الفصل الأول

ماهية الدليل الإلكتروني في الشريعة والقانونين الإماراتي والمصري

تمهيد:

يعد التطور الكبير الذي شهدته نظم المعلومات الإلكترونية في الآونة الأخيرة العامل الرئيسي لتطور نوعية الجرائم المرتكبة، ونوعية الجناة الذين يرتكبون هذه الجرائم، كما إنها كانت أحد العوامل الأساسية التي أثرت بشكل كبير في طرق الإثبات الجنائي، فكان لابد من مواكبة تلك التطورات بابتكار طرق حديثة للعمل على إثبات هذا النوع من الجرائم، ومن هنا ظهر نوع حديث من الأدلة والذي يمكن من خلاله إثبات الجرائم الإلكترونية، كما يقوم على تحديد مرتكبها ونسبة تلك الجرائم إليه، ويعرف هذا النوع من الدلائل باسم الدليل الإلكتروني أو الرقمي[٣٦]. واللفظ الأكثر شيوعًا هو "الدليل الإلكتروني" حيث استخدمه المشرع الأوروبي فيما يتعلق بالمعوقات التي تواجه الإجراءات الجنائية التي ترتبط بوسائل التكنولوجيا الحديثة، وهو ما ورد في توصية رقم (٩٥) ١٣ وتم اعتمادها من لجنة الوزراء في ١١ سبتمبر عام ١٩٩٥م، بالإضافة إلى استخدام هذا المصطلح في اتفاقية بودابست التي تم عقدها في ٢٣ نوفمبر من عام ٢٠٠١م، حيث تم ذكرها في الفقرة الثانية من المادة (١٤)، بجانب ذكره فيما يعرف ب "عنوان المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولًا إلى الدليل الإلكتروني في التحقيقات الجنائية" في عام ١٩٩٤م[٣٧].

---

[٣٦] بيل جيتس . ١٩٩٨ . *المعلوماتية بعد الإنترنت: طريق المستقبل* . ترجمة: عبد السلام رضوان . الكويت: المجلس الوطني للثقافة والفنون والآداب . ص . ٤١-٦٣.

[٣٧] بن يونس، عمر محمد . ٢٠٠٦ . *الإجراءات الجنائية عبر الإنترنت: المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولًا إلى الدليل الإلكتروني في التحقيقات الجنائية* . د.ن . ص . ٦ وما بعدها.

فبالنظر إلى الارتباط الوثيق بين الجريمة الإلكترونية والدليل الإلكتروني، نجد اكتساب الدليل الإلكتروني سمة الذاتية الخاصة، والتي أثرت بشكل كبير على طرق وإجراءات الحصول على هذا النوع من الدلائل، حيث تخطت طرق جمع الدليل الإلكتروني الأساليب التقليدية المتمثلة في المعاينة والتفتيش وغيرها، فتم استخدام طرق أكثر حداثة لمواكبة تطور أساليب وطرق الجرائم الإلكترونية وذلك من خلال العمل على سرعة التحفظ على البيانات التي تم تخزينها، والقيام باعتراض الاتصالات الإلكترونية الخاصة، وهو ما يعد ذا أهمية كبيرة للتصدي إلى هذا النوع من الجرائم، فإن غياب الدليل الإلكتروني يؤدي إلى عدم القدرة على نسب الجريمة إلى مرتكبها[٣٨].

ومن خلال ما سبق سيتم التعرض في هذا الفصل إلى مبحثين كالتالي:

المبحث الأول: ماهية الدليل الإلكتروني.

المبحث الثاني: إجراءات جمع الدليل الإلكتروني.

المبحث الأول: ماهية الدليل الإلكتروني وطبيعته:

تعتبر الأدلة الجنائية حقيقة حتمية في طبيعتها، حيث إن وجود الدليل الجنائي مرتبط ارتباطا وثيقًا بوجود الجريمة نفسها، وقد يكون ذلك في مرحلة ما قبل ارتكاب الجريمة والتي تتمثل في التجهيز والترتيب أو الشروع في ارتكابها، أو متوافقة مع لحظة ارتكابها، أو لاحقًا عند قيام مرتكب الجريمة بإخفاء معالمها[٣٩].

---

[٣٨] هدى حامد قشقوش . ١٩٩٣ . "جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات" . *مؤتمر الجمعية المصرية للقانون الجنائي المنعقد بالقاهرة خلال الفترة من ٢٥ إلى ٢٨ أكتوبر ١٩٩٣* . القاهرة: دار النهضة العربية . ص . ٥٧٦ .

[٣٩] الحمادي، خالد حمد محمد . ٢٠١٥ . *الثورة البيولوجية ودورها في الكشف عن الجريمة DNA* . الإسكندرية: دار الجامعة الجديدة . ص . ١٩.

وبذلك يمكن القول بأن الدليل الإلكتروني يتواجد في حالة ظهور الجريمة الإلكترونية والتي تقوم سلطات الاتهام بادعاء حدوثها، ويتحدد دور الدليل الإلكتروني في القدرة على إثبات الجريمة وإدانة الجاني وإسناد الجريمة إليه، ولذلك ستتناول الباحثة في هذا المبحث تعريف الجريمة الإلكترونية وتحديد خصائصها، بالإضافة إلى معرفة طبيعتها الخاصة حتى يمكن إثباتها جنائيًا، حيث ستقسم الباحثة المبحث إلى مطلبين كما يلي:

المطلب الأول: محل الدليل الإلكتروني (الجريمة الإلكترونية).

المطلب الثاني: مفهوم الدليل الإلكتروني.

المطلب الأول: محل الدليل الإلكتروني (الجريمة الإلكترونية)

حتى نتمكن من دراسة الدليل الإلكتروني يجب أن نتناول في المقام الأول الجريمة الإلكترونية، وذلك لكونها محل الدليل الإلكتروني، حيث أنها تختلف اختلافًا كبيرًا عن غيرها من الجرائم التقليدية التي تحدث في العالم بشكل عام، وفي الدول العربية بشكل خاص، فهذا النوع من الجرائم يعتبر حديثًا نسبيًا وخاصةً بالنسبة للدول العربية لكونها حديثة في مجال التقنيات التكنولوجية الجديدة، بالإضافة إلى أن العديد من هذه الدول لم تقم بتوفير خدمات الإنترنت لشعبها إلا في الآونة الحديثة.

ولذلك كان لابد من التطرق إلى أبعاد هذه الظاهرة بشكل كلي من خلال تناول تعريفها، والتعرف على خصائصها، ومن ثم معرفة كيفية إثبات الجريمة الجنائية عن طريق التعرف على أثر طبيعتها الخاصة.

الفرع الأول: مفهوم الجريمة الإلكترونية

لقد تعددت المفاهيم المتعلقة بالجريمة التي يتم ارتكابها في بيئة الحاسوب أو في بيئة الشبكات الإلكترونية، فلا يوجد مصطلح قانوني متعارف عليه لهذه الظاهرة، وقد أدى هذا الاختلاف إلى تطور ظاهرة الإجرام المتعلقة بالتقنية التكنولوجية وتقنية المعلومات، وما يصاحبها من سوء استخدام الحاسوب وصولًا إلى الجرائم المعلوماتية والتي تتمثل في الجرائم التي يتم ارتكابها عن طريق الحاسوب والإنترنت، وهو ما يعرف باسم الجرائم الإلكترونية.

فإن أي من الاكتشافات الحديثة التي تسهم بشكل كبير في عملية الازدهار والتطور للمجتمعات، من شأنها فتح أبوابًا أخرى للجريمة، وبغض النظر عن تباين المصطلحات والمسميات التي تطلق على هذا النوع من الجرائم، فإنها تعتبر أحد أخطر أنواع الجرائم على المستوى المحلي أو العالمي، ويرجع ذلك إلى تأثيرها السلبي فيما يتعلق بأمن واستقرار المجتمعات سواء أكان ذلك في البلاد المتقدمة أو النامية على حد سواء.

ونظرًا لما سبق ذكره، فإنه من المفضل استخدام مصطلح "الدليل الإلكتروني" في هذه الدراسة، ويرجع ذلك إلى:

١. نظرًا إلى طبيعة هذا النوع من الجرائم من حيث نشأته في بيئة إلكترونية قائمة في الأساس على التطور التكنولوجي؛ مما قد ينتج عنه تطور دائم في طرق وأساليب ارتكاب مثل تلك الجرائم نسبة إلى مدى التطور الذي يشهده مجال تكنولوجيا الاختراعات والمعلومات الإلكترونية وغيرها من التطورات التي سيشهدها المستقبل، ولذلك يجب على المصطلحات القانونية أن تتحلى بالمرونة وبعد النظر .

وكمثال على ذلك، ما اشتمل عليه مصطلح الجرائم الإلكترونية الذي وضعته وحدة مكافحة الجرائم الإلكترونية في نيوزلندا، حيث تضمنت "الهاتف المحمول" كأداة للجريمة[٤٠] .

٢. يشمل مصطلح الجريمة الإلكترونية كل ما هو متعلق بجرائم الحاسوب والإنترنت وغيرها من الجرائم التي تنتج عن تقنيات المعلومات وشبكات الاتصال المحلية، كما تتضمن الجرائم التي تستهدف النظم المعلوماتية والشبكات، فضلًا عن استخدامهم كطرق لتنفيذ جرائم أخرى.

وفيما يلي ستتناول الباحثة أهم المفاهيم التي ذكرت بشأن الجرائم الإلكترونية، ومن ثم سيتم تحديد خصائصها، ومنها إلى طرق اكتشاف هذه الجرائم وأساليبها ومدى صعوبة إثباتها؛ وذلك لكونها ذات طبيعة خاصة.

تعريف الجريمة الإلكترونية:

من الصعب حتى الآن الوصول إلى تعريف محدد وشامل لظاهرة الجرائم الإلكترونية، مما أثار العديد من المشكلات، أهمها عرقلة محاولات إيجاد حلول للحد من انتشار هذه الظاهرة، بالإضافة إلى عدم تقدير حجم الظاهرة، وصعوبة تعاون كافة الدول للتصدي لها والحد منها[٤١] .

وقد قام بعض الباحثين بتعريفها بأنها: الجرائم التي يتم ارتكابها عن طريق الحاسب والذي يعتبر الأداة الأساسية في تنفيذها[٤٢]، وعرفها خبراء منظمة التعاون الاقتصادي والتنمية بأنها: كل تصرف محظور قانونيًا أو أخلاقيًا أو غير مصرح به، ويرتبط ارتباطًا وثيقًا بمعالجة البيانات أو نقلها[٤٣] .

---

[٤٠] محمد بن نصير محمد السرحاني . ٢٠٠٤ . *مهارات التحقيق الفني في جرائم الحاسوب والإنترنت: دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية في العلوم الشرطية* . (رسالة ماجستير) . الرياض: جامعة نايف العربية للعلوم الأمنية . ص . ٢٩.

[٤١] قورة، نائلة عادل محمد فريد . ٢٠١٥ . *جرائم الحاسب الآلي الاقتصادية: دراسة نظرية وتطبيقية* . بيروت: منشورات الحلبي الحقوقية . ص . ٢٨.

[٤٢] هشام محمد فريد رستم . ١٩٩٩ . "الجرائم المعلوماتية: أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين" . *مجلة الأمن والقانون* . دبي . السنة الرابعة . العدد (٢) . ص . ٧٨.

[٤٣] انظر موقع المنظومة على شبكة الإنترنت: تاريخ الدخول للموقع: ٢٠٢١/١٠/١٠ http://www.oecd.org

وتعرف الجريمة الإلكترونية أيضًا، بأنها: الجريمة التي يجب أن يتوافر لدى مرتكبها معرفة كبيرة بتقنيات الحاسب الآلي[٤٤]، كما تم تعريفها أيضًا بأنها: هي مجموعة الجرائم الجنائية التي يمكن ارتكابها من خلال شبكات الإنترنت[٤٥]، وقد رجح البعض أنه يمكن تعريفها بأنها: هي الجرائم التي لا يمكن للحدود الجغرافية أن تحد الجناة من ارتكابها، وأنها: هي الجرائم التي يتم ارتكابها عن طريق الحاسوب أو الإنترنت، ويتوجب على مرتكبها أن يكن شخصًا ذا مهارات كبيرة بتلك التقنيات[٤٦] . ويمكن القول بأن الجرائم الإلكترونية هي مجموعة من السلوك والأفعال غير القانونية، والتي ترتكب من خلال شبكات الإنترنت أو قد تبث محتوياتها عن طريقها[٤٧] .

وفي ضوء الناحية القانونية تعرف بأنها: كل فعل غير مشروع صادر عن إرادة آثمة، ويتشكل في القانون على هيئة عقوبة أو تدبير احترازي ويعتمد هذا النوع من الجرائم على استخدام المعلومة بشكل أساسي، وهذا ما ينص عليه القانون[٤٨]، وتستهدف جرائم الغش المعلوماتي وجرائم المحتوى فئة معينة من الأشخاص لعرض المواد الإباحية وغيرها من جرائم التعدي على الملكية الفكرية، وتعتبر من جرائم التعرض على المصنفات الموجودة على الإنترنت[٤٩] .

---

[44] David Thompson . 1991 . "Current Trends in Computer Crime" . *Computer Control Quarterly* . Vol . (9) . No . (1) . p.2.

[45] La cybercriminalité: "c'est l'ensemble des infraction pénale qui se commettent sur le reseau internet" La définition du minister de l'intérieur francais, disponible en ligne á l'adresse suivant: http://vsabourni.free.fr

٤٦ الجنبيهي منير محمد والجنبيهي، ممدوح محمد . ٢٠١٤ . *جرائم الإنترنت* . الإسكندرية: دار الفكر الجامعي . ص . ١٣.

٤٧ عادل عبد الجواد محمد . ٢٠٠١ . "إجرام الإنترنت" . *مجلة الأمن والحياة* . الرياض: أكاديمية نايف العربية للعلوم الأمنية . العدد (٢٢١) . السنة العشرون . ص . ٧٠.

٤٨ آمال قواجلية .٢٠٢٠. "الجرائم الإلكترونية بين دور النظام القانوني والمعايير الإجتماعية المكتسبة لمستخدمي المواقع الاجتماعية: دراسة حالات لجرائم إلكترونية من القضاء الجزائري قضاء ولاية باتنة". *مجلة دراسات وأبحاث*. جامعة الجلفة. مج ١٢، ع ٣. ص ٦٩٦-٦٩٧.

٤٩ أشرف عبد القادر قنديل .٢٠٢١. "الوسائل الإلكترونية ودورها في الإثبات الجنائي". *مجلة العلوم الشرطية* – أكاديمية العلوم الشرطية بالشارقة. ص ٨٤.

وتعرف الجرائم الإلكترونية أيضًا بالمخالفات التى ترتكب ضد الأفراد بهدف إلحاق الأذى لسمعة الضحية بشكل مادى أو عقلى، ومباشر وغير مباشر عن طريق استخدام شبكات الاتصال مثل الإنترنت (غرف الدردشة، والبريد الإلكترونى، والهاتف)، ويشمل مضمون الجريمة الإلكترونية وصفًا آخر، فالأعمال ذات الصلة بالحاسوب تكون بهدف تحقيق أهداف شخصية أو مكاسب مالية ويتمثل فى أشكال الجرائم المتصلة بالهوية والأفعال ذات صلة بمحتويات الحاسوب جميعها تندرج ضمن معنى أوسع لمصطلح الجريمة الإلكترونية [٥٠].

وقد تناول المشرع الإماراتي تجريم مثل تلك الجرائم التي ترتبط بالمساس بالحاسب الآلي، كباقي مشرعي الدول الأخرى مثل فرنسا[٥١]، فنجد أن الإمارات العربية المتحدة قد تأثرت بما نتج عن تلك الثورة المعلوماتية من مظاهر جديدة متعلقة بالإجرام الذي لم يشهد مثله العالم من قبل، مما دفع المشرع الإماراتي إلى صد هذه الجرائم.

ونظرًا إلى ما سبق ذكره، فإن بعض المفاهيم تتحقق بها الشمولية التي يجب توافرها لتعريف هذه الجرائم، حيث إنها لم تتحدد في الجرائم المرتكبة عن طريق الحاسوب أو شبكة الإنترنت . فنجد مثلًا أن بعض تلك الجرائم تستهدف للكيانات المادية، والأجهزة التقنية التي تتمثل في تخريب وتعطيل شبكات الإنترنت أو سرقة الحاسب، ففي تلك الحالات يمكن اللجوء إلى الطرق التقليدية للتجريم، ويرجع ذلك إلى كونها جرائم تتعلق بالجانب المالي المادي المنقول، بخلاف الجرائم الإلكترونية والتي تتعدى على الكيانات المنطقية التي تتحدد في البرامج والمعطيات، وهنا يعد تطبيق مثل تلك النصوص الجنائية التقليدية عليها أمرًا مشكوكًا فيه.

---

٥٠ آمال قواجلية .٢٠٢٠. "الجرائم الإلكترونية بين دور النظام القانوني والمعايير الاجتماعية المكتسبة لمستخدمي المواقع الاجتماعية: دراسة حالات لجرائم إلكترونية من القضاء الجزائري قضاء ولاية باتنة". ص ٦٩٧.

