الجامعة العربية الأمريكية

كلية الدراسات العليا

إجراءات التحقيق الابتدائي في الجريمة الإلكترونية

(دراسة مقارنة)

إعداد الطالب:

محمد جواد محمد غنام

إشراف:

د. حكمت عمارنة

تم تقديم هذه الرسالة استكمالاً لمتطلبات درجة الماجستير

في تخصص

العلوم الجنائية

2023

إجازة الرسالة

إجراءات التحقيق الابتدائي في الجريمة الإلكترونية
(دراسة مقارنة)

إعداد

محمد جواد محمد غنام

نوقشت هذه الرسالة بتاريخ: ٢٠٢٣/٠٩/٢٠ وأجيزت.

أعضاء لجنة المناقشة:

		التوقيع
١. الدكتور حكمت عمارنة	مشرفاً ورئيساً	.....
٢. الدكتور غسان عليان	ممتحناً داخلياً	.....
٣. الدكتور عصام الأطرش	ممتحناً خارجياً	.....

الإقرار

انا الموقع أدناه مقدم الرسالة التي تحمل عنوان:

إجراءات التحقيق الابتدائي في الجريمة الإلكترونية

(دراسة مقارنة)

أُقر بأن ما اشتملت عليه هذه الأطروحة إنما هي نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه حيثما ورد وأن هذه الرسالة ككل أو أي جزء منها، لم يقدم من قبل لنيل أية درجة علمية أو بحثية لدى أي مؤسسة تعليمية أو بحثية أخرى.

اسم الطالب: محمد جواد محمد غنام

التوقيع:

التاريخ: 2023/12/19

الرقم الجامعي: 202012030

الإهداء

أهدي هذا الإنجاز وهذا العمل

إلى ذلك الرجل الذي علمني العزة وكحل عيني بالكبرياء

إلى من بذل قصار جهده لأقف أمامكم اليوم

إليك أبي

إلى من كان دعاؤها سر توفيقي ونجاحي

واليد التي اندست في خصال شعري وصوتها الشجي الذي يروي لي

حكايا الجد والاجتهاد

إليك أمي

إلى من ساندوني ولم يتوقفوا عن دعمهم لي طيلة فترة دراستي

إليكم أخوتي

شكر وتقدير

نحمد الله عز وجل الذي منّ علينا بإتمام هذا البحث العلمي المتواضع،

فالحمد لله حمداً كثيراً طيباً مباركاً فيه

أتقدم بجزيل الشكر والعرفان من الدكتور المشرف "حكمت عمارنة" على كل ما قدمه لنا من توجيهات وإرشادات علمية قيمة ساهمت في إخراج هذا العمل المتواضع للوجود في جوانبه المختلفة، كما وأتقدم بجزيل الشكر إلى أعضاء لجنة المناقشة الموقرة.

كما وأتقدم بالشكر لكل من ساهم في إنجاز هذا البحث العلمي من قريب أو بعيد

الملخص

يعتبر التقدم العلمي والتطور على مستوى التكنولوجيا الحديثة، من أهم الظواهر ذات الأهمية الخاصة على مستوى الحياة اليومية للأفراد داخل أي مجتمع من المجتمعات، والمجتمع الفلسطيني مثله مثل أي مجتمع آخر؛ ليس بمنأى عن هذا التطور والتقدم العلمي، حيث اتسعت لديه كغيره من المجتمعات دائرة الاستخدام اليومي لشبكة الانترنت باعتبارها وسيلة اتصال وتواصل في مجالات الحياة كافة.

وبالرغم من الفوائد المتعددة "لتكنولوجيا المعلومات والعالم الافتراضي" للأشخاص في أي مجتمع، فإنها تشكل العديد من المخاطر وتخلق نوعا جديدا من الجرائم التي أصبحت تعرف باسم الجريمة الإلكترونية، والتي تنوعت أشكالها وصورها.

والتحقيق بهذه التجاوزات لجرائم الحاسوب والانترنت وطرق ضبط الأدلة التي تثبت ارتكاب فعل جرمي، يعتبر من الموضوعات الحديثة والمستجدة لدى أجهزة القضاء الفلسطيني، لاسيما إذا ما أخذنا بعين الاعتبار أن أول تنظيم قانوني خاص في مثل هذا النوع من الجرائم على مستوى فلسطين قد جاء من خلال قرار بقانون رقم (10) لسنة 2018 بِشأن الجرائم الإلكترونية، وَتعديلاته عام 2020.

إذ تتولى سلطة التحقيق في هذا النوع من القضايا وحدة خاصة تسمى "وحدة الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات"، وذلك حسب قواعد وإجراءات خاصة يتميز بها التحقيق الابتدائي في الجرائم الإلكترونية عن التحقيق في الجرائم التقليدية، وإن كانت الإجراءات المتبعة في تعقب هذا النوع من الجرائم ، إلاّ أنها تحظى بخصوصية تميزها عن الأخرى، نظراً لما تنطوي عليه هذه الجرائم من أساليب ووسائل حديثة تساعد على ارتكابها، الأمر الذي استدعى مواجهتها بإجراءات ووسائل إثبات خاصة، وتولي مهمة التحقيق فيها عبر أجهزة متخصصة.

وبناءً تعلى ذلك فقد ركزت هذه الدراسة في التعمق بتلك الإجراءات الخاصة بالتحقيق الأولي في الجرائم الإلكترونية في ظل التشريع الجزائي الفلسطيني، على مستوى قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 وكذلك القرار بقانون رقم (10) لسنة 2018، ومقارنتها مع نظيراتها من التشريعين المصري والأردني؛ ولذلك اختار الباحث لهذه الدراسة المنهج التحليلي المقارن.

وقد خرجت الدراسة بمجموعة من النتائج، كان من أهمها: أن التشريع الفلسطيني مازال بحاجة ماسة إلى التطوير في مجال مكافحة جرائم التقنية العالية بصفة عامة، مع الآخذ بعين الاعتبار

ضرورة مواكبة التطورات التكنولوجية الحديثة في هذا الجانب، بالإضافة إلى أن هناك نقص في الكادر العلمي المؤهل للتعامل مع هذا الأمر كخبراء التحقيق في الجرائم الإلكترونية.

وفي ختام هذه الدراسة أوصى الباحث بمجموعة من المقترحات للجهات المعنية كان من أهمها: العمل على تطوير المستوى العملي لخبراء التحقيق الجنائي في جرائم الحاسوب والانترنت، وذلك بعقد الدورات التكوينية المستمرة في مجال الجرائم الإلكترونية، وكذلك تعديل قوانين مكافحة الجرائم الإلكترونية بالشكل الذي يتماشى مع تطور سبل ووسائل ارتكاب هذه الجرائم من الناحية التقنية والتكنولوجية.

الكلمات المفتاحية: الجريمة الإلكترونية، التحقيق بالجريمة الإلكترونية، الدليل الرقمي.

فهرس المحتويات

المقدمة

تطورت وسائل التحقيق الجزائي بشكل كبير في عصر تكنولوجيا المعلومات والتي كانت تهدف إلى مواكبة تطور وسائل ارتكاب الجرائم والتنوع والتعدد في استحداث أساليب جديدة لها، ويرجع ذلك إلى حقيقة أن العالم يشهد اعتماداً شبه كامل على استخدام الوسائل الالكترونية في مختلف المجالات ومناحي الحياة.

إن أهم ما يميز العصر الحالي عن غيره من العصور، هو التطورات المثيرة التي نشهدها في مجال التكنولوجيا، والتي تنعكس بشكل مباشر على شتى أمور الحياة للأفراد، وهو ما يمكننا معه القول بأنه لم يعد هناك شأن يتصل بالحياة الإنسانية إلا ناله نصيب من هذا التطور التكنولوجي المثير الذي أحدث ثورة أدخلت البشرية في عصر جديد.

على الرغم من النقاط الإيجابية العديدة التي جلبتها تكنولوجيا الإنترنت في تسهيل نقل وتبادل المعلومات هناك خوف متزايد من زيادة الانتهاكات والسلبيات التي تؤثر بشكل أساسي على حقوق الإنسان وتؤثر بشكل مباشر على حرياته الأساسية.

ومع انتشار أجهزة الكمبيوتر والإنترنت، ومع صعود المستوى العام للأفراد الذين يستخدمون هذه التقنيات الحديثة لتحقيق أهدافهم، أدى استخدام التكنولوجيا في جميع مناحي الحياة إلى تحويل الكوكب إلى قرية صغيرة، تتدفق بسهولة ويسر بين أجزائه، ومن هنا بدأوا في الحصول على أكبر قدر ممكن من المعلومات السرية، والتي كانت تسمى "ثورة المعلومات".[1]

وفي ضوء ذلك، فإن إساءة استخدام هذه الوسائل الالكترونية بطريقة غير قانونية أو استخدامها لتحقيق أهداف غير قانونية أدى إلى ظهور نوع جديد من الإجرام، حيث أصبحت التقنيات الحديثة وسيلة لارتكاب مختلف الجرائم التقليدية في أسرع وقت دون أن تترك أي أثر يدل على المجرم، يمكّن الجهات المختصة من تتبعه وملاحقته بناءً عليه.

نظراً لوجود العديد من الرواد في البيئة الالكترونية أو الافتراضية، فإنه يعتبر مجالاً خصباً لارتكاب أشكالاً متعددة من الجرائم الالكترونية من خلال الوسائل والتقنيات الحديثة، ومن أهمها في الوقت الحاضر نجد: شبكة الانترنت والبريد الالكتروني ومختلف وسائل التواصل الاجتماعي الحديثة.

---

[1] العجمي، عبد الله، المشكلات العلمية والقانونية للجرائم الإلكترونية دراسة مقارنة، رسالة ماجستير–جامعة الشرق الأوسط، الأردن، 2014، ص 6.

ومما لا شك فيه أن الجريمة السيبرانية الحديثة لا وجود لها إلا إذ كان ذلك بسبب إساءة استخدام الوسائل الالكترونية والتقنيات الحديثة، كما أن أشكال ظاهرة الجريمة السيبرانية متنوعة ومتعددة. بعضها يتعلق بالاحتيال الإلكتروني والتزوير الإلكتروني والاعتداء على حقوق الخصوصية الشخصية والاعتداء على المعلومات بما في ذلك تلك المتعلقة بأشكال وأنواع أخرى كثيرة من هذه الجرائم[2].

وبناءً على ما سبق فإن التقدم التقني والتكنولوجي ورغم فوائده العديدة والإيجابيات الكثيرة التي نجمت عنه، إلاّ أنه قد صاحبه العديد من السلبيات التي نتجت عن سوء استغلال واستخدام شبكة الانترنت لغايات ارتكاب أفعال تندرج تحت طائلة التجريم، بموجب القوانين الجزائية الجاري بها العمل في مختلف الدول.

بالإضافة إلى ما سبق، فإن انتشار الجرائم الالكترونية وما تتمتع به من مميزات وخصائص تدفع الكثير من رواد شبكة الانترنت إلى ارتكابها، وقد تكون هذه الدوافع ذات طبيعة ربحية؛ بحيث يسعى الجاني من ورائها إلى الحصول على الأموال وقد يكون الهدف هو الرغبة في إثبات نفسه وتحقيق انتصار على تكنولوجيا نظم المعلومات، وقد يكون الدافع هو تعرض الشخص للتهديد والضغط، كما وقد يكون ذا طبيعة سياسية وغيرها[3].

وفي ضوء تلك المؤشرات، يمكن القول إن الجريمة الالكترونية ظاهرة عالمية ونوع مختلف ومغاير تماماً لما يشهده أي مجتمع من أشكال الجريمة المتعارف عليها في كافة المجتمعات، والإجرام الالكتروني يهدد المجتمع الفلسطيني كغيره من المجتمعات في مختلف دول وبلدان العالم، وقد دفع ذلك بالمشرع الفلسطيني إلى تخصيص بعض التشريعات الجزائية الخاصة للتصدي لهذه الجريمة، يأتي في مقدمتها القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية، وتعديلاته بموجب القرار بقانون رقم (28) لسنة 2020.

وذلك بالإضافة إلى تطبيق التشريعات الجزائية العامة، متمثلة بقانون العقوبات رقم (16) لسنة 1960، وقانون الإجراءات الجزائية رقم (3) لسنة 2001.

---

[2] بن سليمان، عبد السلام. الإجرام المعلوماتي في التشريع المغربي: دراسة نقدية مقارنة في ضوء أداء الفقه وأحكام القضاء، ط1. دار الأمان. الرباط. المغرب، 2017، ص12.

[3] - مركز هردو لدعم التعبير الرقمي، التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات، القاهرة، مصر، 2018، ص 5.

إشكالية الدراسة

لا يخفى على المتتبع للمجال التشريعي والقانوني لمواجهة الجرائم التي تهدد أمن المجتمعات ونظامها العام، من كون أن التقدم العلمي والتقني والتكنولوجي الذي شهده العالم المعاصر قد أفرز صنفاً أو نوعاً جديداً من الجرائم التي تختلف في سبل ارتكابها وآثارها عن الجرائم التقليدية.

وقد ترتب عن مثل هذه الجرائم تحديات كثيرة للقوانين التي وضعت لغايات مكافحتها، وذلك نظراً لاختلاف سبل ارتكاب هذا النوع من الجرائم والآثار المادية والمعنوية التي تنجم عنها، ناهيك عن أنّ التشريعات والقوانين التي وضعت خصيصاً لمواجهة هذا النوع من الجرائم لا تكون تتماشى في الغالب مع تطور الجريمة الإلكترونية، وبالتالي قصور هذه التشريعات عن ضبط مرتكبي هذه الجرائم وإحالتهم للعدالة كما هو الحال في الجرائم التقليدية.

وعلى الجانب الإجرائي -تماشياً مع موضوع الدراسة- ونظراً لاختلاف أساليب ارتكاب الجرائم الالكترونية، فقد استلزم ذلك استحداث قواعد جديدة تتلاءم والطبيعة القانونية لمثل هذا النوع من الجرائم، خلال كافة إجراءات الملاحقة الجزائية، والتي من ضمنها: مرحلة التحقيق الابتدائي.

فالتحقيق في الجرائم الإلكترونية وكيفية ضبط الأدلة وجمعها، يعتبر من الموضوعات القانونية التي تحتاج إلى بحث علمي وأكاديمي يبين ماهية وخصوصية هذا الإجراء في الحالات التي ترتكب فيها الجريمة الإلكترونية.

