجرائية التقليدية في قانون أصول المحاكمات الجزائية السوري من خبرة معاينة وتفتيش وضبط لتستوعب الحصول على الدليل الإلكتروني وتحديثها على نحو يكفل استجابتها بشكل كاف للحصول على هذا الدليل المستحدث، وبغير أن تتعرض حقوق الإفراد وحرياتهم للخطر عند الإثبات به.

٢٣- ضرورة اعتماد نماذج المحاكاة الحاسوبية لمسرح الجريمة الإلكتروني في المعاينة والتفتيش وذلك من خلال قيام خبراء البحث الجنائي بالمشاركة مع مصممي نماذج المحاكاة بإعداد نماذج تصور الواقع الحقيقي لإجراءات المعاينة والتفتيش وما يتم أثناء عمليات المعاينة والتفتيش والواجب مراعاته من قبل القائم بها وبيان الأخطاء الشائعة التي يقع بها.

٢٤- سَنّ القوانين والأنظمة الخاصَّة التي تسدُّ كافَّة ثغرات الحصول على الدليل الإلكتروني، ولا سيما الاهتمام بالإجراءات الفنية الحديثة للحصول على الدليل الإلكتروني كونها تساعد كثيراً في اكتشاف الدليل الإلكتروني، وحفظه، حيث أن الطرق العلمية والفنية للحصول على الدليل الإلكتروني قد أصبحت هي الأكثر فاعلية للحصول على هذا الدليل.

٢٥-نظراً لأهمية تقييد التحفظ المعجل على البيانات المخزنة بمدة معينة لكونه من أهم ضمانات مشروعية إجراءه، لذلك نقترح على المشرع السوري الأخذ بهذه الضمانة لما فيها من حماية أكبر لحق خصوصية الفرد.

٢٦- ضرورة إحاطة الإجراءات المتعلقة بالبيانات الساكنة، بضمانات معينة تكفل مشروعية الدليل الإلكتروني وأهم هذه الضمانات، وقوع جريمة معينة وأن تكون هذه الجريمة من نوع الجناية والجنحة فقط دون المخالفات، والاشتباه بالمدعى عليه أنه مرتكب الجريمة، وإعطاء هذه السلطة لسلطة التحقيق فقط دون غيرها لخطورة هذا الإجراء.

٢٧- بالنسبة لتحديد خصوصية المكالمة الهاتفية وتسجيل المحادثات الشخصية، نقترح بضرورة تبني معيار طبيعة الكلام وعدم الأخذ بمعيار طبيعة المكان، وذلك لأن حرمة المحادثات ينبغي أن تصان سواءً أكانت في مكان خاص أم عام، وأن المحادثات الهاتفية هي بطبيعتها سرية، ولها خصوصية بصرف النظر عن المكان الذي يجري فيه الحديث الهاتفي.

٢٨-نقترح بعدم جواز إجراء المراقبة الإلكترونية إلا في الجنايات والجنح أما المخالفات فلا يمكن أن يبرر إجراء المراقبة الإلكترونية فيها نظراً لبساطتها والتي تمنع انتهاك حرمة الاتصالات الإلكترونية، ولا يكفي ذلك بل لابد من تحديد الجنايات والجنح كما فعل المشرع الجزائري على أن يكون معاقباً عليها بحد أدنى من العقوبة لتجوز فيها المراقبة الإلكترونية.

٢٩-ضرورة تسبيب الإذن الصادر بشأن مراقبة الاتصالات الإلكترونية بالنظر إلى أهمية التسبيب كضمانة مهمة لتبرير هذه المراقبة.

٣٠- ضرورة مراعاة الإجراءات التقليدية والفنية الحديثة للحصول على الدليل الإلكترونية جميع الضمانات المنصوص عليها في القوانين والدساتير والمواثيق الدولية، وذلك من أجل الحصول على دليل إلكتروني مشروع يمكن الاعتماد عليه أمام أجهزة تنفيذ العدالة الجزائية، ويكون ذلك عن طريق تدريب القائمين بهذه

الإجراءات سواء التقليدية (الخبرة– المعاينة – التفتيش – الضبط)، والفنية الحديثة ولا سيما المراقبة الإلكترونية على إتباع إجراءات صحيحة ومشروعة لا تمس حقوق الأفراد أو حرياتهم وتضمن بنفس الوقت مصلحة المجتمع في أن تبقى حقوقه مصونة ومحمية من جميع المجرمين الذي قد يعتدوا عليه.

٣١– ضرورة تقرير بطلان الإجراء غير المشروع للحصول على الدليل الإلكتروني الذي خالف ضمانات إجراءه، ذلك لأنه لا يجوز الاستناد على إجراء غير مشروع ينتهك حقوق وحريات المشتبه به، وإلا أصبح مبدأ المشروعية الإجرائية حبراً على ورق.

٣٢– يجب التمييز بين الضمانات الموضوعية والضمانات الشكلية لإجراء التفتيش، فالضمانات الموضوعية للتفتيش تشكل ضمانات جوهرية ويترتب على مخالفتها بطلان مطلق متعلق بالنظام العام لأنه تتعلق بالمصلحة العامة وحسن سير العدالة، أما الضمانات الشكلية فيترتب عليها بطلان نسبي متعلق بمصلحة الخصوم، أما بالنسبة لطبيعة بطلان الإجراءات التقليدية الأخرى للحصول على الدليل الإلكتروني من خبرة ومعاينة وضبط، وكذلك طبيعة بطلان الإجراءات المتعلقة بالبيانات الساكنة (التحفظ المعجل – تقديم بيانات عن المشترك) باستثناء الإجراءات المتعلقة بالبيانات المتحركة (المراقبة الإلكترونية)، فيكون البطلان نسبي متعلق بمصلحة الخصوم وذلك لأن هذه الإجراءات لا تبلغ في خطورتها إجراء التفتيش الذي يعد من أخطر الإجراءات التقليدية للحصول على الأدلة لأنه يقع على مستودع السر وينتهك حريات الأفراد وحياتهم الخاصة. أما بالنسبة لعدم مراعاة ضمانات المراقبة الإلكترونية التي تُعد بحق إجراء خطير ينتهك حق الفرد في أن تبقى أحاديثه الشخصية مصانة ومحمية يترتب عليها البطلان المطلق وهذا البطلان متعلق بالنظام العام ويجوز إثارته في أي مرحة من مراحل الدعوى.

٣٣– ندعو المشرع السوري أن يقوم بسن نصوص عقابية وإجرائية تتكفل بحماية الحياة الخاصة المخزونة في الحاسوب والإنترنت، بحيث تمنع اقتحام الملفات

الشخصية دون سند قانوني، حماية للحقوق والحريات الفردية التي كفلها الدستور السوري بالإضافة إلى المواثيق الدولية.

٣٤-ضرورة تعريف الجريمة الإلكترونية حسب المعيار الموضوعي والفني معاً، لأنهما يصلحان معاً لكل الجرائم الإلكترونية بأنها: " سلوك إيجابي أو سلبي يقع بواسطة الحاسوب الإلكتروني أو أي جهاز تقني آخر أو بواسطة شبكة الإنترنت ويكون السلوك فيها مستهدفاً المكونات المعنوية كالبرامج والبيانات والمعلومات الإلكترونية".