٥١ طه، أحمد حسام . ٢٠٠٠ . *الجرائم الناشئة عن استخدام الحاسب الآلي* . القاهرة: دار النهضة العربية للنشر والتوزيع . ص . ٨٢.

وعلى النقيض مما تم ذكره، فقد مالت بعض التعريفات بتحديد نطاق هذه الجرائم عن طريق وضع بعض الشروط، ومثال على ذلك، أنه يجب أن يكون مرتكب تلك الجرائم على دراية تامة بتقنية تلك المعلومات، وهى لا تعد شرطًا يتوجب توافره بسبب التطور الهائل في مجال تكنولوجيا المعلومات والتي عملت على تبسيط وتسهيل طرق المعاملة مع تلك التقنيات، مما مكن مرتكبي تلك الجرائم من ارتكاب جريمتهم دون امتلاكهم للدراية التامة بتقنية المعلومات.

بالإضافة إلى ذلك، نجد أن تلك التعريفات قد ميزت بين الجرائم التي ترتكب عن طريق الحاسب والتي تتمثل في مراحل التخزين والمعالجة والاسترجاع وغيرها من جرائم الحاسب[٥٢]، وبين جرائم شبكة الإنترنت أو تقنية المعلومات المنقولة من خلالها والتي تعرف بجرائم الإنترنت، ولكن يعتبر هذا التمييز مخالفًا للمفاهيم التقنية، وغير دقيق نسبةً إلى التطور الذي تشهده هذه التقنيات والتي تقوم في أساسها على المزج بين الحاسوب ووسائل الاتصال بكافة أنواعها، فإن نظام الحاسوب يعتبر مفهومًا يتضمن خلاله جميع الهياكل المادية والمعنوية المرتبطة بعمليات الإدخال والمعالجة والتخزين ونقل المعلومات عن طريق شبكات الإنترنت، مما يثبت وجود أن هناك ترابطًا وثيقًا بين نظام الحاسوب وشبكات الإنترنت، حيث يمكن اعتبارهما فكرة واحدة تكاملية للنظام.

أما بالنسبة للمشرع الفرنسي فقد جاءت المادة (٣٢١-١) من قانون العقوبات الفرنسي الجديد لتتبنى هذه الفكرة، حيث نصت على تجريم الأفعال التي تتحدد في الدخول أو البقاء غير القانوني داخل نظم المعالجة الآلية للمعلومات، ووفقًا للأعمال التحضيرية للقانون فنجد أن الفقه الفرنسي قد اتفق على أن نظام المعالجة الآلية للمعطيات يمكن من خلاله الوصول إلى المعلومات والنظام الذي يتضمنها، بل شملت شبكات المعلومات، وقد صدر القانون المتعلق بالمعلوماتية وحماية الحريات في عام ١٩٧٨م،

[٥٢] يوسف، أمير فرج . ٢٠٠٨ . *الجرائم المعلوماتية على شبكة الإنترنت* . الإسكندرية: دار المطبوعات الجامعية . ص . ١٠٥.

وهدفه وضع مفهوم لنظم المعالجة الآلية للمعطيات[٥٣]، وينص هذا القانون على أن تلك النظم تشمل جميع العمليات التي تتم من خلال الوسائل الإلكترونية، وتتمثل تلك العمليات في تجميع، وتخزين، ومعالجة، وحفظ، ونقل المعلومات، ومن الجدير بالذكر هنا، اتخاذ المشرع الإماراتي نفس النهج، والذي يمكن الاستدلال عليه من القانون (٠٤ – ١٥) من قوانين العقوبات الجنائية بالإمارات، المادة (٣٩٤ مكرر) التي صدرت في ١٠ نوفمبر لعام ٢٠٠٤م.

وتعد الحاسبات الآلية الأداة الأساسية المستخدمة في هذه الجرائم، فيمكن من خلالها الدخول إلى شبكات الإنترنت؛ لأنها تستهدف المعلومات التي يتم معالجتها وتخزينها والتي يتم حفظها وتخزينها في خوادم هذه الحواسيب، والتي يمكن من خلالها الولوج إلى شبكة الإنترنت وإدارتها[٥٤] .

ومما سبق ذكره، يمكن استنتاج أن أكبر المشاكل المتعلقة بالجرائم الإلكترونية ووفقًا للتعاون الدولي هي عدم وجود مفهوم موحد عام بين تلك الدول يمكن من خلاله التوصل للنشاط الذي يتبلور منه هذا النوع من الجرائم، فضلًا عن عدم توافر الخبرة الكافية لدى جهات القضاء والادعاء وأجهزة الشرطة والتي تمكنهم من جمع الأدلة وفحصها، مما يشكل عائقًا أمام المجهودات المبذولة للتصدي للجرائم الإلكترونية.

ويمكن تحديد تلك المجهودات التي تبذلها الدولة في اتجاهين أساسيين، وهما:

الأول: الاتجاه الداخلي والذي تقوم من خلاله الدول بوضع القوانين اللازمة للحد من تلك الجرائم.

---

[٥٣] أيمن أعزان . ٢٠٠٧ . *الحماية الجنائية للتجارة الإلكترونية* . (رسالة دكتوراة) . القاهرة: كلية الحقوق . جامعة عين شمس . ص ١٣١ وما بعدها.

[٥٤] عرب، يونس . *جرائم الكمبيوتر والإنترنت: المعنى والخصائص والصور واستراتيجية المواجهة القانونية* . على الموقع التالي:
www.arablaw.org/download/cybercrimes-general.doc تاريخ الدخول للموقع ٢٠٢١/١٠/١٢

الثاني: الاتجاه الدولي، ويتحقق ذلك عن طريق عقد الاتفاقيات الدولية التي تهدف إلى حماية المجتمع الدولي من الآثار المترتبة على الجرائم الإلكترونية.

الفرع الثاني: أثر الطبيعة الخاصة بالجريمة الإلكترونية على الإثبات الجنائي

تتمتع الجرائم الإلكترونية بطبيعة خاصة جعلتها تعتبر واحدة من أقوى المشكلات التي تواجه الدول للقضاء على هذه الجرائم؛ ويرجع ذلك لصعوبة اكتشافها، وحتى إن تم اكتشافها فيحدث ذلك بمحض الصدفة، فقد أثبتت الإحصائيات أن ما تم اكتشافه من الجرائم الإلكترونية المرتكبة لم يتجاوز (١%) فقط منها، أما بالنسبة للجرائم التي تم الإبلاغ عنها فلم تتجاوز (١٥%) من نسبة الجرائم المكتشفة، وحتى في حالة القضايا التي تم اكتشافها وتم عرضها على القضاء، لم تجمع الأدلة الكافية لإدانة مرتكبيها إلا خمس فقط[٥٥].

ومن هنا نستنتج أنه من الصعوبة إثبات الجرائم الإلكترونية؛ نظرًا لعدم كفاية الأدلة التقليدية التي تقوم على أن الاعتراف سيد الأدلة، ويتبعه شهادة الشهود، ومن ثم القرائن والآثار المادية التي تنتج عن هذه الجرائم، وكل هذا لا يجدي نفعًا في محاولات إثبات الجرائم الإلكترونية . ويرجع هذا القصور إلى ما يأتي:

١. إن طبيعة الجرائم الإلكترونية تخرج من دائرة القضايا الجنائية التقليدية، حيث إنها تقع في بيئة غير تقليدية، فليس لها وجود مادي ملموس كغيرها من القضايا، بل تعتمد في الأساس على وجود الحاسوب والإنترنت، ولذلك تعرف بيئة الجرائم الإلكترونية بمسمى "البيئة الرقمية"، فهي عبارة عن نظام معلوماتي يتكون من نبضات إلكترونية، الأمر الذي من شأنه منح مرتكب الجريمة

[٥٥] حسن، سعيد عبد اللطيف . ١٩٩٩ . *إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت* . القاهرة: دار النهضة العربية . ص . ٩٥.

الإلكترونية القدرة على إخفاء الدلائل أمر في غاية السهولة، بل ولن يتطلب وقتًا كبيرًا لإخفائها[٥٦]، مما يترتب عليه العديد من المعوقات التي تتعلق بكشف هوية الجاني وملاحقته، هنا تدعو الحاجة إلى أهمية تدخل المشرع بوضع حالات الجرائم الإلكترونية كنوع استثنائي من الجرائم، مما يتيح لرجال السلطة القضائية جمع الأدلة اللازمة في أسرع وقت دون انتظار إذن مسبق من النيابة العامة، حرصًا على عدم فقد الأدلة أو تعديلها عن طريق الجاني[٥٧].

وعلى سبيل المثال إحدى الجرائم التي ارتكبت في ألمانيا حين قام أحد الجناة بإدخال تعليمات أمنية في نظام حاسبته هدفها حماية البيانات التي تم تخزينها داخله، من المحاولات التي تسعى للوصول إليها، والتي قد تؤدي إلى محوها بالكامل إذا تم اختراقها عن طريق المجال الكهربائي[٥٨].

٢. في كثير من الأحيان لا يقوم المجني عليه بالإبلاغ عن الجريمة التي تعرض لها، مما يؤدي إلى تزايد مدى صعوبة اكتشافها والتوصل إلى الجاني وإثبات الجريمة، بالإضافة إلى صعوبة دراسة هذه الظاهرة بأكملها، مما يجعل للمجني عليه دورًا سلبيًا في المساهمة للحد من هذه الجرائم، وهو ما يعرف بالرقم الأسود، فمن شأنه زيادة المشكلات والمعوقات في طريق رسم السياسة الجنائية الصحيحة للتصدي إلى هذا النوع من الجرائم واختيار أفضل الوسائل للحد من وقوعها.

ومثال على ذلك، نجد أن بعض الهيئات التي يتم اختراق أنظمتها المعلوماتية تفضل عدم الإفصاح عما قد تعرضت له، حتى بين موظفيها، ولا تقوم بإبلاغ السلطات المختصة وتكتفي فقط باتخاذ إجراءات إدارية، ويرجع ذلك إلى حرصها الشديد على عدم المساس بسمعة تلك الهيئات؛ حتى لا تفقد ثقة عملائها فيها، لهذا نجد أن أكثر المؤسسات عرضة لهذا النوع من الجرائم على المنشآت المالية التي

---

[٥٦] حسن، سعيد عبد اللطيف . *إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت* . ص . ٩٥ وما بعدها.

[٥٧] أيمن عبد الحفيظ . ٢٠٠٤ . "حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية" . *مجلة مركز بحوث الشرطة* . الشارقة . العدد (٢٥) . ص . ٣٧٣.

[58] Sieber, Ulrich . 1986 . *The International Handbook on Computer – Related Economic crime and the Infringement of Privacy* . New Jersey: John Willy and Sons . p.149.

تتمثل في البنوك، والمؤسسات الادخارية، والسمسرة، وغيرها[٥٩]. أو قد يكون الهدف خلف إخفاءه لتعرضه إلى هذه الجرائم، هو حرصه على عدم نشر الوسيلة التي قام الجناة باتباعها حتى لا يقوم الآخرون بتقليدها وتطوير طرقها[٦٠].

وقد تم عقد المؤتمر الدولي الخامس عشر للجمعية العامة لقانون العقوبات في الفترة من ٤ – ٩ سبتمبر لعام ١٩٩٤م في ريو دي جانيرو، والذي قام من خلاله المجلس الأوروبي بالتوصية على أهمية تشجيع المجني عليهم على التقدم بالإبلاغ فور حدوث مثل تلك الجرائم معهم، فمن خلال ذلك يمكن تخفيض الرقم الأسود للجرائم الإلكترونية في الفضاء الأوروبي[٦١].

٣. وتعد أحد أهم أسباب القصور في إثبات الجرائم الإلكترونية هو عدم توافر الخبرات الفنية والتقنية اللازمة لدى سلطات الاستدلال والتحقيق والقضاء، مما قد يؤدي إلى إخفاق الأجهزة القائمة على تنفيذ القانون في تقدير حجم هذه الجرائم، حيث إنها لا تقوم بتوفير وبذل الجهود اللازمة والتي تتناسب مع حجم تلك المشكلة، فظهرت ضرورة القيام بتدريب وتأهيل الجهات المختصة بمجال تقنية المعلومات على طرق جمع الأدلة والملاحقة في البيئة الإلكترونية وأساليبها، فإذا لم يكن المحقق قد تلقى التدريب الكافي قد يقوم بتدمير الأدلة أو إتلافها عن طريق الخطأ، أو بالتعامل بطريقة غير ملائمة مع الأدلة كالأقراص المرنة وغيرها[٦٢].

---

[٥٩] هشام محمد فريد رستم . "الجرائم المعلوماتية: أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين" . ص . ٢٣.

[٦٠] زكي أمين حسونة . ٢٥ – ٢٨ أكتوبر ١٩٩٣ . "جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي" . *بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي* . القاهرة . ص . ٤٧٦ .

[٦١] هشام محمد فريد رستم . "الجرائم المعلوماتية: أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين" . ص . ٢٥-١٧.

[٦٢] حجازي، عبد الفتاح بيومي . ٢٠١٢ . *الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دراسة متعمقة في جرائم الحاسب الآلي والإنترنت* . المحلة الكبرى: دار الكتب القانونية . ص . ٢٨-٢٩.

المطلب الثاني: مفهوم الدليل الإلكتروني

إن عملية إثبات وقوع الجريمة الإلكترونية في غاية الصعوبة لما لها من طابع خاص تختلف فيه عن الجرائم التقليدية، حيث تتطلب وجود دلائل ذات طبيعة خاصة حتى يتم كشف هذا النوع من الجرائم، ويتمثل هذا النوع من الدلائل في استخدام تقنيات الحاسوب والإنترنت، وهو ما يعرف باسم (الدليل الإلكتروني)، وبذلك يمكن القول بأن الدليل الإلكتروني هو الطريقة الوحيدة التي يمكن من خلالها إثبات هذا النوع من الجرائم، وهو ما ستتناوله هذه الدراسة، ففي هذا المطلب ستقوم الباحثة بتناول مفهوم الدليل الإلكتروني (الفرع الأول)، وأهم الخصائص التي تميزه (الفرع الثاني)، بالإضافة إلى أهم تقسيمات هذا الدليل (الفرع الثالث)، وذلك من خلال الفروع التالية:

الفرع الأول: تعريف الدليل الإلكتروني

ستقوم الباحثة في هذا الفرع بتناول أصل الدراسة المتمثلة في مفهوم الدليل الجنائي بشكل عام، حيث يمكن من خلاله التوصل إلى التعرف على ماهية الدليل الإلكتروني.

أولًا: فكرة عامة عن الدليل الجنائي:

الدليل لغة: هو المرشد وما يتم به الإرشاد، وما يستدل به، والدليل هو الدال أيضًا، والجمع أدلة ودلالات[٦٣]، وورد في مختار الصحاح أن الدليل ما يستدل به، وقد دله على الطريق أي أرشده، يدله بالضم، دلالة بفتح الدال وكسرها ودلولة بالضم والفتح أعلى، ويقال أدل، والاسم الدال بتشديد اللام،

[٦٣] صليبا، جميل . ٢٠١٥ . *المعجم الفلسفي* . بيروت: دار الكتاب اللبناني . ص . ٢٣ .

فلان يدل فلانًا أي يثق به، قال أبو عبيد: الدال قريب المعنى من المعني من الهدى، وهما في السكينة والوقار في الهيئة والمنظر وغير ذلك[٦٤] .

والدليل اصطلاحًا: هو ما يلزم من العلم به شيء آخر، وغايته أن يتوصل العقل إلى التصديق اليقيني بما كان يشك في صحته، أي التوصل به إلى معرفة الحقيقة[٦٥].

أما الدليل في الاصطلاح القانوني، فقد كان هناك العديد من المحاولات التي قام بها الباحثون للتوصل إلى وضع تعريف محدد له[٦٦]، حيث ذهب البعض إلى تعريفه بأنه الطريقة التي يستطيع من خلالها القاضي أو يتوصل إلى الحقيقة المنشودة، ويقصد بالحقيقة هنا كل ما له صلة بالوقائع التي يتم عرضها على القاضي حتى يقوم من خلالها بإصدار الحكم بشأنها[٦٧] .

في حين عرفه البعض بأنه الواقعة التي يقوم عن طريقها القاضي باستخلاص البرهان الذي من شأنه التأكد بشكل تام من اقتناعه بالحكم الذي يتوصل إليه[٦٨] . وبالنظر إلى كلا التعريفين نستخلص أن الإشارة إلى الدليل بأنه "الطريقة" أو "الوسيلة" في التعريف الأول أفضل من الإشارة إليه بأنه "الواقعة" في التعريف الثاني، ويرجع ذلك إلى أن لفظ "الواقعة" يطلق على الجريمة نفسها على دليل إثباتها، وأما كلمة "الوسيلة" فهي تطلق على ما يتوصل به إلى الشيء وهو عمل الدليل[٦٩].

---

[٦٤] الرازي، محمد بن أبي بكر بن عبد القادر . ١٩٢٠ . *مختار الصحاح* . القاهرة: المطبعة الأميرية . ص . ٢٠٩ .

[٦٥] أبو القاسم، أحمد . ٢٠١٥ . *الدليل الجنائي ودوره في إثبات جرائم الحدود والقصاص* . الرياض: بحث منشور بالمركز العربي للدراسات الأمنية والتدريب . ص . ١٧٤ .