وفي ضوء ما تقدم ذكره، تتمثل الإشكالية الرئيسية لهذه الدراسة بما يلي:

ما التنظيم القانوني لإجراء التحقيق الابتدائي في الجرائم الالكترونية؟

ويتفرع عن هذه الإشكالية، العديد من التساؤلات الفرعية التي يمكن ذكر بعضها على النحو الآتي بيانه:

1. ماهية التحقيق الابتدائي كإجراء من إجراءات الدعوى الجزائية المتعلقة بجريمة إلكترونية؟
2. أين تكمن خصوصية التحقيق الابتدائي في الجرائم الالكترونية في التشريع الفلسطيني ونظيره في كل من مصر والأردن؟

3. من هي جهة الاختصاص الأصيل في التحقيق الابتدائي في الجرائم الالكترونية، وما هي الصلاحيات الممنوحة لها في ظل التشريع الفلسطيني ونظيره في كل من مصر والأردن؟

أهمية الدراسة

تتجلى أهمية الدراسة على المستويين النظري (العلمي) والتطبيقي (العملي)، نوضح ذلك كما يلي:

على المستوى النظري (العلمي) تتناول الدراسة أحد مراحل الدعوى الجزائية، والتي تتمثل بالتحقيق الابتدائي باعتباره أولى المراحل التي يتم فيها مواجهة المتهم بما نُسب إليه من أفعال غير قانونية، تمثل جريمة يتم المحاسبة والمساءلة عنها أمام القضاء المختص، ناهيك عن الخصوصية التي تتمتع بها الجرائم الالكترونية باعتبارها واحدة من الجرائم الحديثة إلى حد ما، والتي تشهد مستجدات على مستوى الأفعال المرتكبة والتي تمثل تعديات ومخالفة للقوانين الجزائية الجاري بها العمل، ناهيك عن متطلبات الوقاية من الجرائم الالكترونية من ناحية التحديث المستمر لمنظومة التشريعات ذات العلاقة، وبالتالي تتطلب متابعة علمية حثيثة ومستمرة من طرف الباحثين في مجال التشريعات الجزائية الناظمة لمثل هذا النوع من الإجرام.

أما من الناحية العملية، واستناداً إلى ما سلف ذكره من تسارع التطور التكنولوجي، وما ينتج عنه من تنوع وتجدد للأفعال الجرمية المتعددة استناداً لتلك الوسائل الإلكترونية الحديثة، فيمثل البحث في هذه الجرائم وسبل مواجهتها ومحاسبة ومساءلة مرتكبيها ضرورة قصوى لبيان نقاط القوة ونقاط الضعف لمنظومة التشريعات المقررة للوقاية والحماية من هذه الأفعال، وبناءً على ذلك: يمكن القول باعتبار هذا النوع من الأبحاث يمثل بوصلة تساعد على توجيه المشرع في أي بلد إلى تدارك أوجه التقصير في التشريعات من جهة، ومساعدة الجهات المسؤولة عن تطبيق وتنفيذ القوانين في تراكم معارفها وخبراتها لحل النزاعات التي تظهر نتيجة لارتكاب هذه الجرائم، من جهة أخرى.

عـلاوة علـى ذلـك فـي الأهميـة العمليـة لهـذه الدراسـة، مـا يمكننـا اسـتنتاجه مـن أهميـة الحقـوق التـي يشـكل ارتكـاب مثـل هـذا النـوع مـن الجـرائم انتهاكـاً لهـا، يـأتي علـى رأسـها الحق في الخصوصية.

أهداف الدراسة:

نتـوخى عنـد الانتهـاء مـن هـذه الدراسـة تحقيـق مجموعـة مـن الأهـداف، نـذكر بعضـاً منهـا على النحو الآتي بيانه:

1. بيان الطبيعة القانونية للتحقيق الابتدائي كإجراء من إجراءات الدعوى الجزائية ذات العلاقة بالجرائم الالكترونية.
2. توضيح الخصوصية التي تميز التحقيق الابتدائي في الجرائم الالكترونية عن التحقيق في الجرائم العادية.
3. تحديد جهة الاختصاص في التحقيق الابتدائي في الجرائم الالكترونية، والصلاحيات المخولة لتلك الجهة.
4. تبيان جوانب القصور في النصوص التشريعية التي نظمت عملية التحقيق في الجرائم الإلكترونية.

منهج الدراسة:

تماشياً مع طبيعة الموضوع المطروح والحديث نوعاً ما في الواقع الفلسطيني، والذي يتناول مجموعة من المجالات ذات العلاقة بمحلّ الدراسة، سوف يعتمد الباحث المنهج التحليلي المقارن، والذي من خلاله سيقوم بتحليل نصوص القوانين والتشريعات الفلسطينية ومثيلتها الأردنية والمصرية ذات العلاقة بموضوع الدراسة، ولتحقيق أكبر قدر من الفائدة وحتى نصل الى نتائج البحث المرجوة، كما سيستعين الباحث بالمنهج الوصفي لبيان طبيعة الجرائم الإلكترونية.

حيث سنقوم بمراجعة النصوص القانونية الناظمة لعنوان بحثنا وهو إجراءات التحقيق في الجريمة الالكترونية وفقا للقانون الفلسطيني، من خلال آراء الفقهاء والباحثين القانونيين عبر كتبهم وأبحاثهم ودراساتهم القانونية، وتحليل هذه النصوص والآراء الفقهية ودراستها دراسة محكمة، ومقارنتها ببعض التشريعات الأخرى ذات العلاقة، في كل من الأردن ومصر.

مصطلحات الدراسة:

- **الجرائم الالكترونية**: هي فعل يتسبب بضرر جسيم للأفراد أو الجماعات والمؤسسات، بهدف ابتزاز الضحية وتشويه سمعتها من أجل تحقيق مكاسب مادية أو خدمة أهداف سياسية باستخدام الحاسوب ووسائل الاتصال الحديثة مثل الإنترنت.[4]
- **التحقيق الابتدائي**: مجموعة إجراءات تقوم بها هيئة التحقيق، ويمثل حلقة الوصل بين مرحلتي جمع الاستدلالات والمحاكمة، حيث يقوم المحقق في هذه المرحلة بجمع الأدلة التي تسند التهمة إلى المتهم وتلك التي تنفي التهمة عنه. أو هو قيام الدولة عند وقوع الجريمة ومن خلال أجهزتها المختصة، باتخاذ الإجراءات الكفيلة للوصول إلى اقتضاء حقها بمعاقبة من أخل بالنظام الاجتماعي، وهو مرتكب الجريمة.[5]

الدراسات السابقة:

وحيث أن الدراسة تهدف إلى التوصل لحل الإشكاليات المتعلقة بعنوان البحث، فإن الباحث سيعرض بعضاً من الدراسات السابقة التي من الممكن أن نؤيد بعضها وننقد بعضها الآخر، والبناء عليه حتى يتسنى لنا معالجة الإشكالية المطروحة لهذه الدراسة. ومن تلك الدراسات ما يلي:

- **الخوالدة سليمان، دراسة بعنوان "جريمة الدخول غير المشروع إلى موقع إلكتروني أو نظم معلومات وفق التشريع الأردني – دراسة مقارنة"، دار الثقافة، 2012.**

عرض الباحث في هذه الدراسة الطبيعة القانونية لجريمة الدخول غير المشروع لموقع إلكتروني أو نظام معلومات وذلك بتطبيقها على واقع النص القانوني من خلال وصف أركان هذه الجريمة وصور النشاط الجرمي المكون لها، ومسؤولية مرتكب هذا النوع من الجرائم المستحدثة، والجزاء المقرر لها وفق نصوص قانون الجرائم الالكترونية الأردني رقم 17 لسنة 2023، مقارنة مع بعض التشريعات الجنائية الأخرى. وخلصت الدراسة إلى عدد من النتائج والتوصيات كان أهمها: أنه من الضروري إدخال نصوص قانونية تعاقب على جريمة إتلاف المعلومات والبيانات بحد ذاتها وتقرر مسؤولية الشخص المعنوي في حال ارتكاب الجرائم المعلوماتية، والمعاقبة على الشروع في مثل

---

[4] – المومني عبد القادر، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع – عمان – الأردن، الطبعة الأولى، السنة 2012، ص 50.

[5] – عبد الباقي مصطفى، شرح قانون الإجراءات الجزائية الفلسطيني (دراسة مقارنة)، وحدة البحث العلمي والنشر – جامعة بيرزيت، السنة 2015، ص 180.

هذه الجرائم، وهذه الدراسة تتشابه في بعض مفرداتها مع دراستي الحالية، إلا أنها تختلف عنها كون أن دراستي تبحث حصراً في الأحكام الإجرائية الخاصة بالتحقيق الابتدائي في الجرائم الالكترونية في ضوء التشريع الفلسطيني، ومقارنتها مع الإجراءات المتبعة في التشريعين الأردني والمصري.

- **إبراهيم رأفت، دراسة بعنوان "الحماية القانونية لخصوصية مراسلات البريد الإلكتروني" جامعة المنصورة، مصر، 2013.**

بينت هذه الدراسة أن مراسلات البريد الإلكتروني تتعرض للعديد من المخاطر التي تهدد بالاعتداء عليها سواء من قبل الأفراد أو الحكومات. وتعد مراقبة ومعرفة مكان تواجد الشخص وانتماءاته وميوله السياسية وغيرها من الأمور التي تمكن من تكوين صورة كاملة عن صاحب تلك المراسلات . وتتميز الدراسة عن موضوع دراستنا في أن الاخيرة تناولت الحماية القانونية لخصوصية مراسلات البريد الإلكتروني بينما تركز الدراسة الحالية على مرحلة التحقيق الابتدائي في الجرائم الالكترونية، وقد استفاد الباحث من هذه الدراسة في موضوع انتهاك الخصوصية في الجرائم المعلوماتية.

- **عبد الله دغش (2014) دراسة بعنوان" المشكلات العملية والقانونية للجرائم الالكترونية "دراسة مقارنة".**

إن انتشار وتوسع إطار الجرائم الالكترونية أصبح أمراً واقعاً في ظل الثورة المعلوماتية والتطور الهائل في وسائل الاتصال الحديثة، إلا أن هناك مشكلات موضوعية وإجرائية تثيرها الجرائم الالكترونية على الصعيدين التشريعي والعملي. وقد تصدى المشرع الأردني لتجريم وعقاب الصور التي ترتكب بها الجرائم الالكترونية وذلك بموجب القانون الأردني المتعلق بجرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010م، بخلاف المشرع الكويتي الذي لم يتدخل حتى هذه اللحظة لا بسن قانون خاص بالجرائم الالكترونية ولا بإجراء تعديل تشريعي على قانون الجزاء بإضافة نصوص تعالج هذا النوع من الجرائم، ونظراً للمشكلات التي تثيرها الجرائم الالكترونية فقد جاءت هذه الدراسة لبيان طبيعة هذه المشكلات والحلول التشريعية والعملية لمواجهتها. وقد خرج الباحث بعدد من النتائج، ومن أهمها أن القواعد التقليدية في التشريع الجزائي الكويتي غير كافية لمواجهة الجرائم الالكترونية وما تثيره من مشكلات، وأما أهم توصيات هذه الدراسة فهي: دعوة المشرع الكويتي للإسراع بسن قانون خاص بالجرائم الالكترونية، أو استحداث فصل خاص بها في قانون الجزاء، وكذلك دعوة المشرعان الكويتي والأردني لمواجهة تحديات ومشكلات الجريمة الالكترونية، سواء أكانت الموضوعية منها أم الإجرائية.

تقسيم الدراسة:

لمعالجة الإشكالية الرئيسية والإجابة على مجموعة التساؤلات الفرعية في ضوء المنهج المعتمد لهذه الدراسة، ارتأى الباحث تقسيم دراسته إلى فصلين أساسيين على النحو التالي:

الفصل الأول: ماهية الجريمة الإلكترونية

الفصل الثاني: القواعد الإجرائية الناظمة للتحقيق الابتدائي في الجريمة الإلكترونية

الفصل الأول: الطبيعة القانونية للجريمة الإلكترونية

شهدت الحياة اليومية تطورات ملحوظة في مجال تقنية المعلومات، وشهدت البيئة الالكترونية عدداً كبيراً من رواد وزوار المواقع الالكترونية بشكل يومي ، مما فتح مجالاً واسعاً لمجرمي التكنولوجيا الذين وجدوا في هذه البيئة مجالاً خصباً لارتكاب أنواعاً كثيرة من الجرائم الالكترونية عبر وسائل الاتصال الحديثة.

تعتبر الجريمة الالكترونية صنفاً مستحدثاً من الجرائم، حيث يستند مرتكبوها بشكل أساسي إلى الأنظمة المعلوماتية وشبكات الاتصالات، أي انتقال الجريمة من صورتها التقليدية إلى صورتها حديثة، الأمر الذي جعل من التحكم بها والتعامل معها يتسم بالصعوبة.

الجريمة السيبرانية ظاهرة عالمية، ونوع جديد، يختلف تماماً عن الأنواع والوسائل التقليدية للجريمة، وهي ظاهرة تهدد أمن واستقرار جميع المجتمعات، وتتطلب وجود وسن قوانين خاصة أكثر ردعاً من القوانين القائمة للتخفيف من المشاكل القانونية والعملية التي يطرحها هذا النوع من الجرائم.

وإن بيان الإشكال القانوني والعملي التي تثيرها ظاهرة الجرائم الالكترونية عموماً، يتطلب بالضرورة من الباحث أن يقوم أولاً وقبل كل شيء ببحث ماهية هذه الجرائم، وذلك من خلال التطرق إلى مفهومها والأركان التي تتشكل منها هذه الجرائم، وأمثلة على بعض أنواع الجرائم الالكترونية.

لذا سنتناول في هذا الفصل مفهوم الجريمة الالكترونية وخصائصها في (المبحث الأول)، ونتناول أركان وبعض أنواع الجرائم الالكترونية في (المبحث الثاني).

المبحث الأول: مفهوم الجريمة الالكترونية وخصائصها

تعد الاتصالات المفصل الأساسي للكثير من المجالات الحيوية في مسار حياة المجتمعات كونها تعمل كشبكة مترابطة ببعضها، الأمر الذي يعرضها لخطر الاختراق، وفي ظل الانفتاح الواسع والمتسارع وإتاحة المعلومات غير المشروط، الأمر الذي جعل منها مجالاً مفتوحاً تحيق به أخطار الجرائم المرتكبة عبر الوسائط الالكترونية، المقصودة منها والتي ترتكب بطريق الخطأ.

وعليه سيتم في هذا المبحث الحديث عن مفهوم الجريمة الالكترونية (المطلب الأول)، ثم الحديث عن خصائصها (المطلب الثاني).