٣٥- ضرورة تنظيم المشرع السوري في قانون أصول المحاكمات الجزائية السوري كيفية إثبات صحة الدليل الإلكتروني بالنص على الشروط الواجب توافرها في هذا الدليل كشرط يقينية هذا الدليل وضرورة خضوعه للمناقشة وكذلك مشروعيته.

٣٦- ضرورة قبول الدليل الإلكتروني غير المشروع في أحكام الإدانة في الجرائم التي تهدد الدولة في كيانها ووجودها كالجرائم الإرهابية وجرائم أمن الدولة الداخلي والخارجي حفاظاً على المصلحة العامة.

٣٧- ضرورة إنشاء مخابر للأدلة الإلكترونية والتي تستخدم لفحص الأدلة الإلكترونية وذلك لبيان مشروعية الحصول عليها ومصداقيتها للقبول أمام المحاكم الجزائية، وهذا يتطلب مايلي:

* **متطلبات بشرية:** ويتمثل ذلك في ضرورة تدريب وتأهيل جميع أجهزة تنفيذ القانون من ضابطة عدلية وقضاة تحقيق وقضاة حكم على التعامل مع هذه الأدلة نظراً لطبيعتها الخاصة والمختلفة عن الأدلة التقليدية، كما لابد من إنشاء فرع جديد في معامل الأدلة الإلكترونية يتم تدريسها في معاهد مختصة يهتم بدراسة الأدلة الإلكترونية.

* **متطلبات قانونية:** ويتمثل ذلك في ضرورة تعديل قوانين أصول المحاكمات الجزائية ليشمل الأدلة الإلكترونية، ولاسيما كيفية اعتماد الدليل الإلكتروني في المحاكم.

* **متطلبات تقنية:** ويتمثل ذلك بضرورة تزويد هذه المعامل بأحدث الأجهزة أو المعدات أو التقنيات الحديثة التي يتوصل إليها العلم لفحص الأدلة الإلكترونية وذلك للحصول على دليل إلكتروني ذو قيمة علمية ولتنقية هذه الأدلة من أي خطأ قد يشوبها.

٣٨- في نهاية هذا البحث نقترح من أجل الوصول إلى دليل إلكتروني مقبول ومشروع في الإثبات الجزائي وأيضاً يتمتع بحجية أمام القضاء الجزائي، فلا بد من أن نتبع مايلي:

- أن يتم الحصول على الدليل الإلكتروني بطريق مشروع وذلك ضمن ضمانات قانونية إجرائية ذات مشروعية تضمن سلامة وصحة ودقة هذا الحصول وتراعي عدم التعرض والعصف بحقوق وحريات الأفراد.

- ضرورة خضوع الدليل الإلكتروني كونه دليل علمي لاختبارات الثقة، والمقصود بذلك أن يتم التأكد من حجية هذا الدليل بإجراء اختبارات الثقة، وألا يتم قبول الدليل الإلكتروني كدليل إثبات جزائي إذا لم يستكمل اختبارات الثقة وذلك للتأكد من صحته ودقته وصحته وكفاءة جميع الأجهزة الإلكترونية المستخلص منها، وكذلك مدى توافر الدقة والاطمئنان في الشخص القائم على عملية الحصول على الدليل الإلكتروني.

- أن يناقش القاضي الجزائي جميع الظروف والملابسات التي وجد فيها الدليل الإلكتروني.

- بعد خضوع الدليل الإلكتروني لجميع الاختبارات والشروط التي تهدف إلى التأكد من سلامته من العبث وكذلك من الخطأ في الحصول عليه فإنه يصبح ذو قيمة إثباتية قاطعة وينحصر دور القاضي الجزائي في إثبات صلة هذا الدليل الإلكتروني بالجريمة المرتكبة أو عدم صلته بها.

**مشروع قانون يتضمن تعديل وإضافة مواد قانونية إلى قانون أصول المحاكمات الجزائية السوري الصادر بالمرسوم ١١٢ تاريخ ١٩٥٠/٣/١٣م، وقانون**

**مكافحة الجريمة المعلوماتية وتنظيم التواصل عبر الشبكة السوري رقم (١٧) لعام ٢٠١٢م، يتضمن مايلي:**

**أولاً: في قانون أصول المحاكمات الجزائية السوري الصادر بالمرسوم ١١٢ تاريخ ١٩٥٠/٣/١٣م:**

١- إضافة مادة قانونية حول إلزامية الخبرة في الجرائم الإلكترونية على أن يكون نصها كالتالي: " يجب على موظفي الضابطة العدلية وقضاة التحقيق الإستعانة بخبير إلكتروني في حال كانت الجريمة إلكترونية".

٢- إضافة نص قانوني في التشريع السوري يُلزم الشاهد والعاملين على النظم المعلوماتية بالمعاونة الفعالة مع سلطات التحقيق، ويكون نصه كالتالي:

"على الشاهد والعاملين على النظم المعلوماتية بالمعاونة الفعالة مع سلطات التحقيق عن طريق إمدادهم بالشفرات أو كلمات السر اللازمة لتفتيش البيانات اللازمة لأجل الحصول على الدليل الإلكتروني على أن يستثنى من ذلك حالة التزامهم بالمحافظة على السر المهني".

٣- إضافة مادة قانونية إلى قانون أصول المحاكمات الجزائية السوري تتعلق بجواز تفتيش وضبط المكونات المعنوية للحاسوب، ويكون نصها كالتالي:

" في حال وقوع جريمة إلكترونية على نظم الحاسوب والإنترنت فيجوز لجهة التحقيق تفتيش وضبط المكونات المعنوية للحاسوب وهذه المكونات تشمل البيانات والمعلومات والبرامج ".

٤ - بما أن هنالك تشابهاً بين التنصت والمراقبة الإلكترونية لشبكات الحاسوب والإنترنت ومراقبة المحادثات الهاتفية وتسجيلها، وعدم كفاية النصوص الحالية في قانون أصول المحاكمات الجزائية السوري لمواجهة هذه التقنيات الحديثة، فنرى أن نص المادة (٩٦) أصول سوري يشمل هذا النوع من المراقبات مع إضافة تعديل مهم للمادة (٩٦) من خلال إضافة عبارة (وشبكات الحاسوب والإنترنت) ليصبح هذا النص المعدل كالتالي:

" لقاضي التحقيق ان يضبط لدى مكاتب البريد كافة الخطابات والرسائل والجرائد والمطبوعات والطرود، ولدى مكاتب البرق كافة الرسائل البرقية، كما يجوز له مراقبة المحادثات الهاتفية **وشبكات الحاسوب والإنترنت** متى كان لذلك فائدة في ظهور الحقيقة".