[٦٦] عزمي، برهامي أبو بكر . ٢٠١٦ . *الشرعية الإجرائية للأدلة العلمية: دراسة تحليلية لأعمال الخبرة* . القاهرة: دار النهضة العربية . ص . ٨٩ وما بعدها .

[٦٧] سرور، أحمد فتحي . ٢٠١٢ . *الوسيط في قانون الإجراءات الجنائية* . القاهرة: دار النهضة العربية . ص . ٤١٨ .

[٦٨] سلامة، مأمون . ٢٠١٦ . *الإجراءات الجزائية في التشريع المصري* . القاهرة: دار النهضة العربية . ص . ١٩١ .

[٦٩] أحمد أبو القاسم . ٢٠١٦ . "المفهوم العلمي والتطبيقي للقانون الجنائي المادي" . *مجلة مركز بحوث الشرطة* . الشارقة . العدد (٢٧) . ص . ١٥٢ .

وقد عرف المشرع المصري الدليل الإلكتروني في المادة الأولى من قانون رقم (١٧٥)[٧٠] لسنة ٢٠١٨م بشأن مكافحة جرائم تقنية المعلومات بأنه: "أى معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة، أو منقولة، أو مستخرجة، أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما فى حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة".

ونظرًا إلى ما قد سبق ذكره، يمكن القول بأن مصطلح الدليل الجنائي يمكن تعريفه بأنه المعلومة التي يقبلها كل من العقل والمنطق، ويمكن التوصل إليها عن طريق إجراءات قانونية محددة، ويمكن من خلالها إثبات مدى صحة انتساب ارتكاب الجريمة لشخص بعينه من عدمه، والهدف من ذلك رفع أو خفض درجة اليقين والاقتناع لدى القاضي في الواقعة . ولذلك فإن أهمية الدليل الجنائي في المواد الجنائية عظيمة؛ وذلك لتجلي دوره في تحويل الشك إلى يقين فيما يتعلق بكشف الحقيقة وإنساب الواقعة إلى الفرد الذي قام بارتكابها، حيث إن الحقيقة بشكل عام تعني كشف حقيقة الشيء بأن يكون أو لا يكون، ولا يمكن تحقيق ذلك إلا عن طريق الدليل باعتباره المعبر عن هذه الحقيقة .

ثانيًا: تعريف الدليل الإلكتروني:

لقد تباينت وتعددت التعريفات التي تم ذكرها فيما يتعلق بالدليل الإلكتروني وفقًا لموضع العلم الذي ينتمي إليه هذا الدليل، فاختلفت ما بين الباحثين في المجال التقني، والباحثين في المجال القانوني، وفيما يلي سيتم التعرض لأهم هذه التعريفات:

[٧٠] المادة (١) من قانون رقم (١٧٥) لسنة ٢٠١٨م بشأن مكافحة جرائم تقنية المعلومات .

لقد قام البعض بتعريف الدليل الإلكتروني بأنه جميع البيانات والمعلومات التي يمكن إعدادها أو تخزينها في شكل رقمي، والتي من خلالها يتمكن الحاسوب من إتمام المهام المطلوبة[٧١]، كما ذهب البعض إلى تعريفه بأنه الدليل الذي تقع الجريمة فيه أساسًا في العالم الافتراضي[٧٢]، فضلًا عن تعريفه بأنه المعلومات التي يعتمدها العلم ويقبلها العقل والمنطق، والذي يمكن الوصول إليه عن طريق الإجراءات القانونية والعلمية من خلال ترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، والتي يمكن عن طريقها إثبات الحقيقة المتعلقة بالجريمة أو الشخص المنسوب إليه فعل معين خلال أي مرحلة من مراحل التحقيق أو المحاكمة[٧٣].

وقد عرف البعض الدليل الإلكتروني بأنه: الدليل الذي يتم استخلاصه من أو عن طريق النظم البرامجية المعلوماتية الحاسوبية، أو من خلال شبكات الاتصال بإجراءات قانونية وفنية محددة، فبعد تحليلها وتفسيرها علميًا وتقنيًا في شكل نصوص مكتوبة أو رسومات أو صور أو أشكال أو أصوات، يتم تقديمها للقضاء حتى يقوم القاضي بتقرير إثبات وقوع الجريمة، كما يقوم بإثبات ما إذا كان الشخص المنسوب إليه الواقعة مدانًا أم بريئًا[٧٤]، وبالنسبة ل "كيسي" فقد قام بتعريف الأدلة الجنائية بأنها الأدلة التي تتضمن كل البيانات والمعلومات الرقمية والتي يمكن من خلالها أن يتم إثبات وقوع الجريمة من عدمها، أو إذا ما كانت توجد علاقة بين الجريمة والجاني أو المجني عليه، والبيانات الرقمية هي مجموعة

---

[71]Christin Sgarlata and David J Byer . 22 September 1998 . "The Electronic paper Trail: Evidentiary Obstacles to Discovery of electronic Evidence" . *Journal of Science and Technology Law* . p 4.

[٧٢] عمر محمد أبو بكر بن يونس . ٢٠١٤ . *الجرائم الناشئة عن استخدام الإنترنت* . (رسالة دكتوراه) . القاهرة: جامعة عين شمس . ص . ٩٦٩.

[٧٣] البشري، محمد الأمين . ٢٠٠٤ . *التحقيق في الجرائم المستحدثة* . الرياض: مركز الدراسات والبحوث . جامعة نايف العربية للعلوم الأمنية . ص . ٢٣٤.

[٧٤] عبد الناصر محمد محمود فرغلى وعبيد سيف سعيد المسماري . ٢٠٠٧ . "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة" . *ورقة بحث مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي المنعقد في الفترة: ٠٢ – ٠٤/ ١١/١١٤٨ هـ الموافق ل ١٢-١٤/١١/٢٠٠٧م* . الرياض . ص . ١٣.

الأرقام التي تشكل العديد من المعلومات، والتي تتخذ شكل نص مكتوب، أو رسومات، أو خرائط، أو صوت، أو الصورة[٧٥]، أما التعريف المقترح للدليل الإلكتروني من قبل المنظمة الدولية لأدلة الحاسوب[٧٦] بأنه المعلومات المخزنة أو المتنقلة في شكل ثنائي، والتي يمكن الأخذ بها كدليل في المحكمة[٧٧]، ويعتبر هذا التعريف أقرب لما ذكره الفريق العلمي العامل على مستوى الأدلة الرقمية، رغبة منهم في توحيد الجهود التي تقوم المنظمة الدولية لأدلة الحاسوب، فضلًا عن تطوير كافة التخصصات والمبادئ التوجيهية حتى يتمكنوا من استرجاع المحافظة ودراسة الأدلة الرقمية بما فيها الصوتية والمصورة[٧٨].

وفي ظل ما سبق ذكره من تعريفات لمصطلح الدليل الإلكتروني، هناك بعض الأمور التي تم ملاحظتها وأولها أنها متقاربة من بعضها البعض، فبالرغم من حداثته وارتباطه الوثيق بمجال التقنية الرقمية، حاولت تلك التعريفات الإلمام بكافة جوانب هذا النوع من الدلائل، إلا أن هناك بعض الملاحظات ينبغي الإشارة إليها وتتمثل فيما يأتي:

خلط بعض الفقهاء لتعريف الدليل الإلكتروني المتعلق ببرامج الحاسب الآلي[٧٩]، حيث عرفه البعض بأنه عبارة عن بيانات رقمية يتم إدخالها إلى الحاسوب بهدف القيام بمهمة محددة، مما ينطبق بشكل تام مع مفهوم برامج الحاسب الآلي[٨٠].

---

[75] Casey, Eoghan . 2004 . *Digital Evidence and Computer Crime-Forensic Science: Computers and the Internet* . London: Academic Press An imprint of Elsevier . p . 260.

[٧٦] المنظمة الدولية لأدلة الحاسوب (IOCE).

http: //www.ioce.org/index?php id =15

[77] Casey, Eoghan . *Digital Evidence and Computer Crime-Forensic Science: Computers and the Internet* . p.261.

[78] www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm تاريخ الدخول للموقع: ٢٠٢١/٩/٢٠

[79] Christin Sgarlata and David J Byer . "The Electronic paper Trail: Evidentiary Obstacles to Discovery of electronic Evidence" . p.53.

[٨٠] محمد مسعود خليفة . ٢٠٠٦ . *الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن* . (رسالة ماجيستير) . الإسكندرية: كلية الحقوق . ص . ٦٣ وما بعدها .

فقد يتوافق كل من المفهومين من حيث أن كليهما يستخدم البيانات والمعلومات الرقمية، والتي تتخذ شكل نصوص أو أحرف، أو أرقام، أو رموز، أو أصوات، أو صور، والتي تتحول بدورها إلى طبيعة رقمية، أي أنها تقوم بترجمة أي ملف معلوماتي يتكون من نصوص كتابية أو صور وغيرها، إلى نظام ثنائي في تمثيل الأعداد يفهمه الكمبيوتر قوامه الرقمان "صفر" و "واحد"[٨١]، بالإضافة إلى وجود برامج تعد دليلًا إلكترونيًا في حد ذاتها، ومثال على ذلك برنامج الاختراق (Asylum_014_fe) [٨٢].

ولا يعني ذلك أن للدليل الإلكتروني وبرامج الحاسوب نفس المفهوم، فيكمن الفرق الأساسي في الركيزة التي يؤديها كل واحد منهما، فنجد أن برامج الحاسوب دورها يتحدد في تشغيل الحاسوب وتوجيهه إلى حل المشاكل ووضع الخطط المناسبة، وبدونها لا يعدو أن يكون مجرد آلة صماء كباقي الآلات، وتتوافر ضمن تلك البرامج برامج خاصة تساعد في عملية الوصول إلى الدليل الإلكتروني مثل: برنامج معالجة الملفات مثل: (أكس تري برو جولد)، وبرنامج النسخ مثل (لاب لينك)[٨٣] .

وهنا يجدر الإشارة إلى الدور الذي يقوم به الدليل الجنائي الرقمي وأهميته فيما يتعلق بمعرفة كيفية حدوث الجريمة الإلكترونية، حيث إنه يقوم في الأساس على إثبات الواقعة وإدانة مرتكبيها، خاصة تلك الجرائم المرتكبة في البيئة الافتراضية، غير المحسوسة، حيث يمكن من خلاله التفتيش في محتويات الأقراص الصلبة بغرض كشف كافة الطرق التي قام بها الجاني أثناء ارتكابه للجريمة.

---

[٨١] عبد المطلب، ممدوح عبد الحميد . ٢٠١٦ . *البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت* . القاهرة: دار الكتب القانونية . ص . ٢٢.

[82] www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm تاريخ الدخول للموقع ٢٠٢١/٩/١٣

[٨٣] ممدوح عبد الحميد عبد المطلب . ٢٠٠٣ . "استخدام بروتوكول (TCP /IP) في بحث وتحقيق الجرائم على الكمبيوتر" . *ورقة عمل مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقد في ٢٦ – ٢٨ نيسان ٢٠٠٣* . دبي . ص . ١٠.

ولا يتحدد هدف الدليل الإلكتروني فقط في إثبات الجرائم الإلكترونية، والتي تتمثل في سرقة الملكية الفكرية، واستغلال الأطفال في المواد الإباحية، والتحرش الجنسي، بل يمكن استخدامه أيضًا في إثبات الجرائم التقليدية كالاتجار بالمخدرات وجرائم القتل والاختطاف وغيرها[٨٤]، حيث تسهم التكنولوجيا الرقمية في كشف طرق قيام الجناة بارتكاب مثل تلك الجرائم بسرعة وكفاءة قد تفوق قدرات المحققين من جهة[٨٥]، بل وعلى العكس قد يتم استخدام هذه البرامج من جانب المجرم حتى يقوم بالاختفاء من العدالة، وذلك لاعتقاده بأن البيئة الإلكترونية منفصلة عن العالم المادي مما يجعلها بيئة مناسبة لممارسة جرائمهم، ولكن هذا الاعتقاد غير صحيح؛ وذلك لأن الجرائم التقليدية أيضًا في بعض الأحيان تكون غير واضحة من دون الإنترنت، ومثال على ذلك، لقد قامت المراقبة الإلكترونية باكتشاف العديد من صفقات المخدرات التي يتم إجراؤها على شبكة الإنترنت، مما يدل على إمكانية المعرفة والتوصل إلى مثل هذه الأنشطة الإجرامية والتي يتداخل فيها كل من العالم المادي والالكتروني معًا، وتشمل ضمنها الأدلة الرقمية، مما يستوجب إعادة النظر إليها على أنها امتداد لمسرح الجريمة المادي[٨٦] .

ولقد تحددت التعريفات التي تمت الإشارة إليها مصادر الدليل الإلكتروني المتعلقة بالنظم الحاسوبية، كما هي معروفة لدى باحثين مجال التقنيات، وتعني كل ما هو متصل ببرامج وأجهزة الحاسب الآلي وملحقاته فقط[٨٧]، ويتضمن ذلك نظم الاتصال أيضًا، وقد كشف العلم في الآونة الحديثة عن نظم

---

[٨٤] البشري، محمد الأمين . *التحقيق في الجرائم المستحدثة* . ص ٢٥٧ وما بعدها.

[85] Karer David Land Kartz A.J . 1996 . *Computer Crime: An Emerging Challenge for Law Enforcement* . F.B.I . Bulletin . Available at: http://www.fbi.gov/leb.96text

[86] Jean-François . 2004 . *Plaideur en faveur d'aménagement de la preuve de l'infraction informatique* . revue de science criminel et de droit pénal compare . No.1 . p.72.

[87] Casey, Eoghan . *Digital Evidence and Computer Crime-Forensic Science: Computers and the Internet* . pp.2-13.

أخرى مدمجة بالحواسيب قد تحتوي على العديد من الأدلة الرقمية، ومثال على ذلك الهواتف المحمولة والبطاقات الذكية[٨٨]، والمساعد الرقمي الشخصي[٨٩] .

ونظرًا لما سبق ذكره، يمكن القول بأن التعريف الأشمل لمصطلح الدليل الإلكتروني هو أنه المعلومات والبيانات التي يتم تخزينها وحفظها في أجهزة الحاسوب وملحقاتها، مما تشمله من دسكات وأقراص مرنة وغيرها من وسائل تقنية المعلومات، بجانب الوسائل المتنقلة عبر شبكات الاتصال، حيث يتم تجميعها وتحليلها من خلال برامج وتطبيقات وتكنولوجيا خاصة حتى يمكن عن طريقها التحقق وإثبات وقوع الجريمة ونسبتها إلى مرتكبيها.

وتتفق دراسة (محمد حمزة أحمد كميل، ٢٠١١)[٩٠] مع ما سبق، حيث إن الدراسة تشير إلى الدليل الإلكتروني على أنه: عبارة عن بيانات رقمية داخل الحاسب الآلي أو منقولة عبره، الأمر الذي يتيح جمع المعلومات وتحليلها عن طريق البرامج الخاصة، وذلك عن طريق استخراج هذه المعلومات لتصدر على شكل رسوم ونصوص أو أصوات وصور، وبالتالي يمكن استخدامها كدليل ضد الجاني أمام المحكمة.

الفرع الثاني: خصائص الدليل الإلكتروني

تعرف البيئة التي يتواجد بها الدليل الإلكتروني بمسمى البيئة الرقمية، وهي بيئة متطورة بطبيعتها، حيث إنها تحتوي على العديد من أنواع البيانات الرقمية، سواء أكانت منفردة أو مجتمعة، حتى يمكن من

---

[٨٨] عنب، محمد محمد محمد . ٢٠٠٧ . *موسوعة العلوم الجنائية، تقنية الحصول على الآثار والأدلة المادية* . الجزء الأول . الشارقة: مركز بحوث الشرطة . ص . ٧٠١ وما بعدها .

[٨٩] عنب، محمد محمد محمد . *موسوعة العلوم الجنائية، تقنية الحصول على الآثار والأدلة المادية* . ص . ٧١٤، وانظر أيضًا لموقع التالي: http://www.zu.edu.eg/users/ahmedsalem/page.asp?id=58 تاريخ الدخول للموقع: ٢٠٢١/١٠/٧

[٩٠] محمد حمزة أحمد كميل . ٢٠١١ . *مدى حجية الدليل الإلكتروني في الإثبات الجزائي* .