المطلب الأول: مفهوم الجريمة الالكترونية

تناولت العديد من الدراسات والأبحاث الجرائم الالكترونية ولم تتفق على مصطلح محدد أو تعريف معين لهذه الجريمة حديثة الطهور، الأمر الذي أدى لصعوبة حصرها داخل نطاق تجريمي محدد يمكن أن يحيط بها، وعليه تتسم التعاريف الفقهية التي أعطيت لهذا النمط من الجرائم بالمرونة والمواكبة للتطورات المستمرة والمستقبلية.

المؤتمر العاشر للأمم المتحدة لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا من 10 – 17 نيسان/أبريل عام 2000 يعرفها على أنها: أي جريمة يتم ارتكابها عبر شبكة حاسوبية أو نظام حاسوبي، وتشمل تلك الجريمة مبدئياً جميع الجرائم التي يتم ارتكابها في بيئة إلكترونية. [6]

تتميز هذه الجرائم بحداثة الجريمة السيبرانية، ومن المثير للإعجاب ملاحظة أن نوع النظم القانونية والثقافية بين مختلف البلدان أدى إلى اختلافات في مفهوم الجريمة السيبرانية. وبحسب المفوضية الأوروبية، فإن مصطلح الجريمة الإلكترونية "يشمل جميع العلامات التقليدية للجريمة، مثل الاحتيال والعبث بالمعلومات ،ونشر المواد الالكترونية،بما في ذلك مزاعم المحتوى غير الأخلاقي والتحريض

[6] إعلان فيينا بشأن الجريمة والعدالة، مواجهة تحديات القرن الحادي والعشرين، مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين، المنعقد في فينا من 10 إلى 17 نيسان/أبريل 2000.

الطائفي. ووفقاً لوزارة العدل الأمريكية، يتم تعريفها على أنها: "يجب أن يكون لدى مرتكبها معرفة تقنية بتكنولوجيا الكمبيوتر تسمح له بالقيام بذلك". [7]

اما بالنسبة لمنظمة التعاون الاقتصادي، فقد حددت الجرائم المرتكبة عبر الإنترنت: "إنها جميعا أنشطة غير قانونية أو غير أخلاقية تتعلق بالمعالجة التلقائية للبيانات ونقلها ". [8]

كما عرفها الفقه المغربي بأنها "كل اعتداء يمس البيانات والمعطيات المعالجة آلياً والمحمية جنائياً بغية الإضرار بصاحبها أو بالغير مادياً أو معنوياً"[9].

وبالنسبة للفقه الأردني، فقد عرفها بأنها " جريمة تلعب فيها برامج البيانات والمعلومات الحاسوبية دوراً رئيسيا"، وعرفها جانب آخر بأنها "كل استخدام في صورة فعل أو امتناع غير مشروع لتقنية المعلومات، بهدف الاعتداء على أية مصلحة مشروعة، سواء أكانت مادية أو معنوية"[10].

بينما تُعرّف الجريمة السيبرانية بأنها: هي التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة على كمبيوتر آخر أو أحد وسائل أو أحد الوسائل التقنية الحديثة، مع ضرورة توفر شبكة اتصال فيما بينهما[11]، والبعض الأخر عرفها بأنها نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود[12].

ومما يجدر التنويه إليه، أنه عادة ما يقع الخلط بين مفهوم الجريمة المعلوماتية "السيبرانية" والجريمة الالكترونية، ولكن الواقع أنّ هناك اختلاف بين مفهوم كل من هاتين الجريمتين:

فالجرائم المعلوماتية: هو سلوك غير قانوني يحدث عند انتهاك الأجهزة الإلكترونية والذكية والحواسيب، التي تعتمد على الإنترنت في عملها، فيستغل المجرم شبكة الإنترنت للوصول إلى

---

[7] طيب، ميرفت محمود. "الجريمة الإلكترونية وأنواعها وأشكالها وأدواتها ودوافعها وطرق مكافحتها والعقوبات القانونية لها"، 2017، المصدر: جريدة وموقع غرب garbnews.net تاريخ نشرها، 2017/11/12، 8:56.

[8] مركز هردو لدعم التعبير الرقمي، مرجع سابق، ص8.

[9] بن سليمان، عبد السلام. مرجع سابق، ص66.

[10] العجمي عبد الله، مرجع سابق، ص 22.

[11] أسامة مهمل، الإجرام السيبراني، رسالة ماجستير، كلية الحقوق والعلوم السياسية – جامعة بوضياف/الجزائر، 2017-2018، ص 9.

[12] محمود القرعان، الجرائم الالكترونية، دار وائل للنشر والتوزيع، الطبعة الأولى، الأردن، 2017، ص 19.

المعلومات الشخصية للأفراد، حيث أنّ هذه الوسائل تعتبر من أضخم بنوك المعلومات لدى جميع الناس في هذا الزمن، كما أنّ العديد من الأعمال والصفقات التجارية، أصبحت تنفذ عن طريق الشبكة العنكبوتية وعن بُعد؛ لذلك يجب زيادة الوعي في كل ما يخص البيانات والمعلومات المرفقة على المواقع الإلكترونية[13].

أما الجرائم الالكترونية وكما سبقت الإشارة إليها، هي جرائم جرائم ترتكب ضد أفراد أو جماعات أو مؤسسات كاملة؛ باستخدام وسائل الاتصال الحديثة واستخدام الحاسوب، والهدف الأساسي منها يكون ابتزاز الشخص أو تشويه سمعته، وإلحاق الضرر به؛ للحصول على مقابل مادي مثل النقود أو لتحقيق أهداف سياسية، أو إفشاء أسرار أمنية تكون خاصة بالمؤسسة[14].

وبناءً عليه، يمكن استنتاج بأنه: "لا يوجد إجماع في تعريف الجريمة الالكترونية من حيث كيفية ارتكابها و ما هي الجرائم التي تتضمنها"، **وكما يقول فان دير هلست وونيف** "لا يوجد تعريف عام وإطار نظري ثابت في هذا الحقل من الجريمة، وغالباً ما يتم استخدام المصطلحات الافتراضية والكمبيوتر والالكترونية والرقمية". ويتراوح تعريف الجريمة السيبرانية بين الجرائم التي ترتكب بواسطة الكمبيوتر إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية، وتعريف الجرائم الالكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الهاتف[15].

ومن هذا المنطلق، سيتم تناول تعرف الجريمة الالكترونية: اصطلاحا (أولاً) وقانونا (ثانياً).

ثانيا: الجريمة الالكترونية اصطلاحا

لم يُجمع الفقه الجنائي على تعريف وتسمية موحّدَيْن للجرائم الالكترونية، فهناك من يطلق عليها تسمية الجرائم الالكترونية والبعض يطلق عليها جرائم المعلوماتية، في حين يذهب آخرون

---

[13] لمزيد من التفصيل أنظر الرابط التالي: https://cyberone.co/ ، تاريخ الزيارة: 2023/10/10.

[14] لمزيد من التفصيل أنظر الرابط التالي: https://www.it-pillars.com/ar/blog/ ، تاريخ الزيارة: 2023/10/10.

[15] مركز هردو لدعم التعبير الرقمي، مرجع سابق، ص7.

لتسميتها بجرائم إساءة استخدام تكنولوجيا المعلومات والبعض يطلق عليها جرائم الكمبيوتر والانترنت.

وقد عرّف البعض الجريمة الالكترونية أنها: عمل غير قانوني يتم فيه استخدام تكنولوجيا الكمبيوتر بشكل مباشر أو غير مباشر كأحد الوسائل لتنفيذ الفعل الإجرامي، كما جاء تعريف الجريمة الالكترونية بأنها جرائم الحاسب الآلي [16].

والحاسب الآلي: هو جهاز لمعالجة البيانات والمعلومات المتعلقة بعمليات الرياضية ومنطقية تلقائياً دون تدخل بشري أثناء التشغيل وعادة ما يعمل بالترقيم الثنائي، وهو جهاز متعدد الأعراف يمكن استغلاله لتنفيذ عمل معين من خلال برنامج يقوم بتنفيذ هذا العمل [17].

وعليه يمكن أن نعرف الجريمة الالكترونية، بأنها: "أي نشاط إجرامي يكون للإنترنت دور في تنفيذه، على أن يكون هذا الدور على قدر من الأهمية ولا يختلف الأمر سواء تم النشاط على الشبكة أم كانت الشبكة وسيلة لارتكابه، ففي كلتا الحالتين ينبغي أن يكون لشبكة الانترنت دوراً مؤثراً في إتمام النشاط الإجرامي".

فالجريمة الالكترونية: تعد جريمة معلوماتية، والجريمة المعلوماتية قد ترتكب في بعض الأحيان في إطار حاسب آلي واحد، ولذلك فما ينطبق على الجرائم المعلوماتية من خصائص وسمات ينطبق على جرائم الانترنت.

ثالثا: الجريمة الالكترونية قانوناً

لم يتطرق المشرع الفلسطيني إلى تعريف الجريمة الالكترونية بموجب أي تشريع من التشريعات المتعلقة بالجرائم الالكترونية، وبالنظر للتشريعات العربية نجد المشرع السعودي قد عرفها

---

[16] شاهين، حسن. الجرائم الإلكترونية في التشريع الفلسطيني، 2022 وكالة وطن للأنباء https://www.wattan.net/ar/news/370729.html

[17] ميرغني، فيروز . إجراءات التحري والضبط في الجريمة الإلكترونية، أطروحة دكتوراه–جامعة شندي، السودان، 2017، ص5.

"بأنها أي فعل يرتكب متضمنا استخدام الكمبيوتر أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام" [18].

وبالمثل، فإن المشرع الأردني لم يتطرق إلى تعريف الجريمة السيبرانية في قانون جرائم نظم المعلومات المؤقت رقم30 ل عام2010، والذي حلّ محله قانون الجرائم الالكترونية رقم 17 لسنة 2023 [19].

المطلب الثاني: خصائص الإجرام الإلكتروني

إن الجريمة الالكترونية تنفرد بمجموعة من الخصائص تميزها عن غيرها من الجرائم المتعارف عليها في طريقة ارتكابها وأسلوبها، وعند الحديث عن خصائصها غالباً ما يتبادر للذهن دور الجاني المهم والحيوي في معظم حالاتها وذلك لتعمده التدخل في نظام المعلومات لفضاء الجريمة التي يرتكبها ودوافعه، كما تنفرد بتحديات تختص بها دون غيرها.

وعليه سنتحدث (أولاً) عن مرتكبي الجريمة الالكترونية وخصائصهم، ثم خصائص الجريمة الالكترونية (ثانياً)، ثم دوافع ارتكاب الجريمة الالكترونية (ثالثاً)، ومظاهر تحديات الجريمة الالكترونية (رابعاً).

أولاً: مرتكبي الجريمة الالكترونية وخصائصهم

سنتناول في هذا الفرع من هم مرتكبي الجريمة الالكترونية ثم دراسة خصائصهم:

i. مرتكبي الجرائم الالكترونية

يختلف الشخص الذي يقوم بارتكاب جريمة الكترونية، وتختلف وتتعدد فئاتهم وأصنافهم، مثل:

---

[18] أنظر المادة (8/1) من نظام مكافحة الجرائم المعلوماتية السعودي الصادر بتاريخ 2007/03/26.

[19] قانون رقم (17) لسنة 2023، قانون الجرائم الالكترونية، منشور في الجريدة الرسمية رقم (5874)، ص 3579– 3598، منشور بتاريخ 2023/8/13.

ii. طائفة القراصنة، وهي بدورها تنقسم إلى[20]:

القراصنة الهواة (الهاكرز Hackers) وهم الشباب المفتونون بالمعلوماتية وأنظمة الحاسوب ويطلق على بعضهم صغار أو مهووسون بعلوم الكمبيوتر ومعظمهم من الطلبة، حيث تضم هذه الطائفة الأشخاص الذين يستهدفون أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها، وكسر الحواجز الأمنية الموضوعة لهذا الغرض؛ إما ان يكون بسبب فضولهم أو لاكتساب الخبرة.

القراصنة المحترفين (Crackers) في الغالب تتراوح أعمارهم ما بين 45-55 سنة ويكون لهم مكانة في المجتمع المحيط وهم ودائماً متخصصين في مجال التكنولوجيا الالكترونية، وهم الأكثر خطورة، وعادة ما يعودون لارتكاب الجريمة مرة أخرى.

1. طائفة الحاقدين:

ويعرفوا المنتقمين لأنها ترتكب ضد أصحاب المنشآت والمؤسسات التي كانوا يعملون بها، وانتقاما من رب العمل وهم أقل خطورة. يرى الباحثون أن أهداف وأغراض الجريمة غير متوفرة لدى هذه الطائفة، فهم لا يهدفون إلى إثبات قدراتهم التقنية ومهارتهم الفنية لتحقيق مكاسب مادية أو سياسية، بل يعمدون لإخفاء أفعالهم وتتم أغلب أنشطهم باستخدام تقنيات زراعة الفيروسات والبرامج الضارة لتعطيل وتشويش الأنظمة المعلوماتية[21].

2. طائفة المتطرفين الفكريين:

التطرف في هذا المجال يعني" الأنشطة التي تستخدم الإنترنت لنشر وبث واستقبال وإنشاء مواقع وخدمات تعزز نقل وترويج المواد الفكرية التي تشجع التطرف الفكري "، مما دفع بعض المتطرفين إلى اتخاذ طرق إجرامية. من هذا ظهر ما يعرف بمجرمي المعلومات المتطرفين بما في ذلك شبكات الإعلام الإخبارية التي تتبع أنشطة المجموعة التي ينتمون إليها وتدلي بتصريحات قادتها، وجميع

---

[20] عطايا، ابراهيم. الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية، العدد 30، الجزء الثاني، 2015، ص360 وما بعدها.

[21] سلام، كرم سلام. الجرائم الإلكترونية في الفقه الإسلامي والقانون الوضعي، المؤتمر الدولي العلمي الافتراضي، 2022، برلين، ص49.