٥-إضافة مادة قانونية حول آثار بطلان الإجراءات وتصحيحها، على أن يكون نصها كالتالي: " لا يمتد بطلان الإجراء الباطل إلى الإجراءات السابقة عليها كما لا يمتد بطلان هذا الإجراء إلى الإجراءات اللاحقة له ألا إذا كانت مترتبة على الإجراء الباطل بحيث يكون مقدمة ضرورية لها، ويصحح الإجراء الجزائي الباطل كلما كان ذلك ممكناً ولازماً، ولا يعتد بالإجراء إلا من تاريخ تصحيحه".

**ثانياً: في قانون مكافحة الجريمة المعلوماتية وتنظيم التواصل عبر الشبكة السوري رقم (١٧) لعام ٢٠١٢م:**

ضرورة تعديل الفقرة (أ) المادة (٨) من قانون مكافحة الجريمة المعلوماتية وتنظيم التواصل عبر الشبكة السوري رقم (١٧) لعام ٢٠١٢م، المتعلقة بالتحفظ المعجل على البيانات من قبل مزود الخدمة، وتحديد هذه المدة بـ (٩٠) يوماً كحد أقصى ويصبح نصها كالتالي: " أ- يعاقب مقدم الخدمات على الشبكة الذي يهمل تنفيذ التزامه بحفظ نسخة من المحتوى لديه وحفظ بيانات الحركة **لمدة ٩٠ يوماً كحد أقصى** والتي تسمح بالتحقق من هوية الأشخاص الذين يسهمون في وضع محتوى على الشبكة بالغرامة من مئة ألف إلى خمسمائة ألف ليرة سورية".

**والله ولي التوفيق**

# قائمة المراجع

**أولاً: باللغة العربية:**

**١-المعاجم اللغوية:**

١- ابن منظور، لسان العرب، المجلد الحادي عشر، الطبعة الثالثة، دار صادر، بيروت، لبنان، ١٩٩٤م.

٢- الفيروز آبادي، القاموس المحيط، الطبعة الثانية، مؤسسة الرسالة، بيروت، لبنان، ١٤٠٧هـ.

٣- المنجد الأبجدي، الطبعة الثامنة، دار المشرق، بيروت، لبنان، ١٩٦٧م.

**٢- الكتب العامة:**

١- أحمد الشافعي، البطلان في قانون الإجراءات الجزائية، دراسة مقارنة، الطبعة الثانية، دار هومة، الجزائر، ٢٠٠٥م.

٢- أ. عبد الأمير العكيلي، أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية، ج١، الطبعة الأولى، مطبعة المعارف، بغداد، العراق، ١٩٧٥م.

٣- حسن يوسف مقابلة، الشرعية في الإجراءات الجنائية، الطبعة الأولى، دار الثقافة للتوزيع والنشر، عمان، الأردن، ٢٠٠٣م.

٤- د. أحمد فتحي سرور، أصول الإجراءات الجنائية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، ١٩٦٩م.

٥- د. أحمد فتحي سرور، الوسيط في قانون الإجراءت الجنائية، د.ط، دار النهضة العربية، القاهرة، مصر، ١٩٨٥م.

٦- د. أحمد فتحي سرور، الحماية الحنائية لأسرار الفرد في مواجهة النشر، د.ط، دار النهضة العربية، القاهرة، مصر،١٩٩١م.

٧- د. إلياس أبو عيد، أصول المحاكمات الجزائية، ج٢، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٧م.

٨- د. بارعة القدسي، أصول المحاكمات الجزائية، سير الدعوى العامة، ج٢، الطبعة الأولى، منشورات جامعة دمشق، دمشق، سورية، ٢٠١٠ – ٢٠١١م.

٩- د. جلال ثروت، نظم الإجراءات الجنائية، د.ط، دار الجامعة الجديدة، القاهرة، مصر، ٢٠٠٣م.

١٠- د. حسن الجوخدار، شرح قانون أصول المحاكمات الجزائية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ١٩٩٧م.

١١- د. رمسيس بهنام، الإجراءات الجنائية تأصيلاً وتحليلاً، ج٢، الطبعة الأولى، منشأة المعارف، الإسكندرية، مصر، ١٩٧٨م.

١٢- د. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، الطبعة الحادية عشر، د.د.ن، القاهرة، مصر، ١٩٧٦م.

١٣- د. سليمان الطماوي، القضاء الإداري، قضاء التأديب، د.ط، دار الفكر العربي، مصر، ١٩٧٧م.

١٤- د. سليمان عبد المنعم، بطلان الإجراء الجنائي، محاولة تأصيل أسباب البطلان في ظل قضاء النقض في مصر ولبنان وفرنسا، د.ط، دار الجامعة الجديدة للنشر، القاهرة، مصر، ١٩٩٩م.

١٥- د. سميح عبد القادر المجالي، أثر الإجراء الجزائي الباطل في المركز القانوني للمتهم، دراسة مقارنة، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، الأردن، ٢٠٠٦م.

١٦- د. عبد الحكم فوده، البطلان في قانون الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، مصر، ١٩٩٦-١٩٩٧م.

١٧- د. عبد الحميد الشواربي، البطلان الجنائي، د.ط، منشأة المعارف بالإسكندرية، مصر، ١٩٩٧م.

١٨- د. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، ٢٠٠٣م.

١٩- د. عبد الوهاب حومد، أصول المحاكمات الجزائية، الطبعة الرابعة، المطبعة الحديثة، دمشق، سورية، ١٩٨٧م.

٢٠- د. عمر السعيد رمضان، مبادئ الإجراءات الجنائية، د.ط، دار النهضة العربية، القاهرة، مصر، ١٩٨٥م.

٢١- د. عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، ج١، د.ط، دار النهضة العربية، القاهرة، مصر، ١٩٨٥م.

٢٢- د. عوض محمد، الوجيز في قانون الإجراءات الجنائية، ج١، د.ط، دار المطبوعات الجامعية، الإسكندرية، مصر، بلا تاريخ.

٢٣- د. فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠٠٦م.

٢٤- د. فوزية عبد الستار، شرح قانون أصول المحاكمات الجزائية اللبناني، د.ط، دار النهضة العربية، بيروت، لبنان، ١٩٧٥م.

٢٥- د. مأمون سلامة، شرح قانون الإجراءات الجنائية، د.ط، دار الفكر العربي، الإسكندرية، مصر، بلا تاريخ.

٢٦- د. مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، ج١، دار النهضة العربية، القاهرة، مصر، ١٩٨٨م.

٢٧- د. محمد سامي النبراوي، استجواب المتهم، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، ١٩٦٨م.

٢٨- د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية، القاهرة، مصر، ١٩٩٨م.

٢٩- فاروق الكيلاني، محاضرات في قانون أصول المحاكمات الجزائية الأردني والمقارن، ج٢، د.ط، دار الفارابي، عمان، الأردن، ١٩٨٥م.

**٣- الكتب المتخصصة:**

١- المحامي نزيه نعيم شلالا، الإثبات بواسطة الفاكس، البرقيات، الشريط المغناطيسي، الإثبات على أقراص مدمجة، الإثبات الإلكتروني، دراسة مقارنة (من خلال الفقه والاجتهاد والنصوص القانونية)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٨م.