خلالها التوصل إلى دليل للإدانة أو البراءة، وقد تأثرت طبيعة وخصائص هذا الدليل وفقًا لهذا العالم الرقمي، أدى ذلك إلى اتصافه بعدة خصائص ميزته عن الدليل الجنائي التقليدي، ويمكن التعرض لها فيما يلي:

١. الدليل الإلكتروني دليلًا علميًا: يشتمل الدليل الإلكتروني على عدد هائل من المعلومات والبيانات الرقمية، ذات هيئة إلكترونية غير الملموسة، والذي يعني أنها لا يمكن إدراكها بالحواس العادية، وحتى يمكن للأفراد إدراكها يتوجب عليهم استخدام أجهزة ومعدات والتي تتمثل في الحاسبات الآلية وملحقاتها، واستخدام نظم برامجية حاسوبية، ويرجع ذلك إلى ضرورة تعامله مع مجال تقني، والذي بدوره يشكل البيئة التقنية التي يتواجد بها الدليل الإلكتروني لكونه من طبيعة تقنية المعلومات، وهنا يمكن القول بأن ما يتم تطبيقه على الدليل العلمي يمكن أن ينطبق على الدليل الإلكتروني، فنظرًا للقاعدة المذكورة في القانون المقارن "إن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة"، نجد أنه يتوجب على الدليل العلمي التجاوب مع الحقيقة كاملة، حيث يخضع الدليل العلمي لمنطقه ولا يخرج عليه أبدًا، إذ يستبعد تعارضه مع القواعد العلمية السليمة، ففي المقابل نجد أن الدليل الإلكتروني يخضع لذات المنطق، فلا يجب أن يخرج هذا النوع من الأدلة عما توصل إليه العلم الرقمي وإلا فقد معناه[٩١].

٢. الدليل الإلكتروني دليلًا تقنيًا: تتشكل خصائص الدليل الإلكتروني وفق البيئة التي يعيش فيها وهي ما تعرف بالبيئة الرقمية أو التقنية التي تكمن في أجهزة الحاسب الآلي وملحقاته، وتتمثل هذه البيئة في الجرائم الإلكترونية التي يتم ارتكابها في هذا العالم الافتراضي . فإن الدليل الإلكتروني يختلف في خصائصه عن الأدلة التقليدية، حيث إن الجرائم الإلكترونية لا تترك

[٩١] بن يونس، عمر محمد أبو بكر . ٢٠١٤ . *الجرائم الناشئة عن استخدام الإنترنت* . ص . ٩٧٧.

خلفها أدلة ملموسة يمكن اكتشاف القاتل من خلالها مثلما يحدث في الجرائم الأخرى، حيث أن هذا النوع من الجرائم يكون ذا طبيعة ديناميكية فائقة السرعة، فإنها تنتقل بسرعة من مكان لآخر خلال شبكات الاتصال التي لا تخضع لحدود الزمان أو المكان، ويرجع ذلك إلى كون هذه التقنية عبارة عن نبضات رقمية لا يمكن تخيل شكلها وحجمها، كما لا يمكن معرفة مكان تواجدها.

٣. الدليل الإلكتروني يصعب التخلص منه: وتعد من أهم الخصائص التي يتميز بها الدليل الإلكتروني عن الأدلة التقليدية بصعوبة التخلص منه، فبالنظر إلى الأدلة التقليدية المتمثلة في الأوراق والأشرطة المسجلة وغيرها، والتي تحمل دليل ارتكاب شخص لجرم ما فيمكن التخلص منها بسهولة عن طريق تمزيقها أو حرقها أو إتلافها، أما بالنسبة لبصمات الأصابع فيمكن التخلص منها عن طريق مسحها من مكان الجريمة، فضلًا عن قيام مرتكبي الجرائم بتهديد أو قتل الشهود حتى لا يتمكنوا من الإدلاء بشهاداتهم، أما بالنسبة للأدلة الرقمية فإن الوضع مختلف تمامًا، فلا يمكن التخلص من هذا النوع من الأدلة، ويرجع ذلك إلى أنه إذا قام الجاني بمحو الدليل أو إتلافه أو إخفاءه بأي شكل، فيمكن استرجاعه وإصلاحه وإظهاره، ويمكن تحقيق ذلك من خلال الكثير من البرامج الحاسوبية التي تقوم على استعادة البيانات والمعلومات التي تم محوها بالأمر أو بإعادة تشكيل القرص الصلب، ومثال على هذا النوع من البرامج نجد: (استعادة البيانات المفقودة)، (رسكيو بوكس)[٩٢]، ويقوم هذا النوع من البرامج على استعادة كافة البيانات والمعلومات بكافة أشكالها سواء أكانت صورًا أو رسومات أو كتابات وغيرها، ويترتب على ذلك صعوبة قيام مرتكب هذا النوع من الجرائم بإخفاء الأدلة على ارتكابها عن

[٩٢] لمزيد من التفصيل حول هذه البرامج انظر الموقع التالي:

http://edu.arabsgate.com/showthread.php?t=502020 تاريخ الدخول للموقع: ٢٠٢١/١٠/٨

أعين الأمن والعدالة، فبمجرد معرفة أفراد البحث والتحقيق الجنائي بوقوع الجريمة أصبح من السهل التوصل إلى الدلائل اللازمة لإدانة الجاني، بل إن نشاط الجاني لمحو الدليل يعتبر دليلًا أيضًا، فإن إثبات هذا النشاط على الجاني والذي يتم تسجيله في الكمبيوتر ويمكن استخلاصه فيما بعد كدليل إدانة ضده[٩٣].

٤. الدليل الإلكتروني قابلًا للنسخ: من الخصائص المميزة لهذا النوع من الأدلة أنه من المتاح الحصول على نسخ مطابقة للأصل من الدليل الإلكتروني الرقمي والتي تتمتع بنفس القيمة العلمية، وهذه الخاصية لا تتوافر في الأدلة التقليدية، مما يتطلب الحرص الشديد في التعامل معها حتى لا تتعرض للتلف أو الفقد أو تغيير المحتوى في حالة نسخ الأصل[٩٤]، وهو الأمر الذي دفع المشرع البلجيكي إلى إضافة مادة (bis 39) إلى قانون التحقيق الجنائي المؤرخ في ٢٨ نوفمبر لعام ٢٠٠٠م، حيث أتاحت من خلالها ضبط الأدلة الرقمية التي تتمثل في نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بهدف عرضها على الجهات القضائية[٩٥].

٥. من أهم خصائص الدليل الإلكتروني هي توافر السعة التخزينية العالية، فعلى سبيل المثال، نجد أن آلة الفيديو الرقمية تستطيع تخزين مئات الصور، بالإضافة إلى أن القرص الصلب الصغير يمكنه تخزين مكتبة صغيرة.. . الخ[٩٦].

---

[٩٣] ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم، وعبد الله عبد العزيز . ٢٠٠٣ . "نموذج مقترح القواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر" . *مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون المنعقد في: ١٠ – ١٢ مايو ٢٠٠٣* . المجلد (٥) . ص . ٢٢٤٠.

[٩٤] عبد الناصر محمد محمود فرغلى وعبيد سيف سعيد المسماري . *الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية: دراسة تطبيقية مقارنة* . ص . ١٥.

[٩٥] بن يونس، عمر محمد ابوبكر . ٢٠١٤ . *الجرائم الناشئة عن استخدام الإنترنت* . ص ٩٧٨.

[٩٦] ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم، وعبد الله عبد العزيز . "نموذج مقترح القواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر" . ص . ٢٢٤١.

٦. يقوم الدليل الإلكتروني بالحصول على المعلومات والبيانات المتعلقة بالجريمة المرتكبة وبالجاني الذي قام بارتكابها، بالإضافة إلى تحليل وتفسير هذه البيانات، حيث يمكنه أن يرصد تحركات الفرد وعاداته وسلوكياته، وغيرها من الأمور الشخصية الخاصة به، لذا فان البحث الجنائي قد يصل إلى هدفه بسهولة أكبر من الدليل التقليدي.

ومما سبق ذكره، يمكن القول بأن هذه الخصائص أضفت على الدليل الإلكتروني طابعًا متميزًا، حيث تبلور في هيئة ذاتية خاصة تختلف اختلافًا تامًا عن الأدلة التقليدية، مما دفعنا إلى التساؤل عن مكانة هذا الدليل ضمن تقسيمات الدليل الجنائي بصفة عامة، وحتى نتمكن من الإجابة عن هذا التساؤل، يجب التعرض أولًا إلى معرفة كافة تقسيمات الدليل الجنائي بما يتناسب وموضوع الدراسة، وفي هذا الصدد نجد أن هناك الكثير من المحاولات الفقهية التي حاولت وضع تصنيفات للدليل الجنائي، ومن أهمها ما يأتي:

تقسيم الدليل من حيث وظيفته إلى: أدلة اتهام، أدلة حكم، وأدلة نفي، بالإضافة إلى تقسيم الدليل من حيث قيمه الإثباتية على النحو التالي:

١. الأدلة الكاملة مثل شهادة الشهود، الدليل الكتابي، القرينة، الاعتراف .
٢. الأدلة الناقصة كما في حالة تواجد شهادة شاهد واحد .
٣. الأدلة الضعيفة أو الخفيفة[٩٧].
٤. الأدلة غير الكافية.

[٩٧] مصطفى، محمود محمود . ٢٠١٥ . *الإثبات في المواد الجنائية في القانون المقارن* . الجزء الأول: النظرية العامة . القاهرة: مطبعة جامعة القاهرة والكتاب الجامعي . ص . ٩.

تقسيم الدليل من حيث صلته بالواقعة المراد إثباتهما: إلى أدلة مباشرة كالمعاينة، وشهادة الشهود، والاستجواب، والتفتيش، أما الأدلة غير المباشرة فمثالها القرائن، والدلائل.

تقسيم الدليل من حيث الجهة التي يقدم إليها: إلى أدلة قضائية، وغير قضائية، فالدليل القضائي هو الدليل الذي له مصدر في أوراق الدعوى أمام المحكمة سواء أكانت في محاضر الاستدلال أم التحقيق، أما الدليل غير القضائي، فهو ما لا يكون في الأوراق المعروضة على القاضي، كأن تكون معلومات شخصية يحصل عليها القاضي بنفسه خارج مجلس القضاء[٩٨] .

الدليل الإلكتروني:

يجب التطرق هنا إلى تقسيم الدليل الإلكتروني والذي سيتم وفقًا لنسبته إلى مصدره، ويرجع ذلك لاعتباره الأساس الذي تعتمد عليه المقارنة القائمة بين الدليل الإلكتروني والدليل الجنائي، حيث يمكن تقسيم الدليل الجنائي إلى أربعة أقسام وهي: أدلة قانونية، وفنية، وقوليه، ومادية، وسيتم التعرض إلى أهم الصفات التي تميز تلك التقسيمات فيما يلي:

١. الدليل القانوني: وهو نوع الأدلة التي لا يصلح دونها الإثبات الجنائي، فهي أساس المواد المدنية والتي يقوم المشرع بتحديدها وتحديد مدى قوة كل منها، فبالنسبة إلى القضايا الجنائية نجد أن للقاضي الحرية الكاملة في اتخاذ القرار فيما يتعلق بصحة أي دليل من الأدلة المتعلقة بالدعوى، ولكن يقوم القانون في بعض القضايا بوضع قيود على قرارات القاضي نظرًا لوجود دليل معين لا يسمح للقاضي الأخذ به، كما يحدد القانون ضرورة وجود أدلة معينة من شأنها السماح

[٩٨] أبو القاسم، أحمد . *المفهوم العلمي والتطبيقي للدليل الجنائي المادي* . ص . ١٦٢.

للقاضي بإصدار حكم الإدانة في القضية[٩٩]، والأمثلة على مثل هذه القضايا لا تعد ولا تحصى، فمثلًا يطبق ذلك على حالة إثبات المسائل غير الجنائية والتي تعرف بالمسائل الأولية، وعند إثبات عقود الأمانة في خيانة الأمانة، وإثبات الزنا على شريك الزوجة الزانية[١٠٠].

٢. الدليل الفني: ويعني الدليل الفني بأنه الدليل الذي يقوم الخبير الفني بإصداره، حيث يعتمد في الأساس على قيمة الدليل المادي منه أو القولي فيما يتعلق بالدعوى، ويكون هذا التقييم قائمًا في الأساس على تقارير فنية يقوم الخبير الفني بإصدارها وفق معايير ووسائل علمية معتمدة[١٠١].

٣. الدليل القولي: يطلق عليه أيضًا الدليل المعنوي أو النفسي، ويقصد بهذا النوع من الدلائل، ذلك الدليل الذي يقوم أفراد بعينهم ممن شهدوا بإحدى حواسهم معلومات وبيانات لها أهمية كبيرة في عملية الإثبات الجنائي، ويتمثل هذا النوع من الأدلة في الاعتراف وأقوال الشهود.

٤. الدليل المادي: هي الأدلة التي من شأنها التأثير على قرار القاضي بشأن الإثبات الجنائي بشكل مباشر، حيث يمكن اعتباره الدليل الذي ينشأ عن عناصر مادية ناطقة بنفسها[١٠٢]، كما يمكن القول بإنه حالة قانونية منطقية تتكون وفق فحص علمي أو فني للدلائل المادية، حيث يمكن الاستنباط من خلاله أمرًا مجهولًا لأثر مادي تخلف عن جريمة ما، ويجب أن تتوافر في هذا الدليل صفات محددة تسمح للخبراء بفحصه وتحديد ذاتيته وهويته، والتي عن طريقها يمكن استكمال التحقيقات للتوصل للإثبات[١٠٣]. وقد قام العديد من الباحثين والفقهاء بإجراء

---

[٩٩] ملالي عبد الله أحمد . ١٩٨٤ . *النظرية العامة للإثبات في المواد الجنائية – دراسة مقارنة بالشريعة الإسلامية* . (رسالة دكتوراه) . القاهرة: كلية الحقوق . جامعة القاهرة . ص . ٣٤٩ .

[١٠٠] مصطفى، محمود محمود . *الإثبات في المواد الجنائية في القانون المقارن* . ص . ٩٠ وما بعدها.

[١٠١] فوده، عبد الحكم . د.ت . *حجية الدليل الفني في المواد الجنائية والمدنية – دراسة علمية على ضوء قضاء النقض* . المنيا: دار الألفي لتوزيع الكتب القانونية . ص . ٧ وما بعدها.

[١٠٢] البشري، محمد الأمين . *التحقيق في الجرائم المستحدثة* . ص . ٢٣٤.

[١٠٣] أبو القاسم، أحمد . *المفهوم العلمي والتطبيقي للدليل الجنائي المادي* . ص . ١٧.

الدارسات المتعددة حول هذا النوع من الأدلة[١٠٤]، ويرجع ذلك إلى أنه يرتبط بشكل مباشر بالوسائل العلمية الحديثة التي تهدف إلى الكشف عن الجرائم وإدانة الجناة.

وهنا يظهر العديد من التساؤلات أهمها: ما موقع الأدلة الإلكترونية ضمن هذه الأنواع؟ هل تندرج الأدلة الإلكترونية ضمن الأدلة المادية نظرًا لكونها ناتج عناصر مادية ملموسة، ويتم استخدام وسائل علمية لاستنباطها؟ أم تندرج ضمن الأدلة الفنية؛ نظرًا لاستخلاصها من رأي خبير فني ووفق معايير علمية معتمدة؟

وبالنظر إلى الدراسات التي تم إجراؤها من قبل الفقهاء، فنجد أن الآراء التي تتعلق بتحديد طبيعة الأدلة الإلكترونية وموقعها من الأدلة الجنائية بصفة عامة قد ذهبت إلى اتجاهين، الاتجاه الأول: يذهب أنصار هذا الاتجاه إلى ترجيح أن الأدلة الإلكترونية تقع ضمن الأدلة المادية الملموسة والتي يمكن للأشخاص إدراكها عن طريق الحواس الطبيعية التي يمتلكونها، حيث إنها تعد مرحلة متقدمة منها، حيث أن هذا النوع من الأدلة يتمثل في مستخرجات الحاسوب من بيانات ومعلومات على هيئة مطبوعات، وقد دعم هؤلاء اتجاههم بالقول بأن الأدلة الرقمية لا تختلف في أهميتها ومفهومها عن الأدلة المادية المتمثلة في آثار الأسلحة وبصمات الأصابع والبصمة الوراثية، وغيرها من الأدلة العلمية[١٠٥].

في حين ذهب البعض الآخر من الفقهاء[١٠٦] إلى عدم وضع الأدلة الرقمية ضمن الأدلة المادية، ولكنها تستخلص من:

---

[١٠٤] أبو القاسم، أحمد . ١٩٩١ . *الدليل المادي ودوره في الإثبات في الفقه الجنائي الإسلامي – دراسة مقارنة* . القاهرة: دار النهضة العربية . ص . ١٨٠ وما بعدها.

[105] Casey, Eoghan . *Digital Evidence and Computer Crime – Forensic Science* . p.5.

[١٠٦] أبو القاسم، أحمد . ١٩٩١ . *الدليل المادي ودوره في الإثبات في الفقه الجنائي الإسلامي – دراسة مقارنة* . اص . ١٧.

١. استخدام الوسائل العلمية الحديثة بهدف الكشف عن أسراره الدفينة، والتي قد يكون لها تأثير كبير على صحة الإنسان جسديًا ونفسيًا، ومثال على ذلك، استخدام جهاز كشف الكذب أو جهاز رسم المخ الكهربائي، وإخضاع الفرد إلى مختلف طرق وأساليب التحليل التخديرية وأمصال الحقيقة، وكذلك استخدام التنويم المغناطيسي.