المواقع التي عادة ما يتصلون بها من مقاهي ومكاتب الإنترنت ومحاولة تحقيق أغراض دعائية لصالحهم.[22]

3. طائفة المتجسسون:

حيث يقوم هؤلاء بالعبث أو الإتلاف لمحتويات الشبكة من جانب، ومن جانب آخر وهو الأهم والذي يشكل الخطر الحقيقي على تلك المواقع، قد يتم تنزيل الأسرار الصناعية من حاسوب في إحدى الشركات وإرسالها بالبريد الإلكتروني مباشرة إلى منافستها، ومن أهم أهدافهم باستخدام الأنظمة المعلوماتية هو الحصول على معلومات الأعداء والأصدقاء على حد سواء.[23]

4. طائفة مخترقي الأنظمة:

عند تبادل المعلومات بين الأعضاء لإبلاغ بعضهم البعض عن نقاط الضعف في أنظمة المعلومات تتم عملية تبادل المعلومات بينهم من خلال نشرات إعلامية إلكترونية مثل: يتم دعوة مجموعات الأخبار وحتى أعضاء هذا المجتمع لعقد اجتماعات لجميع قراصنة أنظمة المعلومات، حيث يتم دعوة الخبراء للتشاور فيما بينهم حول آليات التطفل وكيفية النجاح.

i. خصائص مرتكب الجريمة الالكترونية:

1. يتميز بالدهاء والذكاء وله مهارات تقنية عالية ومعرفة ممتازة بأنظمة الكمبيوتر وكيفية التلاعب بالمعلومات وتخزينها والوصول إليها.
2. الشخص المتناغم اجتماعياً قادراً ماليا ، لأنه غالبا ما تكون رغبته هي الرغبة في التغلب على النظام ثم كسب المال [24].
3. غير عنيف، وذلك لانتماء الجرائم الالكترونية إلى جرائم الحيلة[25].

---

[22] سلام كرم سلام، مرجع سابق، ص 50.

[23] سلام كرم سلام، مرجع سابق، ص 50-51.

[24] بومدين وبن مزيان، إيمان وحنان. الجريمة الالكترونية بين دوافع ارتكابها واليات مواجهتها: الإستراتيجية الإمنية للدولة الجزائرية في مكافحة الجرائم الإلكترونية أنموذج، المؤتمر الدولي العلمي الافتراضي، 2022، برلين، ص188.

[25] ميرغني، فيروز. مرجع سابق، 2017.

ثانياً: خصائص الجريمة الالكترونية:

للجرائم الالكترونية خصائص تجعل من الصعب الانتباه إليها، مما يجعل محاربتها صعبة ومعقدة للغاية، وأهم هذه الخصائص هي كما يلي:

1. **متعدية الحدود:** فهي جريمة لا تنحصر بزمان أو بمكان، فهي لا تلتزم بالحدود الإقليمية ولا الدولية، فالجريمة الالكترونية في ظل عولمة الإعلام أصبحت تختزل الزمان والمكان، أي أن الجريمة ستكون مترامية جغرافيا بآن واحد، كما أنها ستكون عابرة للحدود في بعض الأحيان، وقد تكون محلية في أحيان أخرى، فمرتكب الجريمة قد يكون بدولة ما وينفذ جريمته بدولة أخرى، وقد ترتكب في ذات الدولة[26].
2. **صعوبة إثباتها:** يعود هذا لقدرة الجاني على التخفي وإخفاء أداة الجريمة وآثارها، فالكشف عن الجريمة الالكترونية تحتاج لوقت طويل للكشف عنها أو تكتشف بمحض الصدفة ويعود هذا لقدرة الجاني على تدمير الأدلة بسهولة وبوقت قصير جدا قد لا يتجاوز الدقيقة الواحدة أحيانا[27].
3. **عدم التبليغ عنها:** حيث تتحفظ المؤسسات ذات الأسهم العالمية والبنوك على الجرائم الالكترونية التي تتعرض لها وذلك للحفاظ على زبائنها وسمعتها، الأمر الذي يدفع مرتكبو الجرائم الالكترونية للتوسع في نشاطهم وتطوير أساليبهم[28]، وكذلك عدم التبليغ عن الكثير من الجرائم الالكترونية بسبب خوف الضحية من التشهير[29]، كما هو الحال في الجرائم التي ترتكب ضدّ الفتيات.
4. **سهولة إخفاء آثار وأدلة الجريمة:** ويعود ذلك لقدرة الجاني العالية على التحكم بتقنيات برامج الكمبيوتر مما يجعل من عملية تدمير الأدلة سهلة عليه، وبالتالي يصّعب إثباتها وإدانة المجرم[30].

---

[26] بورشاق، زغودة. أسباب الجريمة الإلكترونية من منظور سوسيو انثروبولوجي، جامعة المدية الجزائر، المؤتمر الدولي العلمي الافتراضي، برلين، 2022، ص243-244.

[27] بورشاق زغودة، مرجع سابق، ص 244.

[28] شمسان الجيلي، الجرائم المستحدثة بطرق غير مشروعة لشبكة الإنترنت، دار النهضة العربية – القاهرة، السنة 2009، ص: 39.

[29] معهد أبحاث السياسات الاقتصادية (ماس)، دراسة نقدية للإطار القانوني للجرائم الالكترونية في الأراضي الفلسطينية، 2012، ص 12.

[30] شمسان الجيلي، مرجع سابق، ص 40.

5. **تعدد أنواع المجرمين:** وذلك لتعدد مستويات احتراف اختراق الأنظمة الحاسوبية، فمنهم الهاكرز (المتسللون) وهم على مستوى عال من الاحترافية في أنظمة الاتصالات والحاسوب ويستخدمون مهاراتهم لاختراق مواقع معينة، ومنهم الكراكرز (المخترقون) وعادة ما يكونوا ذوو مستوى متوسط وهم هواه[31].
6. **النعومة:** وهي أهم ميزة تختص بها الجريمة الالكترونية عن الجريمة المتعارف عليها في العادة، إذ تتميز الجرائم الالكترونية بالهدوء والنشاط العقلي المرتكز حول الهدف المقصود بالجريمة على خلاف الجريمة التقليدية والتي تمتاز بالخشونة كونها تعتمد على القوة الجسدية والعنف المباشر[32].

ثالثاً: دوافع ارتكاب الجريمة الالكترونية

لا تختلف أسباب ارتكاب الجرائم الالكترونية عن الجرائم التقليدية كثيرا، ومن أبرزها:

1. **دوافع مادية:** وهو الدافع الأكثر شيوعاً فالأرباح منها كبيرة ومجدية؛ مما يدفعهم إلى سرقة الأموال وتحوليها إلى حساباتهم الشخصية[33].

2. **دوافع شخصية:** ويقصد بها رغبة الأفراد في التعلم، فيقضون أغلب أوقاتهم في التعلم على كيفية اختراق الممنوعات والتقنيات الأمنية.

3. **دوافع ذهنية أو نمطية:** في الغالب يكون للأفراد من خلالها الرغبة في تحقيق ذاتهم والوصول إلى الانتصارات، فيما يخص تقنيات الأنظمة المعلوماتية[34].

4. **دافع الانتقام:** وهو الدافع الأكثر خطورة في ارتكاب الجرائم الالكترونية، وتزيد خطورتها عندما يمتلك هؤلاء الأفراد معلومات كبيرة عن شركات أو مؤسسات معينة[35].

---

[31] هشام رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة – مصر، السنة 1992، ص 40.

[32] هشام رستم، مرجع سابق، ص 40.

[33] طيب، ميرفت محمود. مرجع سابق.

[34] بورشاق، زغودة. مرجع سابق، ص247.

[35] طيب، ميرفت محمود. مرجع سابق.

5. **دافع التسلية:** ويقصد بذلك قيام الأفراد بارتكاب الجرائم الالكترونية بهدف التسلية فقط، ولا يقصد من ورائها إحداث جريمة[36].

6. **دوافع سياسية أو أيدولوجية:** تتبنى العديد من المنظمات في عصرنا وجهات نظر وأفكار سياسية أو أيديولوجية أو دينية معينة؛ وللدفاع عن هذه الآراء تقوم بأفعال إجرامية ضد معارضيها[37].

7. **دوافع تنافسية:** ويتجلى ذلك في محاولة الحصول على المعلومات التقنية الحديثة، والأسرار التقنية أو العسكرية، أو في محاولات الشركات المتنافسة للحصول على معلومات حول المعاملات المصرفية والمالية وذلك بواسطة أشخاص مؤجرين لهذا الغرض بالخصوص.[38]

8. **دوافع نفسية:** ويكون المرتكب يعاني أمراضاً نفسية أو خلل نفسي ينعكس على السلوك، مثل الرغبة في الانتقام أو الإيذاء أو التعرف على نقاط ضعف الآخرين وتتبعهم[39].

9. **دوافع اجتماعية:** تتدخل العوامل الاجتماعية في نشـــوء الجريمة الالكترونية، حيث يعمد المجرم الإلكتروني إلى اختراق الحاسب الشخصي أو الأجهزة الالكترونية الخاصة بشخصية محددة؛ بغية التعرف على نقاط ضعف أحدهم أو الإساءة لأحد من أسرة ذوي أصول ولها مكانتها وتاريخها، أو بدافع الانتقام[40].

رابعاً: مظاهر تحديات الجريمة الالكترونية

يمكن ايجاز مظاهر تحديات الجريمة الالكترونية فيما يلي[41]:

1. عدم وجود اتفاق موحد بين قوانين الدول على مفهوم الجرائم الالكترونية؛ وأصنافها وسبل المساءلة والمحاسبة عليها في ضوء القوانين الجزائية الجاري بها العمل في كل بلد.

---

[36] طيب، ميرفت محمود. مرجع سابق.

[37] بورشاق، زغودة. مرجع سابق، ص247.

[38] طيب، ميرفت محمود. مرجع سابق.

[39] بنار، مراد. الجرائم المرتكبة عبر الوسائط الإلكترونية، رسالة ماجستير – جامعة القاضي عياض، المغرب، 2018 ص14.

[40] بورشاق، زغودة. مرجع سابق، ص247.

[41] راجع بخصوص تلك المظاهر: عطايا، ابراهيم. مرجع سابق، ص375.

2. النقص الواضح في خبرة رجال الشرطة وجهات الادعاء والقضاء تشكل تحدياً كبيراً في القضاء على هذه الجريمة[42].
3. الهجوم على برامج الكمبيوتر والمعلومات الحاسب يجعلنا نواجه مشكلة قانونية ذات طبيعة خاصة، وقد أطلق على هذه الجريمة في فرنسا بجريمة التوصل بطريق التحايل لنظام المعالجة الآلية للبيانات وهي جريمة مستحدثة[43].
4. نمو نشاط الجرائم الالكترونية ووصول الجناة إلى تقنيات جديدة غير مسبوقة في مجال تكنولوجيا المعلومات والاتصالات[44].
5. يصعب تضمين بعض الأنشطة الإجرامية الالكترونية في الأوصاف الجنائية التقليدية في القانون الجنائي المحلي والأجنبي[45].
6. اتخذت ظاهرة الجريمة السيبرانية أنماطاً وأشكالاً جديدة من المعلومات الإجرامية، وهذا بلا شك يمثل تحدياً جديدا اليوم[46].
7. يبدو أن ضعف نظام الملاحقة الجنائية يتمثل في عدم القدرة على استيعاب هذه الظاهرة لإجرامية الجديدة، سواء كانت ملاحقة جنائية بموجب القانون المحلي أو على مستوى الملاحقة الجنائية الدولية[47].
8. يعد الجدل حول مسألة تخزين المعلومات والبيانات المعالجة إلكترونياً خارج الحدود أحد أكبر تحديات الجرائم الالكترونية، إذ نتج عنه اتجاهان لمكافحة هذا الصنف من الجرائم:

<u>يرى الاتجاه الأول</u>: أنه ومن غير المشروع قيام سلطات دولة ما بالتدخل وتفتيش النظم المعلوماتية المتواجدة في دولة أخرى؛ بهدف كشف وضبط أدلة إثبات جريمة كانت قد وقعت على أراضيها، وذلك استنادا إلى مبدأ اقليمية القانون[48].

---

[42] بورشاق، زغودة. مرجع سابق، ص247.

[43] عطايا، ابراهيم. مرجع سابق، ص375.

[44] بورشاق، زغودة. مرجع سابق، ص247.

[45] معاشي، سميرة، ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد 7، جامعة خيضرة بسكرة، الجزائر، 2011، ص258.

[46] معاشي سميرة، مرجع سابق، ص 259.

[47] عطايا، ابراهيم. مرجع سابق، ص376.

[48] بورشاق، زغودة. مرجع سابق، ص249.

<u>أما عن الاتجاه الثاني:</u> فيتمثل في إمكانية تشكيل القانون الدولي من خلال توافق الآراء على الصعيد الدولي باتجاه السماح بتنفيذ هذه الإجراءات حال توافر ظروف معينة يتم تحديدها، مثل إشعار الدولة المراد تفتيش البيانات والمعلومات المخزنة في نظام المعلومات لديها[49].

[49] بورشاق، زغودة. مرجع سابق، ص250.

المبحث الثاني: أركان وأنواع الجرائم الالكترونية

تواجه الجريمة السيبرانية إساءة استخدام شبكة تكنولوجيا المعلومات "الإنترنت"، وإساءة استخدام وسائل التواصل الاجتماعي وأنماط الاتصال التي أنشأتها ثورة تكنولوجيا المعلومات الحديثة، أو هي إساءة استخدام الحاسب الآلي على نحو متعمد في الغالب.

ومن الواضح أن مناط التجريم ينصب على سوء استغلال أو الاستفادة غير المشروعة مما تسمح به الوسائل التكنولوجية الحديثة، من طرف بعض الأشخاص ومستخدمي تلك الوسائل، مما يترتب عليه إضرار بحقوق الأشخاص الآخرين سواء على المستوى المادي أو المعنوي، وهو ما يخلق لدينا فلعاً جرمياً مكتمل الأركان، وجبت المساءلة والمحاسبة عنه.

وعليه، سيتم الحديث في هذا المبحث عن أركان الجريمة الالكترونية (المطلب الأول)، ثم أنواعها (المطلب الثاني).

المطلب الأول: أركان الجريمة الالكترونية

يشترط لقيام الجريمة الالكترونية قانوناً عدة أركان، وهي[50]:

أولاً: الركن المادي

يمكن أن يعزى العنصر المادي في الجرائم السيبرانية بسوء استخدام واستغلال الأنظمة الالكترونية بطريقة غير مشروعة، أو اقحام آثار مادية ملموسة تساهم في التدمير المقصود للبيانات والمعلومات، فالسلوك الإجرامي يعد عنصراً أساسياً في الركن المادي في الجرائم التقليدية، مثل مشاهدة الجاني ورؤيته رأي العين لحظة قيامه بالجريمة، أما بالنسبة للجرائم الالكترونية من الصعب أن يتم امساك الجاني مادياً، ويعود ذلك إلى طبيعة تلك الجرائم كونها ترتكب عن طريق قاعدة البيانات المتواجدة على أنظمة الحواسب الآلية.

وحتى تتضح الرؤية يتكون الركن المادي من العناصر التالية [51]:

أ. **النشاط الإجرامي:** السلوك الإجرامي هو النشاط المادي الخارجي الذي يصدر عن الجاني ليحقق النتيجة الإجرامية التي يعاقب عليها القانون، وهو عنصر ضروري في كل جريمة.

---

[50] سلام، كرم، مرجع سابق، ص57.