٢- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، الطبعة الأولى، دار البداية، عمان، الأردن، ٢٠١٠م.

٣- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠١١م.

٤- د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، (أجهزة الرادار، الحاسبات الآلية، البصمة الوراثية)، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، ٢٠٠١م.

٥- د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩م.

٦- د. رامي متولي القاضي، مكافحة الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، ٢٠١١م.

٧- د. سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠١١م.

٨- د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، د.ط، دار الكتب القانونية، المحلة الكبرى، مصر، ٢٠٠٧م.

٩- د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، د.ط، دار الكتب القانونية، المحلة الكبرى، مصر، ٢٠٠٢م.

١٠- د. عبد الفتاح بيومي حجازي، جرائم الكومبيوتر والإنترنت، بهجات للطباعة والتجليد، القاهرة، مصر، ٢٠٠٩م.

١١- د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، د.ط، دار الكتب القانونية، المحلة الكبرى، مصر، ٢٠٠٧م.

١٢- د. عفيفي كامل عفيفي، جرائم الكومبيوتر، د.د.ن، القاهرة، مصر، ٢٠٠٠م.

١٣- د. علي القهوجي، الحماية الجنائية لبرامج الحاسوب، د.ط، الدار الجامعية للنشر، الإسكندرية، مصر، ١٩٩٧م.

١٤- د. علي حسن الطوالبه، التعاون القضائي في مجال مكافحة الجرائم الإلكترونية، مركز الإعلام الأمني، جامعة العلوم التطبيقية، البحرين.

١٥- د. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، الطبعة الأولى، عالم الكتب الحديث، إربد، الأردن، ٢٠٠٤م.

١٦- د. عمار عباس الحسيني، جرائم الحاسوب والإنترنت الجرائم المعلوماتية، الطبعة الأولى، منشورات زين الحقوقية، بيروت، لبنان، ٢٠١٧م.

١٧- د. عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي "المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية، الطبعة الأولى، ٢٠٠٤ . ٢٠٠٥ م.

١٨- د. عمر محمد بن يونس، الدليل الرقمي، الطبعة الأولى، مصر، ٢٠٠٧م.

١٩- د. عيسى مدلله المخول، الجريمة الإلكترونية، دمشق، سورية، ٢٠١٧م.

٢٠- د. محمد أمين الخرشة، مشروعية الصوت والصورة في الإثبات الجنائي، دراسة مقارنة، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠١٥م.

٢١- د. محمد طارق الخن، الجريمة المعلوماتية، منشورات الجامعة الافتراضية، دمشق، سورية، ٢٠١٢م.

٢٢- د. محمد الألفي، مدى مشروعية الدليل المستمد من الإنترنت، القاهرة، مصر، بلا تاريخ.

٢٣- د. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، منشورات أكاديمية نايف للعلوم الأمنية، الرياض، السعودية، ٢٠٠٤م.

٢٤- د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، ٢٠٠٠م.

٢٥- د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، مصر، ٢٠٠٩م.

٢٦- د. مصطفى محمد موسى، دليل التحري عبر شبكة الإنترنت، الطبعة الأولى، دار الكتب القانونية، القاهرة، مصر، بلا تاريخ.

٢٧- د. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكومبيوتر والانترنت، دار الكتب القانونية، مصر، ٢٠٠٦م.

٢٨- د. نزيهة مكاري، إثبات جرائم الاعتداء على حق المؤلف عبر الإنترنت في التشريع الجزائري، دراسة مقارنة، الطبعة الأولى، دار هومة، الجزائر،٢٠٠٩م.

٢٩- د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، الطبعة الأولى، مكتبة الآلات الحديثة، أسيوط، مصر، ١٩٩٤م.

٣٠- د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، ١٩٩٧م.

٣١- د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، د.ط، دار النهضة العربية، القاهرة، مصر، ٢٠٠٦م.

٣٢- رامي علي وشاح، الصعوبات الماديّة التي تعترض الإثبات بالمحرّرات الإلكترونية، الأكاديمية للدراسات الاجتماعية والإنسانيَّة، ٢٠١٠م.

٣٣- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، د.ط، دار الجامعة الجديدة، مصر، ٢٠١٠م.

٣٤- عبد الرحمن بحر، معوقات التحقيق في جرائم الإنترنت «دراسة مسحيَّة على ضباط الشرطة في دولة البحرين»، أكاديمية نايف العربية للعلوم الأمنيّة، ١٤٢٠هـ- ١٩٩٩م.

٣٥- عبد الناصر محمد محمود فرغلي، د. محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٧م.

٣٦- كوثر أحمد خالند، الإثبات الجنائي بالوسائل العلمية، دراسة تحليلية مقارنة، الطبعة الأولى، مكتب التفسير للنشر والإعلان، أربيل، العراق، ٢٠٠٧م.

٣٧- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٠٧م.

**٤- الرسائل الجامعية:**

**- رسائل الدكتوراه:**

١- أحمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، القاهرة، مصر، ١٩٥٩م.

٢- بهلول مليكة، دور الشرطة العلمية والتقنية في الكشف عن الجريمة، رسالة دكتوراه، كلية الحقوق، جامعة الجزائر ١، ٢٠١٣م.

٣- د. عمر أبو بكر يونس، الجرائم الناشئة عن الإنترنت، رسالة دكتوراه، جامعة عين شمس، مصر، ٢٠٠٠م.

٤- د. رضا عبد الحكيم إسماعيل رضوان، الضبط القضائي بين السلطة والمسؤولية، دراسة مقارنة مع التشريع الفرنسي، رسالة دكتوراه، أكاديمية الشرطة، القاهرة، مصر، ١٩٩٢م.

٥- د. محمد جودت الملط، المسؤولية التأديبية للوظف العام، رسالة دكتوراه، جامعة القاهرة، القاهرة، مصر، ١٩٦٧م.

٦- معمر علي إبراهيم محمد، حجية الأدلة التقنية في الجرائم الإلكترونية، رسالة دكتوراه، جامعة الرباط الوطني، كلية الدراسات العليا والبحث العلمي، السودان، ٢٠١٤م.

**- رسائل الماجستير:**

١- أسامة عبد الله محمد زيد الكيلاني، البطلان في قانون الإجراءات الجزائية الفلسطيني، دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، ٢٠٠٨م.

٢- آمال عبد الرّحمن يوسف حسن، الأدلة العلمية ودورها في الإثبات الجنائي، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، ٢٠١١-٢٠١٢م.

٣- ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية - دراسة تأصيلية تطبيقية - رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، ٢٠١٢م.

٤- د. هدى طلب علي، الإثبات الجنائي في جرائم الإنترنت والاختصاص القضائي بها (دراسة مقارنة)، رسالة ماجستير، كلية الحقوق، جامعة النهرين، بغداد، العراق، ٢٠١٢م.

٥- سهى إبراهيم داود عريقات، ورقة بحثية بعنوان" الطبيعة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي"، كلية الحقوق، جامعة القدس، (من ص١ إلى ص٣٨).