٢. الوسائل السمعية والبصرية التي تتمثل في مراقبة وتسجيل المحادثات التليفونية، واستخدام العدسات المقربة في عمليات التجسس من خلال التسجيل التليفزيوني والصوتي، وأجهزة التنصت، حيث يعد استخدام مثل هذه الوسائل تعديًا على الحياة الخاصة للإنسان، فنجد أن أهم أسباب استبعاد هذا النوع من الأدلة يكون بسبب عدم القدرة على تحديد أبعادها، حتى إذا أقر كل من الفقه والقانون بمشروعيتها، ويرجع ذلك إلى عدم توافر الأثر المادي الملموس الذي يمكن من خلاله القيام بالمعالجة الفيزيائية لها، حتى إذا تم استنباطها عن طريق أساليب ووسائل علمية، ويمكن تطبيق ما سبق بشكل تام على الدليل الإلكتروني؛ وذلك لكونه عبارة عن نبضات كهرومغناطيسية غير ملموسة، لا يمكن إدراكها بالحواس الطبيعية للأشخاص، بل يجب استخدام برامج وتطبيقات خاصة حتى يتم إدراكها.

وهنا يجب الإشارة إلى أن أنصار الاتجاه الثاني[١٠٧] قد ذهبوا إلى اعتبار الأدلة الإلكترونية نوعًا متميزًا من وسائل الإثبات، كما إنها تمتلك عددًا من الخصائص التي تجعل منها نوعًا جديدًا من الأدلة يمكن إضافته إلى أنواع الأدلة الجنائية الأربعة (القانونية، الفنية، القولية، والمادية)، وهو ما تتفق معه الباحثة، حيث إن الخصائص والصفات التي تتميز بها الأدلة الرقمية تميزها عن غيرها من الأدلة الجنائية الأخرى، وتتمثل تلك الخصائص والصفات في البيئة التي ينشأ منها الدليل الإلكتروني، وهي العالم

[١٠٧] البشري، محمد الأمين . ٢٠٠٤ . *التحقيق في الجرائم المستحدثة* . الرياض: جامعة نايف العربية للعلوم الأمنية . ص . ٢٣٥.

الافتراضي الذي يعتمد في الأساس على الكيفية المعنوية غير الملموسة، وهو ما يحدد طبيعة وقالب الدليل الرقمي في مجال تكنولوجيا المعلومات، وهنا يجب أن يكون الشخص القائم على جمع هذا النوع من الأدلة ملمًا بكافة جوانب مجال تقنية المعلومات.

ونظرًا لما سبق ذكره، فقد تم تأسيس منظمة تسمى المنظمة الدولية لأدلة الحاسوب، والتي قامت الولايات المتحدة الأمريكية بإنشائها، ومن ثم رافقها الفريق المتميز العامل على مستوى الأدلة الرقمية، وكان هدف تأسيس هذا الفريق هو العمل على توحيد الجهود لتحقيق الأهداف التي تسعى إليها هذه المنظمة، بالإضافة إلى ذلك، تم إنشاء المجلة الدولية للأدلة الرقمية[١٠٨]، ومما سبق نستنتج مدى تميز خصائص وصفات الأدلة التكنولوجية عن غيرها من الأدلة الجنائية المادية التقليدية، والذي بدوره يوضح مدى أهمية هذا النوع من الأدلة في مجال التحقيق الجنائي بصفة عامة، والتحقيق الجنائي الرقمي بشكل خاص.

وتتفق دراسة (جاري س كيسلر، ٢٠١١)[١٠٩] مع ما سبق، حيث إنها أشارت إلى أن القضاة أنفسهم يعترفون عمومًا بأن توثيق الأدلة الرقمية يتبع طريقة الدليل التقليدي نفسها، وإن كان أكثر تعقيدًا، مثل مصادقة أنواع أخرى من الأدلة؛ وعلى وجه التحديد يجب إثبات أن الدليل حقيقي وصحيح ودقيق، وذلك على الرغم من أن القواعد الحالية لا بد أن يتم تعديلها لمعرفة قدرات وقيود الأدلة الرقمية، كما عبر معظم القضاة عن الحاجة إلى تدريب إضافي وتعليم للأدلة الرقمية، وقد أشاروا للحاجة إلى التوثيق للأدلة الإلكترونية تمامًا مثل أي نوع من الأدلة المعروضة على المحكمة.

---

[١٠٨] المزيد من التفصيل حول المجلة الدولية للأدلة الرقمية انظر الموقع الخاص بها:
http://www.utica.edu/academic/institutes/ecii/publications/ijde.cfm

[109] Gary C . Kessler . 2011 . "Judges' Awareness, Understanding, and Application of Digital Evidence" . Article (4).

الفرع الثالث: تقسيمات الدليل الإلكتروني

لقد اختلفت سمات وخصائص الجرائم الإلكترونية اختلافًا كبيرًا عن الجريمة التقليدية، حيث إن الجرائم الإلكترونية يتم ارتكابها في بيئة غير مادية تعرف بالعالم الافتراضي الذي يعتمد في الأساس على الكيفية المعنوية غير الملموسة، والتي تتمثل في الحاسب الآلي وشبكة المعلومات الدولية "الإنترنت"، فنجد أن هذه البيئة تتيح لمرتكب الجريمة الإلكترونية بالعبث في المعلومات والبيانات المخزنة على أنظمة الحاسوب وبرامجه عن طريق نبضات إلكترونية رقمية، كما يمكن محوها في زمن قياسي، قد يصل إلى جزء من الثانية، عن طريق استخدام برامج خاصة، مما يعرقل وصول تلك الدلائل إلى أيدي العدالة، حيث تغلب الطبيعة الإلكترونية على الدليل المتوافر . وهنا يجب الإشارة إلى تعدد أنواع وأشكال وصور الدليل الإلكتروني، حيث سيتم عرض هذه الأنواع من خلال نوعين من التقسيمات تتضح فيما يلي:

أولًا: المحاولات الفقهية لتقسيم الدليل الإلكتروني:

لم يقم فقهاء القانون الجنائي بإجراء الدراسات الكافية المتعلقة بالأدلة الإلكترونية، وقد يكون السبب في ذلك الحداثة النسبية لهذا النوع من الأدلة، بالإضافة إلى التطور الكبير الذي يشهده مجال الجرائم الإلكترونية من جهة، وعلى العالم الافتراضي من جهة أخرى، وسوف نذكر هنا محاولة فقهية[١١٠]، تم تقسيم الدليل الإلكتروني من خلالها إلى أربعة أقسام تتمثل فيما يلي:

القسم الأول: الأدلة الرقمية المتعلقة بأجهزة الحاسوب وشبكاها .

القسم الثاني: الأدلة الرقمية الخاصة بالإنترنت .

[١١٠] عبد المطلب، ممدوح عبد الحميد . ٢٠٠٦ . *البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت* . القاهرة: دار الكتب القانونية . ص . ٨٨.

القسم الثالث: الأدلة الرقمية الخاصة ببرتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

القسم الرابع: الأدلة الرقمية الخاصة بالشبكة العالمية للمعلومات.

ومن الجدير بالذكر هنا، مدى التشابه بين هذا التقسيم وبين التقسيم الفقهي الذي تمت الإشارة إليه سابقًا للجريمة عبر الكمبيوتر، والتي يمكن تعريفها بأنها نوع من الجرائم التي يتم ارتكابها من خلال أجهزة الحاسوب والشبكة المعلوماتية المعروفة باسم "الإنترنت" أو "الويب" . وبالنسبة لمصطلح "الويب" فيعرف بأنه عبارة عن مجموعة متكاملة من البيانات والنصوص والمعلومات والصور والصوت والفيديو وهي ذات شكل تشعبي مرتبط على مستوى العالم، أما بالنسبة لمصطلح الإنترنت فهو وسيلة نقل المعلومات عن طريق البروتوكولات الخاصة بالاتصال السلكي واللاسلكي[١١١] . وانطلاقًا مما سبق ذكره تم تقسيمها إلى أربعة أنواع أيضًا .

وبالنظر إلى تقسيمات الدليل الإلكتروني التي تم ذكرها، نجد أنها لا تتضمن كافة جوانب هذا الدليل ولكنها اقتصرت على نوع محدد منه، وهي البيانات المسجلة على الحاسوب التي تتضمن نصوصًا، وعلى الرغم من احتواء الدليل الإلكتروني لجميع المعلومات والبيانات الرقمية التي يتم نقلها، والتي تشمل الصور والأصوات والرسوم وغيرها، فإنها حاليًا تقوم بتطبيق بروتوكولات الاتصالات والتطبيقات المعلوماتية في عمليات التحقيق في الجرائم الإلكترونية، ويعد نظام (تي سي بي/ أي بي)[١١٢] جزءًا أساسيًا من شبكات الإنترنت، حيث إنها تعتبر من أكثر البروتوكولات المستخدمة فيها، فمكن مميزاتها إمكانية التوصل إلى مصدر الجهاز الذي تم استخدامه في الجريمة بشكل مؤكد، كما إنها تعمل على تحديد

---

[١١١] عبد المطلب، ممدوح عبد الحميد . *البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت* . ص . ١٨.

[١١٢] مصطفى، عائشة بن قارة . ٢٠١٥ . *حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن* . الإسكندرية: دار الجامعة الجديدة . ص . ٦٧.

الأجهزة التي تضررت إثر الفعل الإجرامي، بل وتحدد نوعية النشاط الإجرامي خلال الفترة الزمنية التي تم بها ارتكاب الجريمة .

ومما سبق الإشارة إليه يمكن القول بأن أي محاولة تسعى إلى وضع تقسيم محدد للدليل الإلكتروني يجب أن يؤخذ في الاعتبار مدى التطور الذي تشهده البيئة الرقمية التي ينشأ بها الدليل الإلكتروني والتي تشكل خصائصه التي يتميز بها، فهو دليل دائم التطور والتحديث بطبيعته، فمن خلال هذا التطور، والذي غالبًا ما يكون تلقائيًا، وقد تتسع هذه البيئة حتى تستطيع أن تتضمن بداخلها مظاهر رقمية جديدة، وبالنظر إلى حداثة هذه الظاهرة فإنه لا يزال في بداياته، ولكنه يتطور بشكل سريع وواسع ليشمل الكثير والكثير من الأبعاد الرقمية، ولذلك فلن يكون من السهل احتوائه[١١٣].

وبالنظر إلى مدى تنوع وتعدد الدليل الإلكتروني، فإن ذلك يؤدي بدوره إلى تعدد الوسائل التي يمكن من خلالها التوصل إليه، ولكن في جميع الأحوال يظل الدليل المستنبط منه رقميًا، حتى في حالة اتخاذه لهيئات أخرى متعددة ومختلفة، فإذا أقر القانون اعترافه بالهيئة الأخرى التي اتخذها الدليل، ففي هذه الحالة يكون مبنيًا على طابع افتراضي يقوم في الأساس على أهمية الدليل الإلكتروني وضرورته، ولكن نظرًا لعدم توافر الإمكانيات الإلكترونية في المحاكم، فيتوجب في هذه الحالة اتخاذ طريق الافتراض لكونه دليلًا أصليًا حتى يمكن تحقيق التواصل بين القانون وبين هذا الدليل[١١٤].

---

[١١٣] بن يونس، عمر محمد أبو بكر . ٢٠١٤ . *الجرائم الناشئة عن استخدام الإنترنت* . ص . ٩٨٠.

[١١٤] عمر محمد بن يونس . مارس ٢٠٠٦ . "مذكرات في الإثبات الجنائي عبر الإنترنت" . القاهرة: *ندوة الدليل الرقمي بمقر جامعة الدول العربية جمهورية مصر العربية* . ص . ١٢.

المبحث الثاني: إجراءات جمع الدليل الإلكتروني:

لا شك أنه لا يوجد ما يطلق عليه مسمى الجريمة الكاملة مهما حاول الجاني إخفاءها، فبالنظر إلى قاعدة "لوكارد لتبادل المواد" التي تنص على أنه عند احتكاك جسمين، فكل منهما يترك أثره على الآخر، حيث ينتقل جزء من الجسم الأول إلى الثاني، أو العكس[١١٥]، ويتكون نتيجة هذا الاحتكاك الدليل الرقمي، أو الدليل الإلكتروني كما يتم تعريفه في مجال الجريمة الإلكترونية، وتتضمن عملية إثبات الجرائم الإلكترونية العديد من العناصر، نتيجة لصعوبة إثباتها نظرًا لحداثتها، ولذلك يجب على الخبراء جمع كافة عناصر التحقيق والدعوى، ومن ثم يتم تقديمها للسلطات المختصة والتي تعرف باسم سلطة التحقيق الابتدائي، وعلى إثرها تقوم السلطة بالنظر في نتائج هذا التحقيق، فإذا أسفر عن دليل يمكنه إدانة الجاني، يتم تقديمه على الفور إلى المحكمة، وفي المحكمة يأتي دور القاضي الذي يقع على عاتقه اتخاذ القرار بشأن مدى صحة الدليل من عدمه، وإذا ما توافرت الأدلة اللازمة لإدانة المتهم، فإذا لم يقتنع القاضي له السلطة التامة أن يقضي ببراءته .

ويجدر الإشارة هنا، إلى أن المفاهيم السائدة المتعلقة بالإجراءات اللازم اتباعها بغرض التوصل إلى هذا الدليل، سيحدث بها تغيير كبير، إن لم يكن تغييرًا كليًا، نظرًا لعدم كفاية دور بعض الإجراءات التقليدية في ظل التطورات التي تشهدها بيئة تكنولوجيا المعلومات التي تتمثل في المعاينة أو الشهادة على سبيل المثال، مما يؤدي إلى ظهور الحاجة الملحة لإيجاد إجراءات حديثة تتماشى مع طبيعة هذه البيئة.

ووفقًا لما سبق ذكره ستقوم الباحثة بتناول ما يلي:

المطلب الأول: الإجراءات التقليدية لجمع الدليل الإلكتروني.

[١١٥] الحمادي، خالد حمد محمد . *الثورة البيولوجية ودورها في الكشف عن الجريمة DNA* . ص . ١٩.

المطلب الثاني: الإجراءات الحديثة لجمع الدليل الإلكتروني.

المطلب الأول: الإجراءات التقليدية لجمع الدليل الإلكتروني

يقوم المشرع باستخلاص الدليل من خلال عدد من الإجراءات، بهدف تحقيق غاياته، وهي جمع هذا الدليل في كافة الجرائم التقليدية منها والمستحدثة، وأهم هذه الإجراءات، كما بينها القانون، هي المعاينة والتفتيش، وضبط الأشياء، سماع الشهود وندب الخبراء، إلا أن دورها يكون بين المد في الجرائم الأولى والجزر في الثانية، وهو ما سوف نتناوله في الفروع التالية من هذا المطلب.

الفرع الأول: الإجراءات المادية

يتناول هذا الفرع الإجراءات التي يتم اتباعها خلال عملية جمع الأدلة، وهي كما سيتضح خلال هذا الفرع ثلاثة إجراءات، تتمثل في: المعاينة، والتفتيش، والضبط، جميعها إجراءات ذات طبيعة مادية، وفي أغلب الأحيان ينتج عنها نتائج مادية ملموسة، وفيما يلي سوف توضح الباحثة دور كل إجراء في استنباط الدليل الإلكتروني.

أولًا: المعاينة:

أ- فكرة عامة عن المعاينة التقنية لمسرح الجريمة الإلكترونية: في هذا الصدد قام الفقه[١١٦] بتعريف المعاينة بأنها: رؤية بالعين للمكان أو شخص أو شيء لإثبات حالته، وضبط كل ما يلزم لكشف الحقيقة، ولتحقيق هذا الإجراء يتوجب سرعة الوصول إلى موقع الجريمة التي تم ارتكابها بهدف محاولة ضبط الأدلة التي تركها الجاني خلفه لإثبات حالة الموقع، مما يسهل عملية إثبات وقوع الجريمة ونسبتها إلى الجاني الذي قام بارتكابها . وفيما يتعلق بعملية المعاينة أثناء جمع

[١١٦] أبو عامر، محمد زكي . ٢٠٠٢ . *الإجراءات الجنائية* . الإسكندرية: دار الجامعة الجديدة . ص . ٢٣٣.

الاستدلالات، جاءت المادة (٣٥) من قانون رقم ٣٥ لسنة ١٩٩٢م بشأن إصدار قانون الإجراءات الجزائية الإماراتي، والتي جاءت تنص على أنه: "يجب على مأموري الضبط القضائي أن يقبلوا التبليغات والشكاوى التي ترد إليهم في شأن الجرائم، ويجب عليهم وعلى مرؤوسيهم أن يحصلوا على الإيضاحات وإجراء المعاينة اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم أو التي يعلمون بها بأية كيفية كانت، وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة"[١١٧] .

وبالنظر إلى المعاينة بأنها أحد إجراءات التحقيق، فنجد أنه في حالة عدم تواجد حالات التلبس التي نص عليها القانون، فيجب على سلطة التحقيق، أو مأمور تقوم بانتدابه[١١٨]، بتحرير محضر يقوم على كتابته كاتب حتى يتفرغ المحقق ذهنيًا للقيام بالمهام المطلوبة منه، ومن ثم تسلك هذه القضية كافة القواعد والإجراءات التي تحكم المحاكمة، والتي تشتمل على إعلام الخصوم بمكان وزمان المعاينة حتى يتمكنوا من الحضور في وقت إجرائها[١١٩] . فإذا كان لإجراءات المعاينة طريقة لكشف الحقائق المتعلقة بالواقعة، فتقوم المحكمة بإجراء المعاينة، سواء أكان ذلك من تلقاء نفسها أو وفقًا لطلب الخصوم[١٢٠].