[51] العجمي، عبد الله. مرجع سابق، 26-29.

ولا يتدخل المشرع الجنائي بالعقاب قبل صدور النشاط المادي الخارجي المكون للجريمة. وتفسير ذلك أن الجاني قبل أن يقدم على الجريمة، يمر بمراحل من النشاط الذهني أو المادي لا يتناولها المشرع بالعقاب ذلك لأن الجريمة تبدأ بفكرة في ذهن الجاني قد يصرف النظر عنها وقد يصمم على تنفيذها. وإلى هذا الحد لا يباشر الإنسان نشاطاً مجرماً يستحق العقاب. لأن المشرع لا يعاقب على النوايا الآثمة والمقاصد الشريرة مهما كانت واضحة، ومهما أقر بها أصحابها. فما لم تخرج إلى حيز الوجود في شكل سلوك مادي ملموس تبقى خارج دائرة العقاب[52].

نظراً لأن مجرم الجريمة السيبرانية يختلف عن مجرم الجرائم الأخرى من حيث أن لديه خبرة كافية في استخدام التقنيات الحديثة، فإن الأعمال الإجرامية الصادرة عنه في مجال ارتكاب الجريمة السيبرانية تختلف بالضرورة عن المجرمين التقليديين. في جريمة الإرهاب السيبراني، فإن الإجراء الإجرامي هنا هو إطلاق صفحة أو موقع يدعوك ويحرضك على الانضمام إلى مثل هذه المجموعات، أو مثلاً تبين كيفية صنع واستخدام القنابل والأسلحة النارية.

ويكون السلوك الإجرامي مرتبط أيضاً بالمعلومات المحتفظة، أو التي يتم إدخالها إلى الحاسب الآلي وقد يتمثل السلوك الإجرامي أيضا في تدمير نظم المعلومات وقواعد البيانات أو التزوير، وذلك من خلال التسلل إلى أرصدة الحسابات المتوافرة في البنوك.

ب. **النتيجة الجرمية:** على مستوى الجرائم التقليدية، هي ما يترتب على الفعل الذي أتاه الجاني، فلا يكفي قيام الجاني بسلوكه الإجرامي مهما بلغت جسامته، بل لا بد من أن ينتج عن هذا السلوك نتيجة، ففي جريمة القتل لا بد من أن ينتج عن سلوك الجاني وفاة المجني عليه، فإذا لم تنتج الوفاة عن فعل القتل لا نكون أمام جريمة قتل وإنما نكون أمام جريمة شروع في القتل[53].

ت. **علاقة السببية:** يجب أن تتوافق العلاقة السببية بين سلوك الجاني وبين العواقب الناتجة عن أفعاله، أي أن النتيجة الجرمية سببها سلوك الجاني، ففي جريمة القتل وفاة الضحية سببه

---

[52] نظام توفيق المجالي، شرح قانون العقوبات – القسم العام، دار الثقافة للنشر والتوزيع، عمان – الأردن، سنة 2015، ص 254.

[53] بورشاق، زغودة. مرجع سابق، ص265.

سلوك الجاني الإجرامي. وقد نستطيع تطبيق ذات القواعد العامة المطبقة في الجرائم العادية على الجرائم الالكترونية فيما يتعلق بعلاقة السببية إذا انطبقت عليها، ففي جريمة سرقة الشيء المعلوماتي: يمثل اختلاس الشيء المعلوماتي عنصراً أساسياً يتحقق به النشاط المادي الصادر عن الجاني سواء بتشغيله للجهاز للحصول على المعلومة أو البرنامج أو الاستحواذ عليها، وهو ليس بحاجة لاستعمال العنف لانتزاع الشيء، إذ بتشغيله للجهاز لاختلاس المعلومة تتحقق النتيجة بحصوله عليها، فرابطة السببية إذن متوافرة بين نشاطه المادي والنتيجة الإجرامية[54].

ثانياً: الركن المعنوي

ويقصد هنا حالة مرتكب الجرائم الالكترونية المزاجية والنفسي، ومن الضروري التركيز على العلاقات المرتبطة ما بين ماديات الجريمة وشخصية الجاني. إذ إن توافر الركن المعنوي في الجرائم الالكترونية يعتبر من أهم الضوابط لتحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص التي يلزم تطبيقها، حيث أنه وبدون الركن المعنوي يعد التمييز بين جريمة الدخول غير المشروع إلى أنظمة معالجة البيانات الآلية وبين جريمة تجاوز الصلاحيات في الدخول على مثل هذا النظام، تمييزاً دقيقاً. [55]

ففي جريمة تجاوز صلاحية الدخول، فإنه يلزم لتوافرها أن يكون هناك صلاحية للدخول إلى نظام ما، على أن تتوافر داخل هذا النظام أنظمة معينة ليس من حق هذا الشخص الدخول إليها، ففي هذه الحالة لا تتوافر سوى جريمة واحدة، حيث إن المذكور يملك صلاحية الدخول إلى النظام الأساسي ولا يملك الدخول على أنظمة أخرى فيه، إلا أن تكوين النشاط المادي هنا يلزم أن يكون السلوك الإجرامي مرتكبا في ألاّ يكون هناك سوى جريمة واحدة هي جريمة الدخول أو الولوج غير المشروع.

والركن المعنوي في الجريمة الالكترونية له ثلاث صور، وهي:

أ. **العمد:** نظرا لأن الجريمة الالكترونية هي جريمة عالية لتقنية تتطلب معرفة مهنية وتعليما من قبل الأشخاص الذين يستخدمون هذا النوع من وسائل الاتصال، فإنه كان من المتصور

---

[54] الجبور، محمد، الوسيط في قانون العقوبات _ القسم العام، ط1، دار وائل، الأردن، 2012، ص238.

[55] الجبور محمد، مرجع سابق، ص 239.

غالباً عدم وقوعها إلا في صورة واحدة وهي صورة العمد، أي أن مرتكب تلك الجريمة قد خطط ودبر لارتكابها سواء من أجل الحصول على المعلومة أو لاختراق شبكة حاسوب آخر.[56]

ب. **القصد المتعدي:** يمكن أن يتوافر القصد المتعدي في جرائم الإنترنت، ومثال ذلك: الحالة التي يكون فيها الوصول بقصد التسلية في مسار القطارات، فيخرج الأمر عن السيطرة ويتم تدمير بيانات تحريك القطارات عبر الحاسوب، وبالتالي تحدث كارثة تكون نتيجتها خسائر مادية وبشرية كبيرة[57].

ت. **الخطأ غير العمدي:** للخطأ مكانه في تطورات الركن المعنوي في جرائم الإنترنت، إذ أن هناك بعض الجرائم تتم نتيجة لخطأ لم يكن مقصوداً، مثل تدمير أجهزة المؤسسة بسبب الإفراط من قبل الموظف المسؤول الذي استخدم جهاز الحاسب العائد لها بعمليات لحسابه الخاص معتمداً على مهاراته في تجنب متاعب الفيروسات[58].

ثالثاً: الركن الشرعي (القانوني)

الركن الشرعي يعني السند القانوني لتجريم الفعل وذلك تطبيقا لمبدأ الشرعية بأن "لا جريمة ولا عقوبة إلا بنص" وإعمالا لذلك فإنه من غير الممكن بحال الاجتهاد من القاضي الجزائي، إذ لا يجوز القياس في التجريم، والجرائم الالكترونية حديثة وذات تقنية عالية، ووضع نصوص خاصة بها ليس بالأمر السهل[59].

وعلى الرغم من ذلك إلا أن هناك بعض الدول وضعت قوانين لمثل تلك الجرائم، وتعد دولة السويد أول دولة تضع قوانين خاصة لهذه الجرائم، حيث أصدرت في عام 1973 قانون البيانات، وبعد ذلك وبين عامي (1976-1985) سنت الولايات المتحدة الأمريكية قانون لحماية أنظمة الحاسب الآلي، فتبعتها فرنسا والتي قامت في عام 1988 بتطوير قوانينها الجنائية لتتوافق مع ما استحدث من جرائم. وأما فيما يخص الدول العربية فقد قامت بعضها بسن بعض القوانين في هذا المجال،

---

[56] إبراهيم خالد ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي – الإسكندرية، الطبعة الأولى، السنة 2009، ص 78.

[57] إبراهيم خالد ممدوح، مرجع سابق، ص 79.

[58] إبراهيم خالد ممدوح، مرجع سابق.

[59] الجبور محمد، مرجع سابق، ص 59.

مثل السعودية التي أصدرت في العام 2007 نظامي التعاملات الالكترونية ونظام مكافحة الجرائم المعلوماتية والإمارات العربية المتحدة التي أصدرت القانون الاتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات 60 ، وفي فلسطين جاء القرار بقانون رقم (10) بشأن الجرائم الالكترونية عام 2018، وفي الأردن قانون الجرائم الالكترونية الأردني رقم (17) لِسنة 2023، وفي مصر جاء القانون رقم (175) بشأن مكافحة جرائم تقنية المعلومات سنة 2018[61].

المطلب الثاني: أنواع الجرائم الالكترونية

من خلال استقراء تعريف الجريمة الالكترونية، يمكننا أن نرى أن هناك نوعان من هذه الجرائم. الأول هو جريمة المعلومات على شبكة الإنترنت. هذا عندما يستهدف مرتكبو الجرائم الالكترونية الإنترنت. أما بالنسبة للجريمة الثانية غير المعلوماتية في الإنترنت، أي عندما يكون الإنترنت وسيلة لارتكاب جرائم إلكترونية.

أولاً: الإجرام المعلوماتي على الإنترنت

1. **القرصنة:** عمل يرتكبه متسلل عن طريق الوصول إلى نظام جهاز الحاسوب الخاص بك دون إذنك، فالهاكرز (المتسللون) عادة ما يكونوا مبرمجي حاسوب ذوي فهم متقدم لأجهزة الحاسوب، غالباً ما يسيئون استخدام فهمهم ومعرفتهم لأسباب خادعة، يفعل بعضهم ذلك لمجرد التباهي بخبراتهم، بينما الآخرون يريدون فقط التسبب في التدمير، وقد يؤدي الميول للتلصص في بعض الأحيان في قيام أحد المتسللين باختراق قواعد البيانات لسرقة البيانات المالية لشركة ما أو المعلومات المصرفية الشخصية[62].
2. **نشر الفيروس:** الفيروسات هي برامج حاسوب ترتبط وتصيب نظاماً أو ملفات، وتميل للانتشار إلى أجهزة حاسوب أخرى على الشبكة ما يعني أنها تعطل تشغيل الحاسوب وتؤثر على البيانات المخزنة عبر تعديلها أو بحذفها. وينظر للفيروسات غالباً على أنها رمز غريب

---

[60] العزام، سهيل محمد. الوجيز في جرائم الإنترنت، ط1، المكتبة الوطنية، الأردن، 2009، ص36.

[61] المضحكي، حنان ريحان مبارك، الجرائم المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، ط1، 2014، ، ص56.

[62] عطايا، ابراهيم. مرجع سابق، 360-403.

مرتبط ببرنامج مضيف، لكن في بعض الأحيان يتم التلاعب بالبيئة بحيث يؤدي استدعاء برنامج شرعي –غير مصاب- لاستدعاء البرنامج الفيروسي. ويمكن أيضاً تنفيذ البرنامج الفيروسي قبل تشغيل أي برنامج آخر، وعادة ما تنتشر فيروسات الحاسوب عبر الوسائط القابلة للإزالة أو عبر الإنترنت، مثل قرص فلاش أو قرص مضغوط أو أي جهاز تخزين آخر كان موجودا في جهاز حاسوب مصاب يصيب جميع أجهزة الحاسوب المستقبلية التي يتم استخدامه فيها،[63].

3. **القنابل الالكترونية:** أو ما يعرف باسم الشفرات، وهي جزء خبيث من التعليمات البرمجية يتم إدخاله قصداً في البرنامج لتنفيذ مهمة ضارة عند تفعيلها بواسطة حدث معين، فهو ليس فيروساً رغم أنه عادة ما يتصرف بطريقة مماثلة حيث يتم إدخاله خلسة في البرنامج فيظل في وضع السكون حتى تستوفى الشروط المحددة[64].

وغالبا ما تحتوي البرامج الضارة مثل الفيروسات على قنابل منطقية يتم تشغيلها في حمولة معينة أو في وقت محدد مسبقاً عادة ما يتم استخدام القنابل المنطقية من قبل موظفين ساخطين يعملون في قطاع التكنولوجيا المعلوماتية، وذلك لحذف قواعد بيانات أصحاب العمل، أو تسخير الشبكة لفترة أو حتى القيام بالتداول من الداخل.

4. **اقتحام الويب:** وذلك بهدف محاولة التحكم بموقع الويب بطريقة احتيالية، حتى يتحكم بتغيير محتوى الموقع الأصلي أو حذف بيانات من عليه، فقد تم الإبلاغ عن حالات طلب فيها المهاجم فدية، وحتى نشر مواد فاحشة على الموقع[65].
5. **المطاردة السيبرانية:** تعد شكلا جديدا من أشكال جرائم الإنترنت عندما يتم ملاحقة شخص ما أو ملاحقته عبر الإنترنت، والمطارد الإلكتروني لا يتبع ضحيته جسديا، يفعل ذلك افتراضيا من خلال متابعة نشاطه عبر الإنترنت، لجمع معلومات حول المطارد ومضايقته أو توجيه تهديدات باستخدام التخويف اللفظي، وهو ما يمثل انتهاكاً لخصوصية المرء على الإنترنت.

وتتم المطاردة عبر الإنترنت بطريقتين أساسيتين وهما المطاردة عبر الإنترنت: هنا يقوم المطارد بمضايقة الضحية عبر الإنترنت، البريد الالكتروني غير المرغوب فيه هو الطريقة

---

[63] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، الطبعة الثانية 2006، ص 195.

[64] أحمد خليفة الملط، المرجع السابق، ص 196.

[65] أحمد خليفة الملط، المرجع السابق، ص 202.

الأكثر شيوعا لتهديد شخص ما، وقد يرسل المطارد محتوى فاحشاً وفيروسات عبر البريد الإلكتروني[66].