٦- عطية عثمان محمد بوحويش، حجية الدليل الرقمي في إثبات جرائم المعلوماتية، رسالة الماجستير، مقدمة إلى أكاديمية الدراسات العليا، بنغازي، ٢٠٠٩م.

٧- محمد نافع فالح رشدان العدواني، حجية الدليل الإلكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية (دراسة مقارنة بين القانونين الكويتي والأردني)، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، ٢٠١٥م.

٨- فايزة جادي، البصمة الوراثية ومدى حجيتها في الإثبات الجنائي، رسالة ماجستير، كلية الحقوق، بن عنكون، الجزائر، ٢٠١١ - ٢٠١٢م.

٩- محمد الطاهر الرحال، بطلان إجراءات التحقيق في قانون الإجراءات الجزائية الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة منتوري، قسنطينة، الجزائر، ٢٠٠٨- ٢٠٠٩م.

١٠- محمد ذيب محمود نمر، أحكام البطلان في الإجراءات والمحاكمات الجزائية، دراسة مقارنة بين القانونين الفلسطيني والأردني، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن،٢٠١٣م.

١١- هلال آمنة، الإثبات الجنائي بالدليل الإلكتروني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، ٢٠١٤ - ٢٠١٥م.

**٥- المقالات والأبحاث:**

١- أ. طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، مجلة الحقوق، المجلد الثاني عشر، العدد الأول، الصفحة (٧٣-٤٠)، جامعة بنغازي، ليبيا.

٢- أ. م. جاسم خريبط خلف، بحث بعنوان: "صعوبات الدليل الجنائي في الجرائم المعلوماتية"، قسم القانون، كلية شط العرب الجامعة، بلا تاريخ.

٣- أمجد خليل حمودة، الوسائل الحديثة لإثبات الجرائم التي ترتكب بواسطة الأجهزة الإلكترونية، مجلة جامعة الأزهر، عدد خاص بمؤتمر كلية الحقوق الخامس المحكّم، المجلد التاسع عشر، الصفحة (١٣٦-١١٣)، غزة، فلسطين.

٤- أ.م.د. علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب الثانوية والأمنية للعمليات الإلكترونية، مؤتمر نظمته أكاديمية شرطة دبي، مركز البحوث والدراسات رقم (١) في الفترة ٢٦- ٢٠٠٣/٤/٢٨م.

٥- د. عمر محمد بن يونس، ورقة بحثية بعنوان" الدليل الرقمي"، ٢٠٠٦م.

٦- د. غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكومبيوتر، بحوث مؤتمر القانون والكومبيوتر والإنترنت، من ١ – ٣ مايو، كلية الشريعة والقانون، جامعة الأمارات العربية المتحدة، المجلد الثاني، الطبعة الثالثة، ٢٠٠٤م، الصفحة (٦٦٠-٦٢٥).

٧- د. محمد أحمد المنشاوي، سلطة القاضي الجنائي في تقدير الدليل الإلكتروني، مجلة الحقوق، السنة السادسة والثلاثون، العدد الثاني، الصفحة (٥١٥- ٥٦٨)، الكويت، ٢٠١٢م.

٨- د. موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مقدَّم إلى: المؤتمر المغاربي الأول حول: المعلوماتية والقانون الذي تنظمه أكاديمية الدراسات العليا . طرابلس خلال الفترة ٢٨ . ٢٩ / ١٠ / ٢٠٠٩م.

٩- د. ميسون خلف حمد الحمداني، مشروعية الأدلة الالكترونية في الإثبات الجنائي، مجلة كلية الحقوق، جامعة النهرين، المجلد الثامن عشر، العدد الثاني، الصفحة (195 -254)، بغداد، العراق،٢٠١٦م.

١٠ – د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، بحوث مؤتمر القانون والكومبيوتر والإنترنت، من ١ – ٣ مايو، كلية الشريعة والقانون، جامعة الأمارات العربية المتحدة، المجلد الثاني، الطبعة الثالثة، ٢٠٠٤م، الصفحة (٥٠٦-٤٠١).

١١- د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، بحوث مؤتمر القانون والكومبيوتر والإنترنت، من ١ – ٣ مايو، كلية الشريعة والقانون، جامعة الأمارات العربية المتحدة، المجلد الثاني، الطبعة الثالثة، ٢٠٠٤م، الصفحة (٧٨٩-٧١٣).

١٢- د. يونس عرب، التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية، ورقة عمل مقدمة أمام الندوة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي، النادي العربي للمعلومات، دمشق، سورية.

١٣- د. يونس عرب، ورقة عمل حول الجرائم الالكترونية وأدلة إثباتها بين الواقع الماثل والمثال المأمول

١٤- عبد العزيز خنفوسي، ورقة بحثية بعنوان" مدى حجية أدلة الإثبات الجنائي التقليدية في إثبات جرائم الإرهاب المعلوماتي، كلية الحقوق والعلوم السياسية، جامعة سعيدة. الصفحة (١٥٥-١٤٢).

١٥- م.م. حسين خليل مطر، إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية، بحث مقدم الى مؤتمر (الاصلاح التشريعي طريق نحو الحكومة الرشيدة ومكافحة الفساد) الذي اقامته مؤسسة النبأ للثقافة والاعلام وجامعة الكوفة، كلية القانون، في الفترة بين ٢٥-٢٦ /٤/٢٠١٨م.

١٦- يونس عرب، جرائم الكمبيوتر والانترنت، (ايجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات).

١٧- ورقة بعنوان: «دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول»، ضمن فعاليات المؤتمر الثالث لرؤساء المحاكم العليا (النقض، التمييز، التعقيب) في الدول العربية المنعقد في جمهورية السودان الشقيقة خلال الفترة ٢٣-٢٥ /٢٠١٢/٩م الموافق ٧- ١٤٣٣/١١/٩هـ.

**٦- المجموعات القانونية:**

١- مجموعة الأحكام المصرية، س١٦، رقم ٢١.

٢- مجموعة الأحكام المصرية، س١٨، رقم٢٤.

٣- مجموعة أحكام محكمة النقض المصرية، س٢٠، رقم ٣٥.

٤- مجموعة أحكام محكمة النقض المصرية، س٧، رقم ,١١٦

٥- ياسين الدركزلي وأديب استانبولي، المجموعة الجزائية لقرارات محكمة النقض السورية من عام ١٩٤٩ - ١٩٩٠م، ج١، الطبعة الثانية، ١٩٩٢م.

**٧-الإنترنيت:**

١- د. حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، منشور على الموقع الإلكتروني التالي:

http:// www.eastlaws.com

٢- د. خالد ممدوح إبراهيم، الدليل الإلكتروني في جرائم المعلوماتية، بحث منشور على الموقع الإلكتروني لكلية الحقوق في جامعة المنصورة www.f - law.com، ص٢. تاريخ الدخول في ٢٠١٧/١٢/١٢م.