من خلال ما سبق ذكره، تم التعرف على الأحكام العامة للمعاينة، وهنا يجب التطرق إلى إجراء المعاينة فيما يتعلق بالجرائم الإلكترونية، وهل تتشابه الجرائم الإلكترونية مع الجرائم التقليدية، بالإضافة إلى التعرف على القواعد التي يجب اتخاذها حتى تتحقق أهداف المعاينة.

---

[١١٧] المادة (٣٥) من قانون رقم ٣٥ لسنة ١٩٩٢م بشأن إصدار قانون الإجراءات الجزائية الإماراتي.

[١١٨] محمد على الجمال . ٢٠٠٠ . "التقاط الدليل المادي من مسرح الجريمة" . *مجلة كلية الدراسات العليا* . العدد (٢) . ص . ١٩٠.

[١١٩] الصغير، جميل عبد الباقي . ٢٠٠١ . *الجوانب الإجرائية للجرائم المتعلقة بالإنترنت* . القاهرة: دار الفكر العربي . ص . ٢٧.

[١٢٠] ثروت، جلال . ١٩٩٣ . *نظم الإجراءات الجنائية* . الإسكندرية: دار الجامعة الحديد . ص . ٤٥٦.

وتعتبر المعاينة أحد أهم الإجراءات المساهمة بدور فعال في الكشف عن الجرائم التقليدية وإثباتها[١٢١]، بغض النظر عن ظهور بعض الحالات التي لا تخضع لهذا الإجراء مثل جريمة التزوير التي تعد جريمة معنوية، وجريمة السب التي تقع بالقول في غير علانية[١٢٢]، ولكن عند الحديث عن مجال الجريمة الإلكترونية فإنها لا تتحلى بنفس الأهمية، نظرًا إلى أن دورها يتمحور حول كشف غموض هذه الجرائم، وضبط الأشياء التي من شأنها إثبات وقوع الجرائم ومدى صحة نسبتها إلى مرتكبيها، ويرجع عدم تميز المعاينة في الجرائم الإلكترونية بالأهمية التي تتميز بها في الجرائم التقليدية إلى العديد من الاعتبارات، وهي[١٢٣]:

١. نظرًا لطبيعة البيئة التي ترتكب فيها الجرائم الإلكترونية، فإنها نادرًا ما تترك خلفها آثارًا مادية ملموسة، حيث إن كل ما ينتج عنها بيانات غير مرئية .

٢. قد يتعرض الدليل للتلف أو التغيير أو العبث نتيجة لكون موقع الجريمة متاحًا للعديد من الأفراد منذ لحظة ارتكاب الجريمة وإلى اكتشاف وقوعها، والذي يسبب بدوره عدم توافر الثقة التامة بالأدلة التي يتم استخلاصها من موقع الجريمة خلال المعاينة .

ووفقًا لطبيعة الجرائم الإلكترونية، فإنها تتيح للجاني إمكانية التلاعب بالأدلة التي تتمثل في عدد من البيانات والمعلومات الرقمية، أو محوها كاملة، كما يمكنه القيام بذلك عن بعد من خلال التدخل من وحدة طرفية، ولهذا السبب يتوجب على المشرع فرض عقوبات جنائية على كل فرد يقوم بإجراء أي تعديل أو محو لأي من البيانات أو المعلومات المخزنة في الحاسوب أو بنك المعلومات أو قاعدة البيانات،

---

[١٢١] سلامة، سعد أحمد محمود . ٢٠٠٧ . *مسرح الجريمة* . القاهرة: دار النهضة العربية . ص . ٣٠.

[١٢٢] رستم، هشام محمد فريد . ١٩٩٤ . *الجوانب الإجرائية للجرائم المعلوماتية: دراسة مقارنة* . أسيوط: مكتبة الآلات الحديثة . ص . ٥٧.

[١٢٣] رستم، هشام محمد فريد . *الجوانب الإجرائية للجرائم المعلوماتية: دراسة مقارنة* . ص . ٥٩.

وذلك في حالة ما قبل اتخاذ سلطة التحقيق لإجراء المعاينة[١٢٤]، وهذا ما ورد عند المشرع الفرنسي من خلال المادة (١/٥٥) من قانون الإجراءات الجنائية الفرنسية[١٢٥]، ويرجع ذلك في الأساس إلى حرصها الشديد على الحفاظ على موقع الجريمة حتى قبل شروعها في البدء بالإجراءات الأولية للتحقيق الجنائي، وهنا نجد أنه بالرغم من أن هذه الأحكام المتعلقة بالمعاينة يتم تطبيقها في الأصل على الجرائم التقليدية، إلا أنها تصلح أيضًا للتطبيق على الجرائم الإلكترونية عند معاينة مكونات الحاسوب ذات الطابع المادي والتي تتضمن أشرطة الحاسوب وكابلاته وشاشة العرض الخاصة به والأقراص وغيرها، ومن الجدير بالذكر، أن هذه الأحكام لا تنطبق على معاينة المكونات غير المادية وذلك لأنها تتطلب إجراءات خاصة .

وبالنظر إلى السمات التي تتميز بها الطبيعة الخاصة التي ترتكب بها الجرائم الإلكترونية، أصبح متاحًا للمحقق أو لمأمور الضبط القضائي الاستعانة بالخبراء الفنيين المتخصصين الذين يقومون بعمليات الفحص وإبداء الرأي فيما يتعلق بالأمور التي يصعب على هؤلاء تفسيرها، ويهدف ذلك إلى دحض أي سبب يدفع إلى التشكيك في مدى صحة هذا الدليل والذي قد يعرقل عملية إثباته .

وتتعدد أشكال وأنواع إجراء المعاينة في الجرائم الإلكترونية وفقًا لنوعية الجريمة التي تم ارتكابها، فعلى سبيل المثال، نجد أن الإجراءات المتخذة في جرائم العدوان على الملكية الفكرية هي القيام بحيازة أو التحفظ على نسخة من المصنف المعتدى عليه عن طريق طباعته أو الاحتفاظ به في هيئة ورقية أو صلبة، وبالنظر للتطور التقني الذي يشهده المجال المعلوماتي أصبحت تستخدم تقنية الطباعة على خشب أو بلاستيك خاص، وبالرغم من ذلك يمكن القول بأن هناك طرقًا متعارفًا عليها تتماشى مع طبيعة البيئة المعلوماتية، ومثال على ذلك، أسلوب تصوير شاشة الحاسوب، ويتم ذلك من خلال آلة تصوير تقليدية

---

١٢٤ مصطفى، عائشة بن قارة . *حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن* . ص . ٨٢.

125 Article (55) du C.P.P.F . dispose que: "Dans les lieux où un crime a été commis, il est interdit . sous peine de l'amende prévue pour les contraventions de la 4o classe, à toute personne non habilitée de modifier avant les premières opérations de l'enquête judiciaire l'état des lieux et d'y effectuer des prélévement quelconques".

أو بواسطة استخدام برمجية خاصة في الحاسوب تعمل على التقاط صورة على الشاشة، وهو ما يعرف باسم "طريقة تجميد مخرجات الشاشة"، كما يمكن حفظ الموقع عن طريق خاصية (save) المتوافرة في نظام التشغيل[١٢٦] .

ب- كيفية إجراء المعاينة التقنية لمسرح الجريمة الإلكترونية: أولى الخطوات التي يتم اتباعها من قبل مأمور الضبط القضائي عند العلم بوقوع الجريمة هي الذهاب الفوري إلى مسرح الجريمة، ويرجع ذلك لكون مسرح الجريمة أهم أركان التحقيق الجنائي، حيث إنه يتضمن الأدلة المادية التي من شأنها إثبات وقوع الجريمة وإدانة الجاني، وهنا يمكن تقسيم مسرح الجريمة الإلكترونية إلى نوعين أساسيين ينبغي التعامل في إطارهما، وهما:

١. مسرح تقليدي: وهو المسرح الذي يتشكل من مكونات ملموسة ومادية للمكان الذي وقعت فيه الجريمة، والتي تقع خارج البيئة المعلوماتية بمكوناتها من الحاسوب والإنترنت، ولهذا يطلق عليه مسمى المسرح التقليدي؛ لأنه يكون أقرب في بيئته من مسرح الجرائم التقليدية، والتي يخلف الجاني خلفه آثارًا مادية متعددة تتمثل في البصمات وبعض المتعلقات الشخصية أو وسائط تخزين رقمية .

٢. مسرح افتراضي: وهو المسرح الذي يقع داخل البيئة الإلكترونية ذاتها، بحيث يتضمن البيانات الرقمية الموجودة بداخل الحاسوب وشبكة الإنترنت، التي يتم تخزينها في ذاكرة الأقراص الصلبة الموجودة بداخله.

ومن الجدير بالذكر هنا، الإشارة إلى أن الانتقال إلى مسرح الجريمة التقليدي، والذي يعتمد على الآثار المادية، لا يتشابه بأي شكل من الأشكال مع التعامل مع المسرح الافتراضي والذي لا يتم من عبر

---

[١٢٦] مصطفى، عائشة بن قارة . *حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن* . ص . ٨٣.

العالم المادي الملموس، بل من خلال العالم الافتراضي، فإن إجراء المعاينة في هذه الحالة قد تتم عبر الحاسوب من مكتب عضو سلطة التحقيق أو مأمور الضبط القضائي في المحكمة، بل ويمكنه القيام بإجراء المعاينة باللجوء إلى بيت الخبرة القضائية أو إلى الخبرة الاستشارية أو حتى إلى مقهى الإنترنت، كما يمكنه أيضًا اللجوء إلى مقر مزود الإنترنت الذي يعتبر أفضل مكان لإتمام إجراء المعاينة[١٢٧] .

ونظرًا لتباين مسرح الجريمة الإلكترونية عن مسرح الجريمة التقليدي لكونه يتميز بوجود الأدلة الإلكترونية ذات الخصائص والسمات التي تتميز بطابعها غير الملموس وغير المرئي، ولهذا يتطلب المعاملة مع هذا النوع من الجرائم في إطار خاص عن طريق إتباع العديد من القواعد الفنية قبل التوجه إلى مسرح الجريمة الإلكترونية، وأهمها ما يأتي:

١. ضرورة توفير معلومات مسبقة عن موقع الجريمة، من حيث نوع وعدد الأجهزة المتوقع مداهمتها، بجانب شبكات الاتصال المتعلقة بها .
٢. وضع خريطة لمسرح الجريمة الذي تتم مداهمته، بالإضافة إلى ضرورة وضع خطة اقتحام هذا المكان، ويجب أن تكون موضحة بالرسومات والمخططات .
٣. تجهيز عدد من المتخصصين ليقوموا بعملية التفتيش، ويجب أن يتوافر مع هذا الفريق مرفقًا بالأمر القضائي اللازم للقيام بالتفتيش، ويرجع ذلك إلى أن الأماكن التي يرتكب بها الجرائم التكنولوجية تكون في الغالب أماكن خاصة[١٢٨] .
٤. الحرص على توافر الأجهزة والبرامج اللازمة والتي يتم استخدامها في عملية الفحص والتشغيل، ومن أمثلتها: برنامج معالجة الملفات، وبرنامج النسخ، وبرنامج (انكسي) الذي يقوم على إنتاج

---

[١٢٧] بن يونس، عمر أبو بكر . ٢٠١٤ . *الجرائم الناشئة عن استخدام الإنترنت* . ص . ٨٩٥.

[١٢٨] محمد الأمين البشري . ٢٠٠٠ . "التحقيق في جرائم الحاسب الآلي والإنترنت" . *المجلة العربية للدراسات الأمنية والتدريب* . المجلد (١٥) . العدد (٣٠) . ص . ٣٥٧.

صورًا مطابقة من القرص الصلب، حيث يطلق عليه الخبراء الفنيون "حقيبة الأدلة الرقمية"، وقد قامت المباحث الفيدرالية الأمريكية باستخدامه بصفة خاصة لأغراض التحقيقات الجنائية .

٥. الحرص على عدم انقطاع التيار الكهربائي عن طريق تأمينه، فإن الانقطاع المفاجئ للكهرباء يؤدي إلى فقد البيانات المخزنة ومحوها من الذاكرة كنتيجة لإغلاق الحاسوب، مما يؤدي إلى فقد الأدلة الإلكترونية التي كان يتم تحصيلها، بالإضافة إلى اتصالات الشبكات، وأنظمة الملفات الثابتة[١٢٩] .

ومن الإجراءات التي يتعين إتباعها عند إجراء المعاينة ما يأتي:

١. ضرورة تصوير جهاز الحاسب الآلي الذي تم من خلاله ارتكاب الجريمة، وكافة ملحقاته من أجهزة جانبية، والمحتويات، والمكان الذي يوجد به بشكل عام، مع مراعاة تصويره من كافة الجهات[١٣٠].

٢. الحرص الشديد على الملاحظة الدقيقة للوسيلة التي تم من خلالها وضع النظام، كما يجب تتبع الآثار الإلكترونية التي تم تركها من قبل الجاني، أو ما قد ينتج عن ولوج النظام أو التردد على المواقع بشبكة المعلومات، وبخاصة السجلات الإلكترونية المتواجدة بشبكات المعلومات، بغرض التوصل إلى موقع الاتصال ونوع الجهاز الذي تم عن طريقه ارتكاب الجريمة الإلكترونية من خلال الدخول إلى النظام أو الموقع[١٣١] .

---

[١٢٩] عبد المطلب، ممدوح عبد الحميد . *البحث والتحقيق الجنائي الرقمي* . ص . ١١٥.

[١٣٠] رستم، هشام محمد فريد . *الجوانب الإجرائية للجرائم المعلوماتية* . ص . ٦٠.

[١٣١] فاضل، سليمان أحمد . ٢٠٠٧ . *المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)* . القاهرة: دار النهضة العربية . ص . ٢٩٠.

٣. مراعاة الدقة الشديدة في عملية نقل المواد المعلوماتية من مسرح الجريمة، والحرص على عدم التسرع، حيث يجب القيام بهذه الخطوة قبل إجراء الاختبارات اللازمة، بهدف التأكد بشكل تام من غياب المجالات المغناطيسية في المحيط الخارجي، والذي قد يؤدي إلى إتلاف البيانات المخزنة على نظم الحاسوب .

٤. العمل على تخزين المعلومات والبيانات الخاصة بالإدخال، وكذلك مخرجات الحاسوب الورقية المتعلقة بالجريمة الإلكترونية التي تم ارتكابها، بالإضافة إلى القيام بجمع الأدلة التقليدية عن طريق رفع ما قد يوجد عليها من بصمات أو آثار مادية قد تركها الجاني .

٥. القيام بربط الأقراص الصلبة، التي قد تحمل في طياتها الأدلة، مع جهاز لا يتيح الكتابة أو التسجيل أو القيام بأي تغييرات على البيانات المخزنة، مما يتيح للمحققين قراءة بياناتها دون التشكيك في صحتها[١٣٢] .

٦. الحرص على التحفظ على محتويات سلة المهملات بما تتضمنه من أوراق وشرائط وأقراص ممغنطة محطمة يتوجب فحصها، ورفع البصمات عنها، فإن هناك احتمالية كبيرة لتضمنها محتويات لها علاقة بالجريمة المرتكبة .

٧. اللجوء إلى المتخصصين الفنيين أصحاب الخبرة[١٣٣] .

وتختلف دراسة (أماندا نجومين، ٢٠١٠)[١٣٤] عما سبق الإشارة إليه، حيث ثبت من المشاركين الخبراء في هذه الدراسة أن قانون الاتصالات والمعاملات الإلكترونية رقم ٢٥ لعام ٢٠٠٢ (أ) لا يوفر مبادئ توجيهية لجمع الأدلة الإلكترونية، وفي جنوب إفريقيا لا توجد إجراءات تم اختبارها من قبل

---

[١٣٢] لمزيد من التفاصيل أنظر الموقع التالي: http://www.paldf.net/forum/showthread.php?T=219932

[١٣٣] مصطفى، عائشة بن قارة . *حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن* . ص . ٨٧.

[134] Amanda Refiloe Ngomane . 2010 . *The use of electronic evidence in forensic investigation* . Diss . University of South Africa.

المحاكم بشأن جمع الأدلة وحفظها وصيانتها، وبينت الدراسة أيضًا أنه توجد معايير عامة راسخة ومعترف بها دوليًا وإجراءات أفضل الممارسات لجمع الأدلة الإلكترونية والتي تشمل على سبيل المثال لا الحصر تحديد الأدلة الإلكترونية وحفظها والحصول عليها والمصادقة عليها وتحليلها.

المطلب الثاني: الإجراءات الحديثة لجمع الدليل الإلكتروني

توجد مجموعة إجراءات تقليدية للحصول على الدليل الإلكتروني، ووضحت الصعوبات التي تحيط بها، وذلك قد يسهل للمجرمين الهروب من العقاب، فيجب أن تتابع التشريعات المتنوعة ذلك التقدم عن طريق نص قواعد قانونية إجرائية حديثة للإجرام غير التقليدي، فمن اللازم الارتكاز على تكونولوجيا المعلومات لجمع الدليل الإلكتروني من أجل تسهيل التفتيش والضبط ولتفاعل الإجراءات مع ذلك التغيير أو تحمل مسؤولية إجراءات حديثة.