6. **سرقة الهوية:** تحدث سرقة الهوية عندما يسرق شخص ما هويتك ويتظاهر بأنه أنت للوصول إلى الموارد المالية للضحية: مثل بطاقات الائتمان والحسابات المصرفية والمزايا الأخرى باسمك[67].
7. **التلاعب بالبيانات:** هو تغيير غير مصرح به للبيانات قبل أو أثناء الدخول إلى نظام الحاسوب ثم تغييرها مرة أخرى بعد انتهاء المعالجة، أي أنه يتم تغيير المعلومات الأصلية التي سيتم إدخالها، إما عن طريق شخص يكتب البيانات أو فيروس مبرمج لتغيير البيانات، أو مبرمج قاعدة البيانات أو التطبيق أو أي شخص آخر يشارك في عملية الإنشاء والتسجيل أو ترميز البيانات أو فحصها أو تحويلها أو نقلها. وهي من أبسط الطرق لارتكاب جريمة متعلقة بالحاسوب، لأنه حتى هواة الكمبيوتر يمكنهم فعل ذلك، على الرغم من أن هذه مهمة سهلة، يمكن أن يكون لها آثاراً ضارة[68].

ثانياً: الإجرام غير المعلوماتي في شبكة الإنترنت

1. **الابتزاز:** يتم الابتزاز من أجل الانتقام من شخص معين عبر سرقة بيانات ومعلومات خاصة بهذا الشخص أو غيره سواء أكان شخصاً طبيعياً أو معنوياً، بناء على نوع الجريمة الالكترونية "الابتزاز الإلكتروني" والذي يحدد لنا سبب الجريمة المرتكبة[69].
2. **تجارة الجنس والدعارة**: والتي تتم على مواقع إلكترونية مخصصة، هدفها تجاري يُستغل فيه بعض الفئات كالأطفال والنساء لغايات جذب عملاء إلكترونيين والترويج للمثلية من خلال إعلانات إشهارية غير أخلاقية والتي تدر عليهم مبالغ طائلة، وهذه الممارسات قد

---

[66] عطايا، ابراهيم. مرجع سابق، 360-403.

[67] صغير يوسف، الجريمة المرتكبة عبر الأنترنيت، مذكرة ماجستير في قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص 45.

[68] عطايا، ابراهيم. مرجع سابق، 360-403.

[69] صغير يوسف، مرجع سابق، ص 45.

تكون سبباً لجرائم إلكترونية ذات طبيعة جنسية عبر الفضاء الالكتروني، وهذا كله يؤدي لترويجها كسعلة استهلاكية خاصة بدول العالم الإسلامي[70].

3. **التجسس الالكتروني على الحكومات**: وذلك عبر اختراق الأنظمة الأمنية للحكومات أو سرقة معلومات سرية، وقد يقود هذا للتنافس السياسي والاقتصادي والذي عادة ما يكون بين دولتين أو معسكرين. وتستهدف هذه الجرائم المواقع العسكرية والأنظمة الأمنية والعبث في السياسة الأمنية لدولة ما أو تدمير وتخريب الأنظمة الأمنية لها، مما يعرض أجهزة الأمن الداخلي للدولة لهجمات إرهابية وأخطار أمنية كبيرة [71].
4. **السب والقذف والتشهير:** وهذا النوع من الجرائم هي الأكثر شيوعا بين جرائم الإنترنت، وإن كانت جريمة التشهير من الجرائم العادية إلا أنه ونظراً لوقوعها عبر الإنترنت تصنف ضمن الجرائم الالكترونية. وتتنوع صور السب والقذف بتنوع الغرض من استخدامها: فمنها ما يكون وجاهيا عبر مجموعات الأخبار خصوصاً إذ ما كان الجاني والضحية يتبادلان الرسائل أو بصدد النقاش بموضوع معين، وقد يكون كتابة أو تسجيلاً صوتياً[72].
5. **الاعتداء على الحياة الشخصية للأفراد:** إذ تقوم على مبدأ التمركز في موقع معين داخل شبكة الإنترنت والعمل على تسجيل وحفظ البيانات المتبادلة فيما بين نظم المعلومات، وتعتبر البيانات الشخصية مكان لتلك الاعتداءات. ووسائل هذه الاعتداءات هي "مبرمجات الحواسيب" والتي هي عبارة عن "جسيمات تنصب على الويب"، التي تستخدمها الشركات الالكترونية لتتبع المستهلكين عبر الإنترنت، ويتم الحماية منها عن طريق برامج رصد متطورة تسمى "ملفات تعريف الارتباط"[73]
6. **السرقة والنصب والاحتيال:** يعد هذا النوع من الجرائم واسع الانتشار عبر الإنترنت، وذلك بسبب عدم وضوح المصدر بالنسبة لمستخدمي هذه الشبكة، فضلاً على عدم توفر سبل الحماية اللازمة للحد من تلك الجرائم، ولعل أشهر صورها النصب ببطاقات الائتمان والذي

---

[70] صغير يوسف، مرجع سابق 2013، ص 48.

[71] بورشاق، زغودة. مرجع سابق، 251-252.

[72] أحمد خليفة الملط، المرجع السابق، ص 202.

[73] عطايا إبراهيم، مرجع سابق، 360-403.

يكون إما من حاملها الشرعي أو من الغير، وإن من بين الوسائل المعتمدة في تلك الجرائم عبر الإنترنت هي وسيلة البريد الإلكتروني[74].

7. **الاعتداء على الملكية الفكرية:** وذلك عن طريق العدوان على حقوق النسخ وكذا عن طريق العدوان على برمجيات الحاسوب وكذا العدوان على براءات الاختراع، ولقد حرمت عدة قوانين هذه الاعتداءات، منها القانون المصري ذو العلاقة بحقوق المؤلف [75].

وبعد أن تناول الباحث في هذا الفصل من الدراسة، ماهية الجرائم الالكترونية وما تشتمل عليه من أركان، والتطرق إلى أبرز أنواعها وصورها، سننتقل للحديث عن القواعد والأحكام الإجرائية الناظمة للجريمة المعلوماتية وإجراءات التحقيق الابتدائي فيها، وذلك في الفصل الثاني.

الفصل الثاني: القواعد الإجرائية الناظمة للتحقيق الابتدائي في الجريمة الالكترونية

تتطلب معالجة الجرائم الالكترونية والحد منها تحقيقاً فعالاً وقدرة عالية على جمع الأدلة والإثبات الجنائي، وهذا النهج يتطلب الاستجابة للصعوبات القانونية التي تعيق تنفيذ القانون وصولا للتحقيق في الجريمة الالكترونية وإثباتها. ومن هذا المنطلق أنشأت السلطة الوطنية الفلسطينية قسماً خاصاً بالتحقيق في الجرائم الالكترونية وجمع الأدلة الرقمية يتبع الشرطة الفلسطينية، وذلك لإدراكهم أهمية تكنولوجيا المعلومات كمفتاح لتحسين أداء الإدارة والأمن على السواء [76].

وعليه سوف نقسم هذا الفصل إلى ثلاثة مباحث، نتناول في المبحث الأول التحقيق الابتدائي والجهة المنوط بها إجراءه، فيما نتناول في المبحث الثاني: الدليل الرقمي وحجيته في الإثبات،

---

[74] أحمد، خليفة الملط، المرجع السابق، ص 203.

[75] عبد الحميد، عائشة. الإطار القانوني والإجرائي للجنوح السيبراني للأطفال في ظل القانون رقم 15-12 في الجزائر، 2022، 157-156.

[76] عبد الباقي، مصطفى. التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، جامعة بيرزيت: دراسات علوم الشريعة والقانون، المجلد 45، عدد 4، ملحق 2، 2018، ص286.

على أن نخصص المبحث الثالث للحديث عن ضمانات المتهم والإشكاليات العملية للتحقيق الابتدائي في الجرائم الإلكترونية.

المبحث الأول: ماهية التحقيق الابتدائي وإجراءاته في الجرائم الالكترونية

يعود تاريخ التحقيق الابتدائي الالكتروني إلى منتصف الثمانينيات من القرن الماضي استجابةً لانتشار الجرائم الالكترونية، وقد شهد التحقيق في هذا النوع من الجرائم تطوراً لافتا في الآونة الأخيرة، حيث أنشئت دوائر مستقلة في مؤسسات إنفاذ القانون، كما تم دعمها بفرق الأدلة الرقمية، مثل فِرق جمع الأدلة الرقمية وتحليلها وفحصها [77].

ومن المعلوم بالضرورة، أنّ الدعوى وقبل رفعها أمام المحكمة، يلزمها جمع المعلومات عن الفعل المرتكب من حيث نوع هذا الفعل ومن الذي ارتكبه والأدلة التي تثبت نسبة الفعل إلى مرتكبه وهذا ما يعرف بالتحقيق، وبناء عليه سيتم في هذا المبحث تناول تعريف التحقيق الابتدائي في الجريمة الالكترونية وأقسامه وخصائص التحقيق الابتدائي في الجرائم الالكترونية في المطلب الأول، وفي المطلب الثاني سيتم تناول إجراءات التحقيق الابتدائي في الجرائم الالكترونية.

المطلب الأول: مفهوم التحقيق الابتدائي في الجرائم الالكترونية والجهة المختصة

يعد التحقيق الابتدائي من أهم المراحل التي تمر فيها الدعوى الجزائية، وتماشياً مع طبيعة الدراسة، سيتناول الباحث تعريف التحقيق وأقسامه وخصائصه في الفرع الأول، على أن يتم تخصيص الفرع الثاني للحديث عن الجهة المختصة بالتحقيق في الجرائم الالكترونية.

---

[77] بخي، فاطمة الزهراء. إجراءات التحقيق في الجريمة الإلكترونية، رسالة ماجستير: كلية الحقوق والعلوم السياسية–جامعة المسيلة، 2014، ص 8.

الفرع الأول: تعريف التحقيق الابتدائي وخصائصه

لا يختلف مفهوم التحقيق الابتدائي في الجرائم الالكترونية عن الجرائم العادية، وحتى يتضح المفهوم تماما: سوف نعرف التحقيق بصفة عامة ثم المحقق وهو العنصر الأكثر أهمية في هذه العملية، وفيما يليه سنتناول مفهوم التحقيق الابتدائي في الجريمة الالكترونية.

التحقيق بالمعنى العام: اتخاذ كافة الوسائل والاجراءات المحددة قانوناً التي تقود لكشف الحقيقة وإظهارها" [78].

وعرّف التحقيق أيضاً: الاجراءات التي تقوم سلطات التحقيق في مباشرتها بالطرق المشروعة، بهدف دراسة الأدلة والبحث عن الحقيقة لكشفها قبل بدء مرحلة المحاكمة [79].

تعريف المحقق: هو شخص يعهد إليه القانون بالتحقيق في حقيقة القضايا الجنائية، والتحقيق فيها، وكشف أسرارها للعثور على حقيقة القضية، وظروف وقوعها وملابساتها، والعثور على الجاني وجمع الأدلة ضده استعداداً لمحاكمته.[80].

أولاً: أقسام التحقيق الابتدائي

هناك من قسم التحقيق لقسمين، وهما[81]:

1. **التحقيق الابتدائي العملي:** وهو جميع إجراءات التحقيق التي يقوم بها المحقق عند وقوع الجريمة توصلاً لمعرفة الحقيقة، وتستند على التجارب العملية التي وصل إليها المحققون في تحقيق القضايا الهامة.
2. **التحقيق الابتدائي الفني:** يعتمد على البحث العلمي والتجارب الفنية التي يمكن تطبيقها لمعرفة حقيقة الجرائم والاهتداء لفاعليها.

---

[78] الشعار، خالد. التحقيق الجنائي في الجرائم الإلكترونية. بحث مقدم لاستيفاء متطلبات الحصول على درجة الدكتوراة في الحقوق، جامعة المنصورة، بدون سنة نشر، ص3.

[79] الشعار، خالد، مرجع سابق، ص4.

[80] الشعار، خالد، مرجع سابق، ص17.

[81] بخي، فاطمة الزهراء. مرجع سابق، ص39.

ثانياً: خصائص التحقيق الابتدائي في الجرائم الالكترونية

يتميز التحقيق الابتدائي في الجريمة الالكترونية بمجموعة خصائص يشترك في بعض منها مع التحقيق الابتدائي في الجرائم التقليدية، مثل السرية وتدوين التحقيق[82]، غير أنه يمتاز بخصائص تقتصر عليه دون غيره، تتلخص فيما يلي:

1. تطور مفاهيمه؛ حيث أصبح هنالك مصطلحات حديثة ملائمة بشكل كبير وأقرب لطبيعته الافتراضية، مثل: استبدال مصطلح التفتيش بالولوج.
2. صعوبة بيانها لهيئة المحكمة وسهولة زرع الشك فيها، ويعود ذلك لصعوبة إدراك مفاهيم التحقيق، حيث لا يوجد هيئة مختصة في البت والفصل بالجرائم الالكترونية، فجوهر اكتشاف هذه الجريمة يعتمد على فطنه وذكاء وخبرة المحقق وتطور أساليبه.
3. تتخذ نمطاً مغايراً للشكل التقليدي، فهي ترتكب على شبكة الإنترنت بواسطة جهاز الكمبيوتر، فحدود هذه الجريمة غير واضحة وآثارها غير مرئية.
4. يواجه التحقيق الابتدائي في الجرائم الالكترونية نوع خاص من المتهمين، فمرتكبي الجرائم الالكترونية يمتازون بالذكاء والقدرة العالية على استخدام التطور التكنولوجي في الإنترنت.
5. يعاني المجتمع من عدم الاهتمام بالجرائم المرتكبة بواسطة الحاسوب وتقنيات الاتصال على المستويين التشريعي والقضائي[83].

الفرع الثاني: الجهات المختصة بالتحقيق الابتدائي والسلطات الممنوحة لهذه الجهات

هيئة التحقيق أو النيابة العامة هي إحدى مؤسسات العدالة الجنائية الرسمية، المتخصصة بشكل أساسي بإقامة الدعوى الجزائية، وتتمثل مهمتها الرئيسية في التحقيق بالجرائم والتصرف بشأنها،

---

[82] عبد الباقي، مصطفى. شرح قانون الإجراءات الجزائية، سلسلة المناهج الدراسية رقم 2، جامعة بيرزيت، 2015، ص185.

[83] راجع فيما يتعلق بخصائص التحقيق الابتدائي في الجرائم الالكترونية: الشعار، خالد، مرجع سابق، ص6-7.

حيث تبدأ عملها فور وقوع الجريمة. فالنيابة العامة في فلسطين تجمع وظيفتي الاتهام والتحقيق، في حين أن قضاة التحقيق مسؤولون عن إجراءات التحقيق الابتدائي في بعض النظم القانونية.

أولاً: وحدة الجرائم الالكترونية

استحدث المشرع الفلسطيني وحدة متخصصة في جهاز الشرطة وقوى الأمن من مأموري الضبط القضائي تسمى "وحدة الجريمة الالكترونية"، وتتولى النيابة العامة الإشراف القضائي عليها، كل في دائرة اختصاصه، بهدف مكافحة الجريمة الالكترونية وذلك عبر قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الالكترونية، ثم تم تعديله بقرار بقانون رقم (28) لسنة 2020 لتسمى "وحدة الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات"[84].