٣- د. علي حسن الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي (دراسة مقارنة)، مركز الإعلام الأمني، جامعة العلوم التطبيقية، البحرين، ٢٠٠٩م، بحث منشور على الموقع الإلكتروني التالي:

www.policeem.gov.bh/reports

٤- د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجريمة الإلكترونية، بحث منشور على شبكة الإنترنت على الموقع التالي:

www.f - law.net/law/showthread.php?t=2208. تاريخ الدخول في ٢٠١٨/٨/٢٢م.

٥- د. محمد ثامر، الحماية القانونية والقضائية لحق الإنسان في الخصوصية، كلية القانون، جامعة ذي قار، لعراق، ٢٠١٥/٥/٥م. متاح على الموقع التالي:

http://www.alnoor.se/article.asp?id=274740

٦- فرج بشير برنوص، ورقة عمل بعنوان" حجية الدليل الرقمي وموقف المشرع الليبي" مقدمة إلى ورشة العمل حول قوانين وتشريعات الأمن السيبراني والمنعقدة في جامعة طرابلس يوم ٢٠١٦/٥/٢٣م، منشور في ٢٠١٦/٧/١م على الموقع التالي:

https://www.slideshare.net/nissaly/ss - 6261086. تاريخ الدخول في ٢٠١٨/٦/٢٢م.

٧- لموسخ محمد، تنازع الاختصاص في الجرائم الالكترونية، جامعة قاصدي مرباح ورقلة، الجزائر،

منشور على الموقع الإلكتروني التالي:

https://revues.univ - ouargla.dz/index.php/numero - 02 - 2009 - dafatir/559 - 2013 - 05 - 02 - 11 - 40 - 10

**٨-القوانين:**

١- قانون الإجراءات الجزائية الجزائري الصادر بموجب الأمر ١٥٥/٦٦ في ١٩٦٦م وفقاً لآخر التعديلات.

٢- قانون الإجراءات الجزائية الفرنسي وفقاً لأحدث التعديلات.

٣- قانون أصول المحاكمات الجزائية السوري الصادر بالمرسوم ١١٢ الصادر في ١٣/٣/١٩٥٠م.

٤- قانون أصول المحاكمات الجزائية اللبناني رقم ٣٢٨ الصادر في ٢/٨/٢٠٠١م.

٥- قانون الأمارات الاتحادي رقم (٢) لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات.

٦- قانون الجرائم الإلكترونية الفلسطيني رقم (١٦) لسنة ٢٠١٧م.

٧- قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري الصادر بالمرسوم التشريعي رقم (١٧) بتاريخ ٨/٢/٢٠١٢م.

٨- قانون جرائم أنظمة المعلومات الأردني المؤقت لسنة ٢٠١٠م.

٩- قانون جرائم تقنية المعلومات البحريني رقم (٦) لعام ٢٠١٤م.

١٠- قانون مكافحة الجرائم الإلكترونية القطري رقم (١٤) لسنة ٢٠١٤م.

١١- مشروع قانون مكافحة الجرائم الإلكترونية المصري لسنة ٢٠١٦م

١٢- نظام مكافحة جرائم المعلوماتية السعودي الصادر في ٢٦/٣/٢٠٠٧م.

**٩- الدساتير:**

١- الدستور السوري الجديد الصادر في ١٥ /٢/٢٠١٢م.

٢- الدستور الفرنسي الصادر في ٤/١٠/١٩٥٨م.

٣- الدستور المصري الصادر في ١٨/٧/٢٠١٤م.

**١٠- الوثائق والاتفاقيات والمؤتمرات الدولية:**

١- الاتفاقية الأوربية لحقوق الإنسان الصادرة في ٤/١١/١٩٥٠م.

٢- الاتفاقية الأوربية لمكافحة جرائم الحاسوب والإنترنت (بودابست ٢٢/١٠/٢٠٠١م).

٣- الإعلان العالمي لحقوق الإنسان الصادر في ١٠/١٢/ ١٩٤٨م.

٤- المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكومبيوتر (٤- ٩ تشرين أول ١٩٩٤م- البرازيل/ ريو دي جانيرو).

٥- مؤتمر الأمم المتحدة لمنع الجريمة ومعاقبة المجرمين، فيينا ١٠- ١٧ نيسان ٢٠٠٠م.

**ثانياً: باللغة الانكليزية In ENGLISH:**

**١ – الكتبBooks :**

1-Hans G. Nilsson, Computer crimes and other crimes aginst information Technology whin the working programme of the council of Europe, R.I.D.P. 1993.

2-Kaspersen (W.K. Henrik):" computer crime and crime against information in Netherlands" R.I.D. P. 1993.

3- Eoghan Casey, '' Cyberpatterms In turvey", B. Criminal Profiling, London Academic, Press, Chapter 25, 1999.

4-Eoghan Casey, Digital Evidence and computer crime, London, academic press, 2000

5- WISE (Edward M), "Computer crimes and other crimes against information Technology in the United States, R. I. D. P, 1993.

6-Eoghan Casey, Digital Evidence and Computer Crime-Forensic Science, Computers and the Internet, Second Edition, Academic Press an imprint of Elsevier, London, 2004.

7- Eoghan Casey, Digital Evidence and computer crime, London, academic press, 2000.

8-Vassilaki (Irini); Computer crimes and other crimes against information technology in Greece, R.I.D, 1993

9-Durham (colo): The emerging structures of criminal information law: tracing the contours of a new pardign general report for the A.I.D.P. 1993.

10-Mohrenschl ager (Manfred): computer crimes and other crimes against information technology in GermanyR.I. P,1993.
11- PIRAGOFF (Donald K), "Computer crimes and other crimes against information Technology in Canda, R I D P, 1993.
12-Anthony Reys and others, Cyber Crime Investigations, Bridging The Gaps Between Security Professional Law, Enforcement and Prosecutors. Published by Elsevier Since and Technology, 2007.
13-Frank J. Donner; The age of Surveillance, Washington, DC, 1981.

**2- الأبحاث Research:**

1-Dr. Kan Wong, Computer Fraud in The U.K The picture, Computer fraud of security, Bulletin, Vol, 9, nal, 1986.

2- David Thompson, current trends in computer crime, computer control quarterly, vol, 9, no, I, 1991.

3-LAW AND COMPUTER TECHNOLOGY: vol 5, no 2, March 1972.

4-The Neis, Argentine Computer Inversion Investigation – FBI- Law Enforcement, Bulletin- Oct 1928, Vol 67- Issue 10.

**3- الانترنيت Internet:**

1- Brian Carrier. Defining Digital Forensics Examination and Analysis Tools. In Digital Research Workshop II, 2002, Available at:
http://www.Dfrws.org/dfrws2002/papars/papars/Brian Carrier.pdf.
2-Brian Carrier, "Open Source Digital Forensic Tolls, the Legal Arguments, October 2002", Available at:
http://www.atstak.com Date 22/9/2018.