ولأن البيانات يمكن أن تصبح متحركة خلال شبكة من الشبكات، فيلزم اتصال الإجراء وماهية المعلومات مع ذلك الإجراء، فالبيانات الساكنة تحتاج لتحفظ سريع، والبيانات المتحركة تحتاج لاحتجاج الاتصالات الإلكترونية الخاصة.

وسوف يتم توضيح ذلك فيما يلي:

الفرع الأول: الإجراءات المتعلقة بالبيانات الساكنة

إن الإجراءات المتعلقة بالبيانات المتحركة أو الساكنة جميعها مستقاة من اتفاقية بودابست المنعقدة في (٢٣ نوفمبر ٢٠١١م)[١٣٥]، وتعد أول معاهدة لمكافحة هذه الجرائم الإلكترونية، وتمت تحت إشراف من المجلس الأوربي ووقعت من قبل ثلاثين دولة، ومنهم أربع دول من غير الأعضاء في المجلس

[135] http://www.convention.coe.int/treaty/EN/terаties/htm1/185.htm تاريخ الدخول للموقع ٢٧-١٠-٢٠٢١

وهي كندا وجنوب أفريقيا واليابان والولايات المتحدة الأمريكة، حيث صدقت عليها في (٢٢ ديسمبر ٢٠٠٦م) وتم فتحها في دول آخرى لترتيب وضبط البيانات والاتصالات بصورة أفضل، وتتكون من (٤٨) مادة موزعة على أربعة أبواب، الباب الأول فيها يعالج: استخدام المصطلحات، والباب الثاني يتناول: الإجراءات اللازمة على المستوى القومي، ويحتوي على ثلاثة أقسام، أولها للقانون العقابي الموضوعي أو المادي، وثانيها: للقانون الإجرائي، وثالثها: للاختصاص القضائي.

أولًا– التحفظ المعجل على البيانات المخزنة:

أقرت اتفاقية بودابست في مادتها (١٦) بأهمية سماح كل طرف لسلطاته بفرض مزود الخدمة التحفظ السريع على البيانات المعلوماتية المحفوظة ومن ضمنها البيانات المرتبطة بالمرور المحفوظة من خلال نظام معلوماتي؛ نتيجة لوجود أسباب تعرض البيانات للتغير أو الفقد خلال ٩٠ يومًا كحد أقصى ويمكن مد تلك المدة.

ويلاحظ أن إجراء حفظ المعلومات يعتبر سلطة قانونية حديثة لمجموعة من الدول بالتحديد العربية مثل مصر والجزائر، فيعتبر وسيلة تلبية جديدة للتصدي للجرائم الإلكترونية، فالمعلومات في تلك البيئة سريعة الفقد والمحو، وقام المشرع الأمريكي بالنص على ذلك الإجراء في القسم (F) (2703C.S U 18) من قانون خصوصية الاتصالات الإلكترونية الأمريكي (ECPA)، وسيتم اختيار معنى ذلك الإجراء وتوضيح المعنى بمزودي الخدمات ودرجة التزامه بالمشاركة مع التحقيق وسلطات التحري[١٣٦].

أ. المقصود بمزودي الخدمات:

[١٣٦] بن قارة، عائشة . ٢٠١٠ . *حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن* . جامعة الإسكندرية: كلية الحقوق . ص . ١٥٤-١٥٥.

هو من يعرض خدمته للجمهور بشكل عام في مجالات الاتصالات الإلكترونية والتي لا تكتفي بمجموعة محددة من المتعاملين بموجب عقد من العقود[١٣٧]، وهناك نوعان من مزودي الخدمة في قانون حماية الحياة الخاصة في مجال الاتصالات الإلكترونية في الولايات المتحدة الأمريكية (ECPA): النوع الأول: مزودو خدمة الاتصالات الإلكترونية، والنوع الثاني: مزودو خدمة معالجة البيانات عن بعد، ويعني بالنوع الأول: كل من يعرض خدمة لمستعملي الشبكة والتي تيسر إرسال واستقبال الاتصالات الإلكترونية والسلكية[١٣٨].

أما النوع الثاني: يعرف طبقًا لقانون خصوصية الاتصالات الإلكترونية الأمريكي في القسم (2) (18 U S.C 2703) أنه "كل من يقدم للجمهور خدمة معالجة البيانات عن بعد بوسيلة من وسائل الاتصالات الإلكترونية".

فإذا أرسل فرد رسالة لفرد آخر من خلال البريد الإلكتروني فمن اللازم أن تمر بمزود خدمة الاتصالات الإلكترونية، وتظل مخزنة لدى مزود الخدمات إلى أن يستلمها المرسل إليه، وبعد الاستلام يتراوح موقفه بين أمرين: إما أن يمحو الرسالة أو يحفظها، وفي حالة تخزينها تعد الرسالة محفوظة من قبل مزود خدمة الاتصالات الإلكترونية.

ب. التزام مزودي الخدمات بمدة معينة للتخلص من البيانات:

---

[١٣٧] عطا الله، شيماء عبد الغني محمد . ٢٠٠٧ . *الحماية الجنائية للتعاملات الإلكترونية* . الإسكندرية: دار الجامعة الجديدة . ص.٢٠٩.

[١٣٨] بن يونس، عمر محمد أبو بكر . ٢٠٠٤ . *الجرائم الناشئة عن استخدام الإنترنت* . (رسالة دكتوراه) . القاهرة: جامعة عين شمس . ص . ٢٨١.

تنص التشريعات المقارنة مثل القانون الفرنسي التزامات على مزودي الخدمات بحذف البيانات المخزنة تلقائيًا والتي ترتبط بالاتصالات الإلكترونية بين مستخدمي الإنترنت والتي لها علاقة بوقت الاتصال وهوية المتصلين[١٣٩].

ج. مفهوم التحفظ المعجل على البيانات المخزنة:

المقصود به "توجيه السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته، وفي انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية "، وهناك مثال لتوضيح الفكرة "قد يعلم رجال الضبط القضائي بوجود صور داعرة للأطفال في اليوم الأول فيقومون باتخاذ إجراءات الحصول على إذن تفتيش في اليوم التالي، وفي اليوم الثالث يحصلون على الإذن ثم يصل علمهم أن المزود قام بشطب السجلات كالمعتاد في اليوم الثالث المذكور".

ومنه يتضح أن التحفظ السريع عبارة عن إجراء تمهيدي أو أولي غرضه الحفاظ على البيانات قبل الفقد، وضحت المذكرة التفسيرية لاتفاقية بودابست أغراض اتباع تلك الإجراءات ومبرراتها في الآتي:

١. سهولة اختفاء البيانات المعلوماتية، حيث تصبح قابلة للتغيير أو الحذف سواء كان الهدف إجراميًا أو غير إجرامي، وذلك في نطاق الحذف الطبيعي للمعلومات التي لم يعد لها استخدام.

٢. تحدث الجرائم الإلكترونية في الغالب من خلال نقل الاتصالات عبر نظم الحاسوب، فمن الممكن احتواءها علي محتويات غير مشروعية، مثل مواد فيروسية أو مواد إباحية للأطفال، أو

[139] Art . L . 32-3-1 alinéa 1 du code des postes et télécommunications dispose que : 11 Les opérateurs de télécommunications et notamment ceux mentionnés à l'article 43-7 de la loi n°86-1067 du 30 septembre 1986 précitée . sont tenus d'effacer ou de rendre anonyme toute donnée relative à une communication dès que celle - ci est achevée . sous réserve des dispositions des II, III et IV"

إثباتات لجرائم آخرى مثل الاتجار بالمخدرات فيمكن معرفة مرتكب الجريمة من خلال تحديد مصدر الاتصالات.

٣. الحفاظ على الدليل الإلكتروني من خلال نسخ الاتصالات غير المشروعة أو إثباتات لنشاط جنائي من خلال مزودي الخدمات، كالمراسلة الإلكترونية المستقبلة أو المرسلة وهكذا تُكشف أدلة الجرائم.

ومن اللازم توضيح أن بيانات المرور المرتبطة باتصالات سابقة تندرج ضمن البيانات المعلوماتية المشمولة، وهذا لمعرفة خط سير الاتصال سواء مكان أو مصدر تلك الاتصالات والتى تعتبر من الأمور الجوهرية لتحديد هوية الأفراد موزعي مواد إباحية طفولية علي سبيل المثال، وعرفت اتفاقية بودابست في مادتها الأولى في الفقرة "د" ذلك الشكل من المعلومات (البيانات المتعلقة بالمرور) "بأنها صنف من بيانات الحاسوب التي تشكل محلًا لنظام قانون محدد، حيث يتم توالد هذه البيانات من الحواسيب عبر تسلسل حركة الاتصالات لتحديد مسلك الاتصالات من مصدرها إلى الجهة المقصودة، وبذلك فهي تشمل طائفة من البيانات تتمثل في: مصدر الاتصال ووجهته المقصودة، خط السير ووقت أو زمن الاتصال وفقًا لتوقيت غرينتش، حجم الاتصال ومدته ونوع الخدمة المؤداة (مثل نقل الملفات أو بريد إلكتروني أو مراسلات فورية)، وفي الغالب يكتسب مقدم الخدمة معلومات المرور الكافية لتحديد مصدر الاتصال أو نهايته بدقة، ويملك كل واحد جزءً من أجزاء اللغز ويجب أن توضع تحت الاختبار لمعرفة مصدرها والجهة المرسلة لها[١٤٠].

[١٤٠] بن قارة، عائشة . ٢٠١٠ . *حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن* . ص . ١٦٠.

ثانيًا: الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك:

تندرج المعلومات الشخصية المرتبطة بمستعملى الشبكة ضمن إطار الحق في الخصوصية التي تدافع عنه الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية (٤ نوفمبر ١٩٥٠م)، لا يسمح بالإعلان عن أي بيانات للغير من قبل مزود الخدمات أو غيره، وهناك مجموعة من التشريعات المقارنة التي تجيز لرجال الضبط القضائي طلب المعلومات من الأفراد والتي تُعرض كإثبات، ومن ضمنها الخاصة بالمشترك التى يملكها مزودو الخدمات، وهو ما يقره القانون الفرنسي (٧١٩ لعام ٢٠٠٠) الذي عُدل للقانون (١٠٦٧ لعام ١٩٨٦) المتعلق بحرية الاتصالات، حيث تنص المادة (٣٤-٩) من على "أنه يتعين على مزودي خدمات الدخول والمسكّنين المحافظة على بيانات مستعملي خدماتهم؛ وذلك تمهيدا لطلب السلطات منهم تلك البيانات التي قد تفيد كدليل في جريمة معية وقعت بالفعل".

وفيما يتعلق باتفاقية بودابست تنص المادة (١٨)[١٤١] على "أنه يجوز للدول الأطراف في تلك الاتفاقية تمكين السلطات المختصة من إلزام مقدمي الخدمات تقديم البيانات المتعلقة بالمشترك، سواء كانت في حيازته المادية أو تحت سيطرته، حيث تكون هذه البيانات مخزنة بعيدًا عن الحيازة المادية لمزود الخدمة، ولكن يمكن السيطرة عليها، ومثال ذلك، أن تكون البيانات مخزنة في وحدة تخزين عن بعد ويتم تقديمها عن طريق شركة أخرى"، ويلزم أن تكون معلومات مخزنة، ويتستثني أي بيانات تخص محتوى وعلاقة البيانات المتعلقة باتصالات مستقبلية.

ويلزم اختيار السلطة المختصة بإعلان أمر عرض المعلومات، فلرجال السلطة العامة الحق في إعلان مثل ذلك الأمر إذا ارتبط بمعلومات المشترك المعلنة للجمهور، ودول أخرى تُلزم السلطات

[١٤١] المادة (١٨) من اتفاقية بودابست.

القضائية بإعلان الأمر، في حال التوصل لشكل محدد من المعلومات المتربطة بالحق في الخصوصية كحساب بنكى للمشترك أو رقم بطاقة ائتمان[١٤٢].

الفرع الثاني: الإجراءات المتعلقة بالبيانات المتحركة (اعتراض الاتصالات الإلكترونية)

تظهر إجراءات البيانات المتحركة في اعتراض[١٤٣] الاتصالات الإلكترونية الخاصة، والمقصود بذلك الإجراء متابعة الاتصالات الإلكترونية خلال عرضها، وليس الوصول للاتصالات الإلكترونية المحفوظة، وهذا لوجود نوعين لكل منهما قواعد، ذلك من ناحية شدة ضمانات التوصل لها في الأولى وسهولتها في الثانية، وتظهر مشكلة اختيار ماهية البريد الإلكتروني المغلق والمنتظر داخل صندوق خطابات الذي يعرض خدمات الإنترنت إلى أن يدخلها المرسل إليه في نظامه المعلوماتي، فهل تعد بيانات معلوماتية محفوظة وتنفذ عليها إجراءات البيانات الساكنة، أم هي معلومات في مرحلة النقل والتحويل فتنفذ عليها إجراءات البيانات المتحركة المتشكلة في اعتراض الاتصالات الإلكترونية، ولم يصلوا إليها إلا من خلال سلطة الاعتراض.

وقد فرقت اتفاقية بودابست بين شكلين من البيانات المعلوماتية، البيانات المتعلقة بمحتوى الاتصال، والبيانات المتعلقة بالمرور، وعرفت الاتفاقية النوع الأول في المادة الأولى منه أنها "كل البيانات التي تعالج الاتصالات والتي تمر عن طريق نظام معلوماتي، والتي يتم إنتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصرًا في سلسلة الاتصال، مع تعيين المعلومات التالية: أصل الاتصال، مقصد الاتصال أو الجهة المقصودة بالاتصال، خط السير، ساعة وتاريخ، حجم وفترة الاتصال، أو نوع الخدمة".

---

[١٤٢] بن قارة، عائشة . ٢٠١٠ . *حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن* . ص . ١٦٢.

[١٤٣] عطا الله، شيماء عبد الغني محمد . ٢٠٠٧ . *الحماية الجنائية للتعاملات الإلكترونية* . ص . ٣٠٥ ومابعدها.

والنوع الثاني "البيانات المتعلقة بمحتوى الاتصال" لم يُذكر له تعريف في الاتفاقية لكنها توضح المحتوى الإخباري للاتصال، بمعنى مضمون الرسالة أو الاتصال أو البيانات المنقولة من خلال الاتصال باستثناء معلومات المرور.

ويوضح ذلك نوعًا من التقارب بينهما من حيث المعنى، ولكن من حيث المساس بالحق في الخصوصية يختلفان تمامًا، حيث إنها مهمة بنسبة أكبر لمراقبة محتوى الاتصال أو المراسلة، ويتم وضع ضمانات أكثر عن الإلمام بمحتوى البيانات في الوقت الفعلي عن حركة المعلومات من حيث السلطة والجرائم.

وأثبتت اتفاقية بودابست ذلك التفريق حيث قسمت كل إجراء بعنوان مختلف، أطلقت على تجميع حركة البيانات بعنوان "التجميع في الزمن الفعلي لبيانات المرور"[١٤٤] المادة رقم (٢٠)، وتجميع محتوى البيانات بعنوان"اعتراض محتوى البيانات"[١٤٥] المادة رقم (٢١).

وتقر الدولة مفهومًا واحدًا لجميع من تجمع حركة المعلومات ومراقبة محتوى المعلومات وبعضها تطبق عليه نفس الضمانات الخاصة عند استخدام إجراء منهما، دون الانتباه للحساسية المتعلقة بأمر مراقبة محتوى المعلومات، وذلك نتيجة لغياب التفريق في القانون الذي لا يتميز باختلافات لمنفعة في الخصوصية أو لتماثل إجراءات التجميع التقني، ومن تلك الدول فرنسا.

ويعتبر حق الإنسان في الخصوصية مقيدًا بالمنفعة العامة في أمر الجريمة ومعاقبة الجناة، مما يتطلب توازنًا واضحًا بين حق المجتمع في العقاب والحق في الخصوصية، وللتوصل لذلك التوزان يجب أن تحاط المراقبة بضمانات تهتم باستخدامه في حيز الهدف الذي شرع من أجله، ومن ثم سيتم تناول النقاط

[144] Collect en temps reels des données relatives au trafique.
[145] Interception de donnée relatives au contenue.

التالية: أولًا: مدى تمتع الاتصالات بصفة عامة والإلكترونية بصفة خاصة بالحماية الجنائية، ثانيًا: الحالات التي يحدث فيها الاعتراض سواء أكان من خلال إذن أو بغيره.

أولًا: حرمة الاتصالات الإلكترونية الخاصة:

من المؤكد مساس مراقبة الأحاديث الخاصة بحق الفرد في الخصوصية وسرية أحاديثه، وهو حق مرتبط بالفرد ذاته[١٤٦]، وأصبح هذا الحق مهددًا بسبب التقدم التكنولوجي الذي أدى لظهور أدوات مراقبة ذات تقنية، وتلتقط أحاديث الأفراد ولم تكتفِ بالتنصت (اعتراض) على الاتصالات اللاسلكية والسلكية فقط[١٤٧]، بل وصلت بقدرتها الضخمة إلى تسجيل الاتصالات التي تحدث عبر الإنترنت، مما ضيع حرية الفرد وخصوصيته وهدد إنسانيته وكرامته، حيث أطلق بعض الفقهاء على أجهزة المراقبة بأنها نكسة نتيجة للتطور المذهل للأجهزة الحديثة.