وفي مصر قامت وزارة الداخلية بإنشاء عدة أجهزة أسندت لها مهمة ضبط ما يقع من جرائم على الشبكة العنكبوتية نعرض لها على النحو التالي: إدارة مكافحة جرائم الحسابات وشبكات المعلومات، حيث أنشئت هذه الإدارة بموجب قرار وزاري، وهي تتبع الإدارة العامة للمعلومات والتوثيق وتخضع للإشراف المباشر لمدير الإدارة العامة، تشرف عليها فنيا مصلحة الأمن العام التابعة لوزارة الداخلية، وتضم ثلاث أقسام رئيسية، هي: قسم العمليات، قسم التأمين وقسم البحوث والمساعدات الفنية، وهي تتكون من ضباط متخصصين في مجال تكنولوجيا الحسابات والشبكات وتختص بمكافحة جرائم الانترنت على مختلف أنواعها[85].

وهناك قسم مُكافحة جرائم الحِسابات وشَبكة المعلومات، حيث أنشئ هذا القسم بالإدارة العامة للبحث الجنائي بمديرية أمن القاهرة، وهو يختص بعمليات تأمين ورقابة نظم وشبكات المعلومات لمنع وقوع أية جرائم عليها باستخدام الأساليب والتقنيات العلمية الحديثة ورصد ومكافحة وضبط الجرائم التي تقع باستخدام أجهزة الكمبيوتر على نظم وشَبكات المعلُومات وقواعد البيانات[86].

أما على مستوى الأردن فقد تم تصنيف الجرائم الالكترونية فاستحدثت (شعبة المتابعة والتحقيق) سنة 2008، والتي تختص في الجرائم الالكترونية. وصدر قانون جرائم أنظمة المعلومات في

---

[84] أنظر نص المادة الرابعة من القرار بقانون رقم 38 لعام 2021.

[85] بنار، مراد، مرجع سابق، ص130.

[86] بنار، مراد، مرجع سابق، ص130.

الأردن سنة 2010، وقبل صدوره كانت تستمد الجرائم المعلوماتية أحكامها من قانون العقوبات الأردني. ولمواجهة مشكلة الجرائم الالكترونية انضمت المملكة الأردنية الهاشمية للاتفاقيات والمعاهدات الدولية التي تجرم جرائم الإنترنت، وسنت قوانين وتشريعات جديدة تجرم الجرائم المعلوماتية، كقانون المعاملات الالكترونية، وأنشئت إدارة جديدة بوزارة الاتصالات تكون مسئولة عن الجرائم الالكترونية [87].

ثانياً: المحقق وأصل سلطته في الجريمة الالكترونية

يعتبر المحقق عضو من أعضاء سلطة إنفاذ القوانين والذي يقوم بأخذ كافة الإجراءات القانونية والإدارية والفنية الهادفة للكشف عن الجرائم والتعرف على فاعليها وإلقاء القبض عليهم وتجميع الأدلة لمساعدة ضحية الجريمة في خروج من أزمته، وقد يكون من قسم النيابة العامة أو قسم الشرطة، أو فرد في لجنة أو فريق وفق ما تقتضيه طبيعة الجريمة وظروفها [88].

وعليه يمكننا القول إنه لا يوجد فرق بين المحققين الجنائيين في الجرائم التقليدية عن الجرائم الالكترونية، ولكن الفرق يكمن في نوعية الجريمة هل تقليدية أم إلكترونية؟

ثالثاً: آلية التحقيق الابتدائي في الجرائم الالكترونية

تمر عملية التحقيق الابتدائي في الجرائم الالكترونية بمرحلتين رئيستين، الأولى: تمثل الإجراءات التي يتم تنفيذها بمسرح الجريمة، وتشمل إغلاقه وتأمينه ومنع العبث به؛ لمنع فقدان أو تلف أو تلوث الأدلة، والثانية: تشتمل على الخطوات التالية التي ينبغي على فريق مسرح الجريمة من مأموري الضبط القضائي ذوي الاختصاص القيام بها.

---

[87] مرعي، جمال. 2022، منشورات موقع حماه الحق، https://jordan-lawyer.com/2021/10/15/cyber-crime-investigation/

[88] الشعار، خالد، مرجع سابق، ص24

الإجراءات التي يتم تنفيذها في مسرح الجريمة

- معاينة مسرح الجريمة وذلك لضمان آلية منظمة للتحقيق في مسرح جريمة ما، إذ أن هناك ثلاث مراحل أساسية لمعالجته، تشمل: تحديد مسرح الجريمة؛ توثيقه؛ وجمع الأدلة. والآلية المنظمة ونقصد هنا بالآلية المنظمة مجموعة متتابعة من الإجراءات والواجبات المتفق والموافق عليها.

- توثيق حالة مسرح الجريمة، أي تدوين كافة المواصفات المتعلقة بحالة الجهاز المرتكب عبره الجريمة، مثل فحص ما إذا كان في وضع التشغيل متصلاً بالإنترنت أم لا وقت ضبطه.
- توثيق الجهاز المستخدم في الجريمة والأجهزة الملحقة به التي يعثر عليها في مسرح الجريمة، وذلك لأهمية رمز بروتوكول الإنترنت الذي يلعب دورا كبيرا في تحديد موقع ومكان المشتبه به.
- توثيق أجهزة التخزين مثل الأقراص المضغوطة الموجودة في مسرح الجريمة.
- تصوير مسرح الجريمة.
- حفظ الأدلة والمواد الرقمية.
- حفظ الوثائق المطبوعة.
- حفظ الأجهزة.
- إجراء استرجاع للوثائق العالقة، من قبيل طباعة الأوراق العالقة في ماكينة الطباعة.
- إجراء استرجاع للوثائق الملغاة أو التي تم حذفها.
- نقل الأدلة التي يتم ضبطها[89].

[89] عبد الباقي مصطفى، التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، مرجع سابق، ص286.

وبالنظر لقانون جرائم أنظمة المعلومات الأردني رقم (17) لسنة 2023، نجد أن المشرع الأردني أجاز لضابطة العدلية (مأموري الضبط القضائي)، بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة، الدخول لأي مكان تشير الدلائل إلى استخدامه في ارتكاب أي من الجرائم الواردة في القانون[90].

والجدير بالذكر: "أن صلاحيات مأمور الضبط القضائي تتسع في حالتي التلبس والتفويض لتشمل إجراءات التحقيق الابتدائي التي هي من حيث الأصل من صلاحيات النيابة العامة، لضرورة الاستعجال من أجل جمع الأدلة التي قد تمتد إليها يد العبث". وبعض من هذه الإجراءات لا يجوز لمأمور الضبط القضائي أن يقوم بها في الأحوال العادية لأنها تمس بحرية المواطن في بعض الأحوال، إنما يستطيع القيام بها في أحوال معينة على سبيل الاستثناء، كالإجراءات التي يقوم بها في حالتي التلبس والجرم المشهود والتفويض[91].

المطلب الثاني: إجراءات التحقيق الابتدائي في الجرائم الإلكترونية

سوف نتناول في هذا المطلب إجراءات التحقيق الابتدائي المألوفة وتطبيقها على الجرائم الإلكترونية، على أن يتم عرض الإجراءات المستحدثة للتحقيق الابتدائي في الجرائم الإلكترونية.

الفرع الأول: المعاينة والانتقال في الجريمة الإلكترونية

تعرف المعاينة لغةً بأنها: "المشاهدة بالعين"، عاين غيره رآه بعينه [92].

أما اصطلاحا: فحص حسي مباشر للأثر المادي الذي نتج عن ارتكاب الجريمة، عن طريق رؤيته أو فحصه فحصاً حسيا مباشرا بهدف المحافظة عليه خوفا من إتلافه أو محوه أو تعديله داخل مسرح الجريمة [93].

---

[90] أنظر المادة (32/أ/1) من قانون الجرائم الالكترونية الأردني رقم 17 لسنة 2023.

[91] عبد الباقي، مصطفى، شرح قانون الإجراءات الجزائية، مرجع سابق، ص185.

[92] بخي، فاطمة الزهراء، مرجع سابق، ص52 وما بعدها.

[93] بنار، مراد. مرجع سابق، ص157.

ومن الضروري هنا توضيح أهمية المعاينة في دورها لتصور آلية وطريقة وقوع الجريمة وظروف ملابساتها لتوفير الأدلة، والتحفظ على المتعلقات التي تفيد البحث والتحقيق. وعلى الرغم من أهمية المعاينة والانتقال إلا أنه تكمن المشكلة في عدم وجود مسرح مادي للجريمة مثل نظيره في الجريمة التقليدية، ففي الأخيرة تتم معاينة وتقفي آثار مادية بينما في الجريمة الالكترونية سيتم فيها تتبع نشاط إلكتروني في فضاء معلوماتي عن طريق وسائل تقنية وأجهزة لاستكشاف النشاط الإجرامي، بالإضافة لسهولة تدمير ومحو الأدلة في هذا الصنف من الجرائم [94].

ونظراً لصعوبة أمر المعاينة والانتقال فلابد أن يجمع مُجري المعاينة الأدلة بعناية فائقة، وأن يأخذ البيانات عن جهاز الكمبيوتر وجميع الأجهزة التي استخدمت في الجريمة، وتتبع أثرها من خلال بوابة الإنترنت[95]، وهنا من الضروري التمييز بين أنواع مسرح الجريمة المتعلق بالجرائم الالكترونية:

ينقسم مسرح الجريمة الالكترونية لقسمين[96]:

أ. المسرح التقليدي (المادي): ويشمل هذا المسرح جميع المتعلقات المادية لجهاز الكمبيوتر، والتي يمكن أن تحتوي على آثار مادية مثل بصمات الجاني أو وسائط تخزين رقمية.

ب. المسرح الافتراضي (الرقمي): ويقع داخل العالم الرقمي لجهاز الحاسب الآلي، ويحتوي على جميع المعلومات والبيانات الرقمية المخزنة فيه والتي تفيد في التحقيق.

أما عن معاينة المسرح الافتراضي للجريمة الالكترونية، ولتصبح معاينة مسرح الجريمة الالكترونية ذو فائدة عملية في الكشف عن ملابسات الجريمة، على المعاين مراعاة العديد من الإجراءات والخطوات الفنية، منها ما يكون قبل القيام بإجراء المعاينة، ومنها ما يكون أثناءها.

---

[94] طاهري، عيد المطلب. الإثبات الجنائي بالأدلة الرقمية، رسالة ماجستير – جامعة المسيلة، الجزائر، 2015، ص32.

[95] مرعي، جمال. 2022، منشورات موقع حماه الحق، https://jordan-lawyer.com/2022/01/02/inspection-in-cybercrime/

[96] بوعناد، فاطمة زهرة، "مكافحة الجريمة الإلكترونية في التشريع الجزائري، " مجلة الندوة للدراسات القانونية، العدد الأول، (دون دار نشر)، 2013، الجزائر، ص 68.

أولاً: الإجراءات والخطوات الفنية المتخذة قبل القيام بإجراء المعاينة

غالبا ما تكون هذه الإجراءات والخطوات تحضيرية، هدفها تهيئة العنصر البشري والأدوات المادية للقيام بإجراء المعاينة، حيث يتم ذلك عبر إعداد خطة عمل تشتمل على إعداد كامل للأدوات المستخدمة في المعاينة، وتوزيع المهام على الفنيين القائمين على هذا الإجراء، إضافة إلى توفير كافة المعلومات التي تم جمعها بالسابق عن مكان وقوع الجريمة وعن الأجهزة المراد معاينة نوعها وعددها، وذلك لتحديد إمكانيات التعامل معها فنيا من حيث التأمين والضبط وحفظ المعلومات، كما أنه يجب في هذا المرحلة توفير الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل وفك التشفير[97].

ثانياً: الإجراءات والخطوات الفنية المتخذة أثناء القيام بإجراء المعاينة

يقوم الفنيون المسؤولون على إجراء المعاينة بتصوير الحاسوب وكافة مكوناته المادية، مع ضرورة التركيز على تصوير الجزء الخلفي له ومراعاة تسجيل الوقت والتاريخ ومكان التقاط كل صورة، بالإضافة للقيام بملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل ملحقات جهاز الكمبيوتر، والاحتفاظ بكافة محتويات سلة المهملات من الأوراق الملقاة أو الممزقة، وكذا الشرائط والأقراص المضغوطة وفحصها [98].

ثم يتم البحث في جهاز الحاسوب عن الآثار الرقمية التي تركها المستخدم خلفه، وذلك بالاستعانة بكافة الوسائل التقنية كالدخول إلى السجلات والملفات، وهنا لا بد من تعطيل حركة الاتصالات السلكية واللاسلكية بشبكة الإنترنت تجنبا لتلف الدليل الجنائي الرقمي أو التلاعب به وتخريبه عمدا عن بعد، وفي حالة ضبط معلومات أو بيانات رقمية، لا بد من مراعاة قواعد تحريز الأدلة الجنائية الرقمية، والتي تتطلب تخزينها عناية فائقة للدعائم المادية وفحصها واستعمالها لاحقا[99].

---

[97] عبد المطلب، طاهري، مرجع سابق، 33-34.

[98] هروال، نبيلة. الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات :دراسة مقارنة، ط1، دار الفكر الجامعي، مصر، 2007، ص219.

[99] هروال، نبيلة، مرجع سابق، ص219-220.

الفرع الثاني: ندب الخبراء في الجريمة الالكترونية

الخبير في اصطلاح المحاكم: "هو الشخص الذي يتم تعيينه بهدف التدقيق في مختلف الأمور المتعلقة بشتى القضايا وله القول الفصل في رأيه"[100].

الخبرة القضائية: " تعرف على أنها الاستشارات الفنية التي يتم الاستعانة بها من قبل القاضي أو المحقق بغية مساعدته في تكوين رأيه نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة، إذن فالخبرة وسيلة لتحديد التفسير الفني للأدلة بالاستعانة بالمعلومات العلمية، فهي في حقيقتها ليست دليلا مستقلا وإنما هي تقييم فني لهذا الدليل"[101].

أما عن الخبير: "هو فرد ذو كفاءة في مجال من المجالات الفنية أو العلمية أو غيرها من المجالات الأخرى، ومن خلال معلوماته وخبرته يمكنه إبداء الرأي في أمر من الأمور المتعلقة بالقضية التي تحتاج إلى خبرة فنية ذات طابع خاص، وإذا كان الاستعانة بخبراء فنيين في المسائل الفنية البحتة في الجرائم التقليدية مطلوباً، فالاستعانة به في مجال الجريمة السيبرانية أكثر من الضروري، وذلك بسبب أن عملية استخلاص الأدلة الجنائية الرقمية تتطلب مهارة ودراية كبيرة في مجال أجهزة الكمبيوتر، ولهذا كان لزاما أن يتم اللجوء إلى خبير فني ومتخصص" [102].