3- Dr. Henry B. wolfe, Forensics and the emerging importance of electronic Evidence gathering, OTAGO university, 2001, P - 4, available on line.
www.e - evidence.info.
4- Hinry, J,F, " Testimony before Permanent Subcommittee On Governmental Affairs, The United States Senate, Ninety, Ninth Congress, 1984, Available at:
http://www.igc.apc.org/nemesis/ACLU/nudisthall of shame/hinry.htmi Date: 17/9/2018.
5- Carter, DL, and Katz. A..J."Computer Crime:An Emerging challenge for Law Enforcement" , Available at:
http://www.fbi.gov/ieb/dec96itxt
6- Open source. Open source Case for Business. Available at:
http://www.opensource.org/advocacy/case for business.php. Date 11/8/2018
7- Linux - NTFS Project.NTFS, Documentation Available at:
http://linux - ntfssourceforgenet/ntfs. Date: 12/7/2018.
8- NIST. Computer Forensics Toll Testing. Available at:
http://www.cftt.nist.gov. Date:13/7/2018.
9- NIST CETT. Disk Imaging Tool Specification, 3,1,6 Edition, October 2001, Available at:
http://www.cftt.nist.gov/DI - spec - 3 - 6/doc. Date 11/9/2018.
10- Scientific Working Group on Imaging Technologies. Definitions and Guidelines for the use of Imaging Technologies in the criminal justice system. Forensic Communications, 1(3) October 1999, Available at:
http://www.fbi.gov/hq/lab/fsc/backissu/oct1999/swgit.htm. Date 10/9/2018.
11-Daved Wheeler. Is Open Source Good for Security? Secure Programming for Linux and Unix HOWTO 13 july 2002. Available at:
http://www.dwheeler.com/secure - programs/Secure - Programs - HO//w/tO/open - source - security.html. Date 21/9/2018.
12-David.G; Masse www.Mase.org/preuve courrie/.thm

13-Eoghan Casey; "Digital Evidence and Computer Crime" February 2002. ISBN:012162885 X, Available at: http://www.apcatalog.com Date 22/9/2018.
14-Eoghan Casey; Computer Crime Investigation" October 2001 ISBN:012631036, Available at: http://www.apcatalog.com Date 22/9/2018.
15- Dr. Henry B. wolfe, Forensics and the emerging importance of electronic Evidence gathering, OTAGO university, 2001, P - 4, available on line.
www.e - evidence.info.
16- The Federal Rules of Evidence
orwww.lawsource.com www.wikipedia.org
17- International Review of Criminal Policy - United Nations " Manual on the Prevention and Control of Computer Related Crime 2000":
http://www.ifs.univie.ac.at/ - przg91/ser4344.html
18- Anabda Giet, Analysis of the police and criminal evidence act sec. 69/ computer generated evidence, WEB jornal of Current Legal issues UK, 1996 Issue 1, p.1. Available on-line in june 2008 at:
Http://webicli.nci.ac.uk/1996/issue1/hoev.html

**ثالثاً: باللغة الفرنسية En Langue Française:**

**١ – الكتبLes ouvrages:**

1 – Bouzet ; La loyauté dans la recherche des preuves, (Problèmes contemporains de procédures pénale, en hommage à Hugueney, Paris, France, 1964 .
2 – BENSOUSSAN ALAIN: Internet. Aspects juridiques, memento - guide, hermes, 1996.
3 – Gassin R, le droit et l'informatique, Dalloz, Paris , France, 1982.
4-HUET PIERRE, Les services multimédia, AFTEL, Le droit du multimédia de la télématique à l'internet ; sous la direction de PIERRE HUET avec le concours de H. MAISL, A. LUCAS, éd. 1996 .

5-KAYSER PIERRE, La protection de la vie privée Economique. Presses universitaires d'AIX - MARSEILLE, 2 ème éd, 1990.
6- Leborgne G ; Le contrôle des actes des agents de la police judiciaire, R. S.C, 1987.
7-Laure rassat M ; Traité de procédure Penale, P U F, Paris, France, 2000.
8-MERLE (R) et VITU (A), Traité de droit criminel, Procédure pénale, 4 ème éd, Cujas, Paris, 1989.
9-STEFANI (Gaston), LEVASSEUR (Georges) et BOULOC (Bernard), Procédure pénale, Précis Dalloz, 16ème éd, Paris, France, 1996.
10-TORELLO NICOLE et LOINTIER PASCAL, internet pour les jurists, Dalloz,1996.
11- VERBIEST(THIBAULT) ; cyber consommateur, Litec, Paris, France, 2002.

**2–الرسائل Les Thèses :**

1- DARAGON (E); Droit de la preuve, Thèse, Grenoble, 1996.
2- VERGUCHT (P); La répression des délits informatiques dans une perspective international. Thèse, Montpellier 1, 1996.

**٣–التقارير Les Rapports :**

1- Pradel J ; La preuve en procédure pénal comparé, Rapport en Revue Internationale de droit pénal,1992.

**٤–أحكام المحاكم Les décisions du cours :**

1-Cour de cassation (Belgique), 13 Mai 1986, R.D.P.C.1986.
2- Cass crim 9 October 1980, Dalloz,1981.
3- Cass crim 13 Juin 1989, Bull.
4- Cass crim 28 Juin 1983, Bull crim no 201.

**٥– الانترنيت Les sites internet:**

1–http://www.legifrance.gouv.fr.

2– http://www.ministère de la justice. Com.

# الفهرس


| العنوان | صفحة |
|---|---|
| المقدمـة | ١ |
| **الباب الأول**<br>**متطلبات مشروعية الدليل الإلكتروني في الإثبات الجزائي** | ١١ |
| **الفصل الأول: مشروعية وجود الدليل الإلكتروني** | ١٧ |
| المبحث الأول: ماهية الدليل الإلكتروني | ١٨ |
| المطلب الأول: مفهوم الدليل الإلكتروني | ٢١ |
| الفرع الأول: تعريف الدليل الإلكتروني | ٢١ |
| الفرع الثاني: خصائص الدليل الإلكتروني | ٢٨ |
| الفرع الثالث: طبيعة الدليل الإلكتروني | ٣٦ |
| الفرع الرابع: مصادر الدليل الإلكتروني في التحقيقات الجرمية | ٣٨ |
| الفرع الخامس: مكانة الدليل الإلكتروني من أدلة الإثبات الجزائي | ٤١ |
| المطلب الثاني: أنواع الدليل الإلكتروني | ٤٣ |
| الفرع الأول: تقسيم الفقه لأنواع الدليل الإلكتروني | ٤٤ |
| الفرع الثاني: التقسيم القضائي لأنواع الدليل الإلكتروني | ٥١ |
| المبحث الثاني: الموقف من مشروعية وجود الدليل الإلكتروني | ٥٥ |
| المطلب الأول: موقف أنظمة الإثبات من مشروعية وجود الدليل الإلكتروني | ٥٥ |
| الفرع الأول: موقف نظام الإثبات المقيد من مشروعية وجود الدليل الإلكتروني | ٥٦ |
| الفرع الثاني: موقف نظام الإثبات الحر من مشروعية وجود الدليل | ٥٨ |