وقد اهتمت أغلب التشريعات بإتاحة كمية كبيرة من الحماية الجنائية المتعلقة بسرية الاتصالات الخاصة للأشخاص، حيث إن المشرع المصري عاقب بالحبس لمدة عام أو أكثر كل من انتهك حرمة الحياة الخاصة في حال ارتكاب تصرف من التصرفات الآتية في ظروف غير المصرح بها في القانون أو بدون موافقة المجنى عليه:

أ. التنصت أو قام بتسجيل أو نقل محادثات هاتفية أو خاصة من خلال أحد الأجهزة بغض النظر عن نوعها.

---

[١٤٦] ياسر الأمير فاروق محمد . ٢٠٠٨ . *مراقبة الأحاديث الخاصة في الإجراءات الجنائية: دراسة مقارنة* . (رسالة دكتوراه) . كلية الحقوق . جامعة القاهرة . ص . ١١.

[147] Guerrier (C) . *les écoutes téléphoniques* . N.R.S . Droit . Paris p . 1 .

وانظر كذلك : فتحي عبد النبي الوحيدي . ١٩٩٨ . "الأثر السلبي للتطور التكنولوجي على الحريات الشخصية" . *مجلة روح القوانين* . العدد (١٣) . ص . ٢، وانظر أيضا: عفيفي، عفيفي كامل . د.ت . *جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ودور الشرطة والقانون، دراسة مقارنة* . ص . ٢٦٤ وما بعدها.

ب. أخذ أونقل صورة شخصية لفرد في مكان خاص عن طريق جهاز بغض النظر عن نوعه.

وبالاطلاع على نص المادتين للقانونين الإماراتي والمصري، يتضح أنهما يرتبطان بالمكالمات الخاصة التي تحدث من خلال الهاتف أو في مكان خاص[١٤٨]، غير محادثات الكمبيوتر والبريد الإلكتروني أو المحادثات الفورية.

حيث يجب على المشرعين الإماراتي والمصري أن ينصا القوانين، لترتيب وضع المحادثات الإلكترونية القانوني، لأن تلك المحادثات تمت من خلال خط هاتفي، ومن ثم فهي طريقة للدخول إلى الشبكة.

ثانيًا: الاعتراض المشروع للاتصالات الإلكترونية الخاصة:

يعتبر التعدي على المحادثات الإلكترونية خطرًا، ولكن في بعض الحالات يعتبر مسموحًا به بغير إذن.

أ. سلطة مزود الخدمات في مراقبة النظام دون إذن:

يكون ذلك نتيجة لشكوى المشترك، أو في مجال المراقبة التقليدية لمزود الخدمة الخاصة بعمل الشبكة، وسنوضح في التالي:

١. المراقبة المعتادة لمزود الخدمة لعمل الشبكة:

[١٤٨] سرور، طارق . ٢٠٠٤ . *حق المجني عليه في تسجيل المحادثات التليفونية الماسة بشخصه* . القاهرة: دار النهضة العربية، ٢٠٠٤ . ص . ١٨ وما بعدها.

أقرت التشريعات المقارنة في المادة رقم (١) (C.S I 2511 (2) 18 U) إمكانية مراقبة الاتصالات الإلكترونية للمشتركين من قبل مزودي الخدمة، للحفاظ على أنظمتهم من أضرار الاستخدام أو سرقتهم.

ومن التطبيقات القضائية لذلك السماح لمزودي الخدمات بالمراقبة للتصدي لسرقة الخدمات والغش، وأمثلتها تزوير خط هاتف للانتفاع بخدمة دون دفع اشتراك، حيث يحتاج من مزود الخدمة أن يراقبه لمعرفة مكانه والفاعل[١٤٩].

٢. المراقبة بناء على شكوى المشترك:

تفاوتت التشريعات المقارنة بخصوص الموافقة على مراقبة الاتصالات الإلكترونية من قبل السلطات نتيجة لمطالبة صاحب الجهاز محل الاعتداء بأن تتم مراقبة جهازه من قبل رجال الضبط القضائي، وظهر أمر يؤيد تلك المراقبة وأمر يعارضها[١٥٠].

ب. اعتراض الاتصالات الإلكترونية بناء على إذن:

لا تكتفي الحماية التي يفرضها المشرع على ذلك الشكل من الاتصالات، ولكن يصل لحماية الاتصالات الإلكترونية من خلال الإنترنت، حيث تعد تلك الحماية من أجل الحياة الخاصة بالأفراد بالحفاظ على أسراره الشخصية التي تكون معرضة للانتهاك في حال عدم استخدام الطرق الإلكترونية للوصول لها، لذلك تتطلب حماية أكثر من الاتصالات العادية، وإذا احتاج التحقيق لاعتراض تلك

---

[١٤٩] عطا الله، شيماء عبد الغني محمد . ٢٠٠٧ . *الحماية الجنائية للتعاملات الإلكتروني* . ص . ٢٢٢.

United States v . Pervaz, 118 F.3ed . 1,5 (1st Cir)

[١٥٠] بن قارة، عائشة . ٢٠١٠ . *حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن* . ص . ١٧٢.

الاتصالات، فسيتم نص ضمانات مثل المحادثات الهاتفية، مع الحفاظ على سرية تلك الاتصالات الحديثة، وتتمثل الضمانات القانونية في التالي:

١. السلطة المختصة بإصدار إذن الاعتراض:

تختص السلطة القضائية بشكل عام بإعلان الإذن، ويعتبر ذلك ضمانة أساسية لمشروعية الاعتراض على الاتصالات السلكية واللاسلكية في القانونين الإماراتي والمصري، فتعتبر ضمانات مخالفة لافتئات أجهزة الدولة المتعلقة بحرمة الحياة الخاصة، أقر الدستور المصري في المادة رقم (٤٥) على هذه الضمانة وجاءت المادتان (٩٥و٢٠٦) من قانون الإجراءات الجنائية لتثبت ذلك، ويتضح منهما أن المشرع ألزم إعلان الإذن بالاعتراض من خلال قاضي التحقيق المختص أو القاضي الجزئي ومنع النيابة العامة من إعلانه، بهدف تقليل سلطتها تجنبًا للتعسف، وفي حالة مسؤولية النيابة العامة عن التحقيق واكتشافها أهمية اعتراض المحادثات التليفونية للمتهم، فمن الضروري أن تحصل على إذن بموجب نص المادة (٢٠٦ إجراءات مصري) من قبل القاضي الجزئي بمتابعة المحادثات الهاتفية[١٥١]، وهو ما أثبتته محكمة النقض في الحكم "أن المشرع أباح لسلطة التحقيق وحدها وهي قاضي التحقيق وسلطة الاتهام في أحوال التصدي للتحقيق أو إجراء تحقيقات تكميلية وللنيابة العامة في التحقيق الذي تجريه بعد استئذان القاضي الجزئي"، ولا يلزم تنفيذ أمر الاعتراض من قبل النيابة العامة أو قاضي التحقيق في حالة إعلان الإذن، ومن حقهم توكيل ذلك لمأمور الضبط القضائي[١٥٢].

ويجب توضيح ماهية الدليل الإلكتروني الخاصة من حيث اختفاءه وسرعة فقده، تلزم بتقليل حدة شرط أهمية استئذان النيابة العامة للقاضي الجزئي لتسهيل متابعة الاعتراض حين توليها التحقيق في

---

[١٥١] هبة أحمد علي حسانين . ٢٠٠٧ . *الحماية الجنائية لحرمة الحياة الخاصة: دراسة مقارنة* . (رسالة دكتوراه) . القاهرة: كلية الحقوق . جامعة عين شمس . ص . ٣٩٦ .

[١٥٢] هبة أحمد علي حسانين . ٢٠٠٧ . *الحماية الجنائية لحرمة الحياة الخاصة: دراسة مقارنة* . ص . ٣٩٦ .

جريمة من الجرائم الإلكترونية وتوضح لها أهمية تسجيل واعتراض الاتصالات الإلكترونية من خلال الإنترنت.

٢. فائدة الاعتراض في إظهار الحقيقة:

يعد "ضابط فائدة المراقبة في ظهور الحقيقة" السند الشرعي المعلل للاعتراض، نتيجة لتضمن الاعتراض اعتداءً ضخمًا على سرية الاتصالات وحرمة الحياة الخاصة، وومن ثم يسمح بالاستبعاد وفي حدود محدودة وذلك لمنفعته المنتظرة المرتبطة بوضوح الحقيقة بضبط الجناة وإظهار غموض الجريمة[١٥٣]، ويكون القاضي الجزئي أو قاضي التحقيق مسؤولين عن تقدير درجة منفعة اعتراض المحادثات الهاتفية في عرض الحقيقة ويرضخ لرقابة قضاء الموضوع[١٥٤].

٣. تسبيب الإذن القضائي الصادر باعتراض الاتصالات الإلكترونية:

من حق القاضي إعلان إذن تتبع الاتصالات الإلكترونية؛ نتيجة لأعمال الاستدلال التى أداها مأمور الضبط القضائي ووضح من خلالها أهمية إعلان الإذن بالموافقة لضرورة وضوح الحقيقة في جريمة نُفذت تتعلق بالجريمة الإلكترونية، وذلك السبب ينتج بشكل عام من درجة اقتناع القاضي بأهمية التحريات التي نفذها مأمور الضبط القضائي، والسبب الناتج عنه الإذن القضائي؛ نتيجة لتعدى الإجراء على حريات الأشخاص، فهو استثناء على القاعدة العامة والتي تتشكل في حرمة الحياة الخاصة للمواطنين وحقهم في خصوصية اتصالاتهم ومراسلاتهم.

---

[١٥٣] عقيدة، محمد أبو العلاء . ١٩٩٤ . مراقبة *المحادثات التلفونية: دراسة مقارنة* . القاهرة: دار الفكر العربي . ص . ١٩٢.

[١٥٤] حسني، محمود نجيب . ٢٠١٢ . *شرح قانون الإجراءات الجنائية* . القاهرة: دار النهضة العربية . ص . ٦٦٨.

٤. الجرائم التي يجوز فيها الاعتراض:

ارتكز المشرع المصري على مقياس جسامة العقوبة، حيث خصص في المادتين (٩٥و٢٠٦) الجرائم المسموح الاعتراض فيها، وهي الجنح والجنايات التي تصل عقوبتها لثلاثة أشهر أو أكثر، ويلزم وقوع الجريمة لتصبح محلًا للاعتراض، حيث يبنى عليه أهمية إعلان الإذن بالاعتراض، أما المشرع الإماراتي فنجد أنه يطبق نصوص القانون الاتحادي رقم (١٢) لسنة ٢٠١٦، بتعديل المرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات، وغيره من القوانين المتعلقة بحماية الخصوصية، ومنع انتهاك البيانات الشخصية عند استخدام وسائل التواصل الاجتماعي، حيث تنص المادة (٢١)[١٥٥] من القانون كل من استخدم شبكة معلوماتية، أو نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانوناً بإحدى الطرق الآتية:

أ. استراق السمع، أو اعتراض، أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية.

ب. التقاط صور الغير أو إعداد صور إلكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها.

ج. نشر أخبار أو صور إلكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية.

[١٥٥] المادة (٢١) من المرسوم بقانون الاتحادي رقم (١٢) لسنة ٢٠١٦م بتعديل المرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات .

كما تحظر المادة رقم (٢٢)[١٥٦] من القانون كل من استخدم، بدون تصريح، أي شبكة معلوماتية، أو موقعاً إلكترونيًا، أو وسيلة تقنية معلومات لكشف معلومات سرية حصل عليها بمناسبة عمله أو بسببه.

وعلاوة على ذلك، تحظر المادة رقم (٣٧٨)[١٥٧] من قانون العقوبات الإماراتي كل من اعتدى على حرمة الحياة الخاصة أو العائلية للأفراد؛ وذلك بأن ارتكب أحد الأفعال في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه:

أ- استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيًا كان نوعه محادثات جرت في مكان خاص أو عن طريق الهاتف أو أي جهاو آخر.

ب- التقط أو نقل بجهاز أيا كان نوعه صورة شخص في مكان خاص .

ج- فإذا صدرت الأفعال المشار إليها في الحالتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك فإن رضاء هؤلاء يكون مفترضًا.

٥. مدة الاعتراض:

اهتمت التشريعات الحديثة بتحديد وقت محدد للاعتراض لتجنب التعسف وإساءة استخدام السلطة، غير أنها لم تتبع شكلًا واحدًا في أمر تلك المراقبة، فالمشرع الأجنبي قام بتخصيص وقت قليل، حيث خصصها بثلاثين يومًا مسموح تجديدها لفترات أخرى مطابقة بموجب التحديد المذكور في نص

[١٥٦] المادة رقم (٢٢) من المرسوم بقانون الاتحادي رقم (١٢) لسنة ٢٠١٦م بتعديل المرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات .

[١٥٧] المادة رقم (٣٧٨) من قانون العقوبات الإماراتي.

المادتين (٩٥ و٢٠٦) إجراءات مصري، والبعض يطيل زمن الفترة لأربعة أشهر مسموح تجديدها، وذلك عند التشريعين الفرنسي (المادة ١٠٠-٢)[١٥٨] إجراءات فرنسي.

وبناءً عليه نتجت المراقبة الصحيحة التي تمت خلال تقدير جميع الضوابط المنصوص عليها في القانون أثر يرتبط احتمالية الاعتداد بالأدلة الإلكترونية الناتجة عنها في تأكيد الجريمة الإلكترونية وإثباتها على المتهم، ولكن المراقبة الباطلة فتُنتج أثرًا عكسيًا يتشكل في تجنب الأدلة الناتجة عنها وعدم السماح بالموافقة عليها في تأكيد إدانة المتهم، بدلًا من تلبية المسؤولية الجنائية عن جريمة الاعتراض غير المشروع (المادة ٣٠٩ مكرر عقوبات مصري) إذا أُتيحت الشروط التي يحتاجها القانون لتنفيذ تلك الجريمة[١٥٩].

الخلاصة:

تناولت الباحثة في هذا الفصل ماهية الدليل الإلكتروني، حيث اتضح من خلال الفصل أن أكبر المشاكل المتعلقة بالجرائم الإلكترونية وفقًا للتعاون الدولي هي عدم وجود مفهوم موحد عام بين تلك الدول يمكن من خلاله التوصل للنشاط الذي يتبلور منه هذا النوع من الجرائم، فضلًا عن عدم توافر الخبرة الكافية لدى جهات القضاء والادعاء وأجهزة الشرطة والتي تمكنهم من جمع الأدلة وفحصها مما يشكل عائقًا أمام المجهودات المبذولة للتصدي للجرائم الإلكترونية، وقد تبين أيضًا من خلال استعراض أثر الطبيعة الخاصة بالجريمة الإلكترونية على الإثبات الجنائي أن الجرائم الإلكترونية تتمتع بطبيعة خاصة جعلتها تعتبر أحد أقوى المشكلات التي تواجه الدول للقضاء على هذه الجرائم، حيث إنها تخرج من دائرة القضايا الجنائية التقليدية، فضلًا عن عدم توافر الخبرات الفنية والتقنية اللازمة لدى سلطات الاستدلال والتحقيق والقضاء.

[158] Article 100-2 de CPP francais dispose que : " Cette décision est prise pour une durée maximum de quatre mois . Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée . "

[١٥٩] عبيد، رؤوف . ٢٠٠٦ . *مبادئ الإجراءات في القانون المصري* . القاهرة: دار الفكر العربي . ص . ٤٤٦.

وتتمثل خصائص الدليل الإلكتروني في كونه دليلًا علميًا، وتقنيًا، ويصعب التخلص منه، كما إنه دليل قابل للنسخ، بالإضافة إلى ذلك، فإنه يمتاز بتوافر السعة التخزينية العالية، وقد تناولت الباحثة أيضًا في هذا الفصل تقسيمات الدليل الإلكتروني، حيث حاول الفقهاء تقسيم الدليل الإلكتروني، وهو ما نتج عنه ظهور أربعة أقسام للدليل الإلكتروني وهى: الأدلة الرقمية المتعلقة بأجهزة الحاسوب وشبكاها، والأدلة الرقمية الخاصة بالإنترنت، والأدلة الرقمية الخاصة ببرتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات، والأدلة الرقمية الخاصة بالشبكة العالمية للمعلومات، كما تمت الإشارة أيضًا إلى إجراءات جمع الدليل الإلكتروني، والتي ظهر منها عدد من الإجراءات التقليدية لجمع الدليل الإلكتروني، ومن أهمها المعاينة، بالإضافة إلى ذلك هناك إجراءات حديثة لجمع الدليل الإلكتروني، وتتمثل تلك الإجراءات في الإجراءات المتعلقة بالبيانات الساكنة كالتحفظ المعجل على البيانات المخزنة، والأمر بتقديم بيانات معلوماتية متعلقة بالمشترك، فضلاً عن الإجراءات المتعلقة بالبيانات المتحركة (اعتراض الاتصالات الإلكترونية) المتمثلة في حرمة الاتصالات الإلكترونية الخاصة، والاعتراض المشروع للاتصالات الإلكترونية الخاصة.