| | |
|---|---|
| الإلكتروني | |
| المطلب الثاني: موقف الاتفاقيات الدولية والفقه والقضاء والقانون من مشروعية وجود الدليل الإلكتروني | ٦٠ |
| الفرع الأول: موقف الاتفاقيات الدولية من مشروعية وجود الدليل الإلكتروني | ٦١ |
| الفرع الثاني: موقف الفقه والقضاء والقانون من مشروعية وجود الدليل الإلكتروني | ٦٣ |
| **الفصل الثاني: مشروعية الحصول على الدليل الإلكتروني** | ٧٧ |
| المبحث الأول: الحصول على الدليل الإلكتروني في الإجراءات التقليدية | ٨١ |
| المطلب الأول: صعوبات الحصول على الدليل الإلكتروني في الإجراءات التقليدية | ٨٢ |
| الفرع الأول: صعوبات متعلقة بالجريمة الإلكترونية | ٨٣ |
| الفرع الثاني: صعوبات متعلقة بالدليل الإلكتروني | ١٠٠ |
| الفرع الثالث: صعوبات متعلقة بأسباب متعددة | ١٠٥ |
| المطلب الثاني: مشروعية الحصول على الدليل الإلكتروني في الإجراءات التقليدية | ١٠٨ |
| الفرع الأول: الخبرة الإلكترونية | ١٠٩ |
| الفرع الثاني: المعاينة الإلكترونية | ١١٦ |
| الفرع الثالث: التفتيش الإلكتروني | ١٤٧ |
| الفرع الرابع: الضبط الإلكتروني | ٢٠١ |
| المبحث الثاني: مشروعية الحصول على الدليل الإلكتروني في الإجراءات الحديثة | ٢١٥ |
| المطلب الأول: مشروعية الحصول على الدليل الإلكتروني في الإجراءات المتعلقة بالبيانات الساكنة | ٢١٩ |

| | |
|---|---|
| الفرع الأول: التحفظ المعجل على البيانات المخزنة | ٢٢٠ |
| الفرع الثاني: الأمر بتقديم بيانات معلوماتية عن المشترك | ٢٢٩ |
| المطلب الثاني: مشروعية الحصول على الدليل الإلكتروني في الإجراءات المتعلقة بالبيانات المتحركة | ٢٣٥ |
| الفرع الأول: ماهية التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية | ٢٣٦ |
| الفرع الثاني: مشروعية التنصت أو الاعتراض على المكالمات الهاتفية والإلكترونية | ٢٤٤ |
| **الباب الثاني**<br>**الأحكام المترتبة على مشروعية الدليل الإلكتروني في الإثبات الجزائي** | **٢٦٥** |
| **الفصل الأول: آثار مشروعية الدليل الإلكتروني في الإثبات الجزائي** | **٢٦٨** |
| المبحث الأول: مؤيدات عدم مشروعية إجراءات الحصول على الدليل الإلكتروني | ٢٦٩ |
| المطلب الأول: المؤيدات الإجرائية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني | ٢٧٠ |
| الفرع الأول: بطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني | ٢٧٢ |
| الفرع الثاني: أحكام بطلان الإجراءات غير المشروعة للحصول على الدليل الإلكتروني | ٢٨٥ |
| المطلب الثاني: المؤيدات العقابية والمدنية والتأديبية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني | ٣٠٣ |
| الفرع الأول: المؤيدات العقابية والمدنية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني | ٣٠٤ |

| | |
|---|---|
| الفرع الثاني: المؤيدات التأديبية لعدم مشروعية إجراءات الحصول على الدليل الإلكتروني | ٣١٦ |
| المبحث الثاني: نطاق العمل بالدليل الإلكتروني | ٣٢١ |
| المطلب الأول: نطاق العمل بالدليل الإلكتروني في الجرائم الإلكترونية | ٣٢١ |
| الفرع الأول: ماهية الجرائم الإلكترونية (*Cyber Crime*) | ٣٢٣ |
| الفرع الثاني: ملاءمة الدليل الإلكتروني لإثبات الجريمة الإلكترونية | ٣٦٢ |
| الفرع الثالث: الحجج المبررة لملاءمة إثبات الجريمة الإلكترونية بالدليل الإلكتروني | ٣٦٥ |
| المطلب الثاني: نطاق العمل بالدليل الإلكتروني في الجرائم التقليدية | ٣٧٠ |
| الفرع الأول: نطاق العمل بالدليل الإلكتروني في الجرائم التقليدية المختلطة | ٣٧٠ |
| الفرع الثاني: نطاق العمل بالدليل الإلكتروني في الجرائم التقليدية الصرفة | ٣٧٨ |
| **الفصل الثاني: تقدير الدليل الإلكتروني في الإثبات الجزائي** | **٣٨١** |
| المبحث الأول: حرية القاضي الجزائي في تقدير الدليل الإلكتروني | ٣٨٣ |
| المطلب الأول: مفهوم السلطة التقديرية للقاضي الجزائي | ٣٨٣ |
| الفرع الأول: تعريف السلطة التقديرية للقاضي الجزائي | ٣٨٣ |
| الفرع الثاني: ضوابط السلطة التقديرية للقاضي الجزائي في تقدير الدليل الجزائي | ٣٨٥ |
| المطلب الثاني: الشروط الواجب توافرها في الدليل الإلكتروني | ٣٨٩ |
| الفرع الأول: شرط يقينية الدليل الإلكتروني | ٣٩١ |
| الفرع الثاني: شرط وجوب مناقشة الدليل الإلكتروني | ٣٩٦ |
| الفرع الثالث: شرط مشروعية الدليل الإلكتروني | ٣٩٩ |
| المبحث الثاني: تقدير القاضي الجزائي للدليل الإلكتروني في أنظمة الإثبات المختلفة | ٤٠٥ |

| | |
|---|---|
| المطلب الأول: تقدير القاضي الجزائي للدليل الإلكتروني في نظام الإثبات الحر | ٤٠٥ |
| الفرع الأول: الأسس العامة لتقدير الدليل الإلكتروني في نظام الإثبات الحر | ٤٠٦ |
| الفرع الثاني: موقف بعض التشريعات اللاتينية من تقدير الدليل الإلكتروني | ٤١٤ |
| المطلب الثاني: تقدير القاضي الجزائي للدليل الإلكتروني في نظام الإثبات المقيد | ٤١٧ |
| الفرع الأول: لأسس العامة لتقدير الدليل الإلكتروني في نظام الإثبات المقيد | ٤١٧ |
| الفرع الثاني: موقف بعض التشريعات الأنكلوسكسونية من تقدير الدليل الإلكتروني | ٤٣٢ |
| المطلب الثالث: النظام المقترح لتقدير الدليل الإلكتروني | ٤٣٩ |
| الفرع الأول: القواعد الواجبة لتقييم القيمة العلمية للدليل الإلكتروني | ٤٤٠ |
| الفرع الثاني: تقدير القاضي الجزائي للدليل الإلكتروني الخاضع لإجراءات التقييم | ٤٤٣ |
| الخاتمة | ٤٤٧ |
| قائمة المراجع | ٤٦٩ |
| الفهرس | ٤٨٩ |