من المعلوم أن هناك حاجة دائمة إلى خبراء وفنيين عند وقوع الجريمة السيبرانية يتم توكيلهم من قبل وكيل النيابة العامة، حيث نص المشرع الفلسطيني في القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية في المادة (32) الفقرة 4 أنه ".. لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يتم انتدابهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات. "وقد تتسع دائرة عملهم لتشمل مرحلة المراجعة والتدقيق على العمليات الآلية للبيانات، وكذلك مرحلة إعداد البرمجيات وتشغيل جهاز الكمبيوتر وعلومه، وان نجاح الاستدلالات وأعمال التحقيق في هذه الجرائم يكون مرهوناً بكفاءة هؤلاء الخبراء، أضف إلى

---

[100] بخي، فاطمة الزهراء، مرجع سابق، ص88.

[101] طاهري، عبد المطلب، مرجع سابق، ص35.

[102] ثنيان ناصر آل ثنيان. إثبات الجريمة الإلكترونية: دراسة تأصيلية تطبيقية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، السعودية، 2012، ص108.

ذلك انه يجب على المحقق الجنائي أن يحدد للخبير الإلكتروني دوره في المسألة المنتدب فيها على وجه الدقة.

وفي ذات السياق، أقر المشرع المصري أنه على مزودي الخدمات الالكترونية التعاون مع الجهات المختصة لضبط الأدلة ذات العلاقة بالجريمة الالكترونية وذلك في المادة 6 الفقرة 3 من القانون رقم 175 لسنة 2018 والتي جاء فيها "أن اتفاق مـقدم الخدمة مع مرتكبي الجرائم حول تسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته وحركة الاتصالات التي تمت على ذلك النظام أو النظام التقني".

ولأهمية توافر الخبرة في كشف الجريمة الالكترونية أصدر رئيس مجلس الوزراء المصري في أغسطس من عام 2020، اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات، حيث تناول قَانون مُكافحة جَرائم تِقنية المَعلومات رقم 175 لسنة 2018، دور الخبراء في المواد 1 و10، وحددت اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات في المواد من 4 إلى 9 شروط تعيين الخبراء وقواعد عملهم، في حين لم ينظم المشرع الأردني مسألة الخبرة الفنية الالكترونية في القانون رقم 17 لسنة 2023.

الفرع الثالث: التفتيش وضبط الأشياء في الجريمة الالكترونية

إن إجراء التفتيش والضبط هو أحد إجراءات التحقيق التي تختص فيها سلطة التحقيق ويناط بالضابطة القضائية القيام بهما في بعض الحالات الاستثنائية، ويعتبر التفتيش وسيلة للحصول من خلاله على أدلة لبيان وظهور الحقيقة، ولا يكفي في التفتيش مجرد توافر شروطه سواء الموضوعية أو الشكلية، ولكن من الضروري أيضا مراعاة حدوده الداخلية وأهمها في ضرورة التقيد بالغرض من التفتيش أثناء تنفيذه وفقا لما ينص عليه القانون [103].

[103] عشماني، عز الدين. 2018. إجراءات التحقيق والتفتيش في الجرائم الماسة أبنظمة الاتصال والمعلوماتية، دائرة البحوث والدراسات القانونية والسياسية – مخبر المؤسسات الدستورية والنظم السياسية (العدد الرابع – جانفي)، جامعة المسيلة، الجزائر، ص60.

التفتيش لغة: من مصدر فتش أي بحث وسأل، فتش الرجل عن الشيء أي تصفحه [104].

تعريف التفتيش اصطلاحا: "البحث المادي في مكان بهدف الوصول لمتعلقات الجريمة الجاري جمع الاستدلالات والتحقيق بشأنها" [105].

في حين عرف المشرع الفلسطيني التفتيش بنظامه التقليدي (أي التفتيش عن الأدلة ذات الطبيعة المادية) بأنه: "إجراء من إجراءات التحقيق الابتدائي الذي لا يتم إلا بمذكرة من النيابة العامة أو في حضورها، بموجبه يتم بناء اتهام موجه إلى شخص معين يقيم في المكان المنوي إجراء تفتيشه بارتكاب جريمة ما؛ جناية أو جنحة أو من خلال اشتراكه في ارتكاب تلك الجريمة. أو لوجود قرائن قوية على أنه يحوز أشياء ذات علاقة بالجريمة التي جرى ارتكابها" [106].

ونظم المشرع المصري أمر التفتيش في القانون رقم 175 لسنة 2018 في المادة 6 الفقرة 2 التفتيش[107]، ما مضمونه أن التفتيش يقصد به عمليات البحث أو الدخول أو النفاذ إلى البرامج الحاسوبية أو قواعد البيانات، وغيرها من الأجهزة والنظم المعلوماتية استجابة لغرض الضبط.

أما عن التفتيش الإلكتروني: يعرف أنه إجراء تحقيقي تقوم به الضابطة القضائية بموجب مذكرة قضائية، أو بدون مذكرة في أحوال استثنائية، للبحث عن أدلة الجريمة الرقمية في جهاز كمبيوتر أو أي من أجهزة الاتصال الذكية [108].

يعد التفتيش أحد إجراءات التحقيق، الذي يهدف إلى البحث عن الأشياء المتعلقة بالجريمة، يقوم به موظف مختص طبقا لإجراءات مقررة قانونا في مكان يتمتع بمكانة خاصة من أجل الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثباتها أو نسبتها لفاعلها [109]. كما يعتبر التفتيش

---

[104] بخي، فاطمة الزهراء، مرجع سابق، ص72.

[105] بخي، فاطمة الزهراء، مرجع سابق، ص72.

[106] المادة (1/39) من قانون الإجراءات الجزائية الفلسطيني، رقم 3 لسنة 2001.

[107] قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018، منشور في الجريدة الرسمية عدد 32 مكرر (ج)، بتاريخ 2018/8/14.

[108] عبد الباقي، مصطفى. التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، مرجع سابق، ص289.

[109] بنار مراد، مرجع سابق، ص 158.

والتحفظ على أجهزة الحاسوب وأنظمة تخزين المعلومات وسيلة هامة في الكشف عن الجريمة الالكترونية. غير أن قانون الإجراءات الجزائية الفلسطيني لم يتطرق للتحفظ المستعجل على بيانات الحاسوب، كما فعل القانون النموذجي للإجراءات الجزائية، حيث أجاز لعضو النيابة العامة إصدار أمر لضمان التحفظ العاجل على بيانات حاسوب معينة وبيانات مرور الاتصالات السلكية واللاسلكية في حالات استثنائية [110].

حيث إن تفتيش المكونات المادية للكمبيوتر لا توجد فيه مشكلة في التنفيذ، لأنه يرد على أشياء مادية لا خلاف فيها لقواعد القانون، لأنه تطبق عليه القواعد التقليدية، لكن مع الأخذ بعين الاعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها، ونظام التفتيش تتطبق عليه الضمانات المقررة قانونا.

أما بالنسبة للقواعد الشكلية للتفتيش على أنظمة الكمبيوتر والانترنت، فإن المبدأ الأساسي للتفتيش يتم من قبل سلطة التحقيق، فيخضع في هذه الحالة للخصائص العامة لكافة إجراءات التحقيق، المتمثلة في وجوب التدوين بمعرفة كاتب والسرية عن الجمهور وحضور الخصوم ووكلائهم كلما أمكن ذلك. وهناك شروط للتفتيش تختص بها الجريمة الالكترونية دون غيرها من الجرائم، من بينها [111]:

- توافر الخبرة الفنية لدى القائم بالتفتيش من خلال أن يتلقى المحقق في الجريمة الالكترونية تدريبات فنية خاصة.
- تجنب التجاوز في التفتيش، وذلك بمنع التفتيش عندما لا توجد تحريات جدية تنبئ عن وجود دلائل قوية عن معلومات تفيد في كشف الحقيقة.
- أن يكون إذن التفتيش محدد المدة والتي تحتسب من يوم الإذن إلى الجهة المأذون لها إجراء التفتيش[112].

---

[110] عبد الباقي، مصطفى. التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، مرص247جع سابق، ص289.

[111] فرغلي والمسماري، عبد الناصر ومحمد، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، جامعة نايف العربية للعلوم الأمنية، الرياض،2007، ص 19

[112] المادة (2/32) من القرار بقانون رقم 10 لسنة 2018.

ولأن التفتيش في مسرح الجرائم ذات الطبيعة الالكترونية يعتبر فن بقدر ما هو علم، ينبغي على رجال الضبط القضائي القيام بما يلي من الخطوات[113]:

- تجهيز طاقم العمل والذي يتكون من رجل الضبط القضائي الموكل إليه مهمة التفتيش.
- التعرف قدر الإمكان على نظم الكمبيوتر قبل إجراء التفتيش.
- العمل على تجهيز وإعداد الخطة التي سيجري من خلالها عملية التفتيش.
- العناية بمسودة إذن التفتيش -اشتمالها على وصف محل التفتيش- وشرح إستراتيجية التفتيش الممكنة.

أما فيما يتعلق بالقواعد الموضوعية لتفتيش أنظمة الحاسوب والانترنت، فهي تتمثل في:

1. أن يكون التفتيش بصدد جريمة إلكترونية واقعة بالفعل سواء كانت جناية أو جنحة.
2. لا بد من توجيه الاتهام لشخص معين أو مجموعة أشخاص مشتبه في ارتكابهم الجريمة الالكترونية محل التحقيق، أو المشاركة في ارتكابها.
3. لا بد من توافر دلالات وإمارات قوية أو قرائن على وجود أجهزة، أدلة معلوماتية تفيد في كشف الحقيقة لدى المتهم.

استناداً إلى أهمية عملية التفتيش في كشف الجريمة الالكترونية قام المشرع الفلسطيني في المادة (32) من قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الالكترونية، بمعالجة هذا الموضوع حيث تضمنت المادة على قدرة الجهة المتولية للتحقيق بتفتيش الأشخاص والأماكن ووسائل التكنولوجيا ذات الصلة بالجريمة المرتكبة، كما أعطت لوكيل النيابة صلاحية الإذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات.

---

[113] خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، ط1، الإسكندرية، 2009، ص225 –226.

ويقصد بضبط الأدلة "وضع اليد على شيء متعلق بالجريمة التي وقعت ويفيد في الكشف عن كافة الحقائق عنها وعن مرتكبيها سواء كان هذا الشيء عقارا أو منقولا، وقد يرد الضبط على الأشخاص وهو ما يصطلح على تسميته بالقبض" [114].

والأصل أن الضبط يرد على الأشياء المادية فقط، وبالتالي هناك صعوبة في ضبط الأدلة في الجريمة الالكترونية، مثل رفع البصمات. وتكمن الصعوبة هنا في ضبط الوسائل الفنية المستخدمة في تدمير الأدلة وفي ضبط بيانات الحاسوب [115].

حيث عالج المشرع الفلسطيني موضوع الضبط بالقانون السابق ذكره في المادة (33) والتي جاء فيها: "1. للنيابة العامة الحصول على الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الالكترونية أو بيانات المرور أو البيانات المتعلقة بحركة الاتصالات أو بمستعمليها أو معلومات المشترك ذات الصلة بالجريمة الالكترونية. 2. للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة. 3. إذا لم يكن الضبط والتحفظ على نظام المعلومات ضرورياً أو تعذر إجراؤه، تنسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات. 4. إذا استحال إجراء الضبط والتحفظ بصفة فعلية، يتعين حفاظاً على أدلة الجريمة الاستعانة بكافة الوسائل المتاحة لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات. 5. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه، بما في ذلك الوسائل الفنية لحماية محتواها. 6. تحرر قدر الإمكان قائمة بالمضبوط المتحفظ عليه بحضور المتهم أو من وجد لديه المضبوط المتحفظ عليه، ويحرر تقرير بذلك، ويحفظ المضبوط المتحفظ عليه حسب الحالة في ظرف أو مغلف مختوم، ويكتب عليه ورقة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية".

ويلاحظ أن المشرع الأردني في قانون الجرائم الالكترونية الأردني رقم 17 لسنة 2023، المادة (32/أ/1+2) قد سمح لمأموري الضبط القضائي وذلك بعد الحصول على إذن من وكيل النيابة المختص الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم الالكترونية، وأجاز القانون لمأمور الضبط القضائي التحفظ على بيانات الحاسوب، وبيانات

---

[114] حجازي، عبد الفتاح، الجوانب الإجرائية لأعمال التحقيق، دار النهضة العربية، القاهرة ط1 ، ص 274.

[115] خالد، ممدوح إبراهيم، مرجع سابق، ص274.

مرور الاتصالات السلكية واللاسلكية بعد الحصول على إذن من وكيل النيابة المختص، وذلك في الحالات الآتية: إذا كان هناك احتمال بأنه تم ارتكاب جريمة، إذا كان لدى عضو النيابة العامة سبب للاعتقاد بأن البيانات متعلقة بالتحقيق في الجريمة، إذا كان لدي عضو النيابة العامة سبب للاعتقاد بأن البيانات المعنية عرضة للفقدان، أو التعديل بشكل خاص [116].

أما المشرع المصري، فقد نص في قانون رقم 175 لسنة 2018 في المادة 6 الفقرة 1 أن ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر، على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لذلك مقتض.

وحيث أن الضبط يكون محله في مجال الجرائم الالكترونية، البيانات المعالجة إلكترونيا، فقد ثار التساؤل: **هل يصلح هذا النوع من البيانات لأن يكون محلا للضبط، الذي يعني كما رأينا وضع اليد على شيء مادي ملموس؟**

كان هناك اتجاهان من قبل الفقه عند الإجابة عن هذا التساؤل: حيث يرى البعض أن بيانات الكمبيوتر لا تصلح لأن تكون محلا للضبط، لانتفاء الكيان المادي عنها، ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس، عن طريق التصوير الفوتوغرافي، أو بنقلها على دعامة أو غيرها من الوسائل المادية. ويستند هذا الراي إلى ان النصوص التشريعية المتعلقة بالضبط محل تطبيقها الاشياء المادية الملموسة[117].

ويرى الاتجاه الثاني أن البيانات المعالجة إلكترونيا 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[118].

---

[116] أنظر قانون الجرائم الالكترونية الأردني رقم 17 لسنة 2023، مرجع سابق.

[117] خالد ممدوح إبراهيم ، مرجع سابق، ص230.

[118] عقيدة، محمد أبو العلا، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، https://www.bibliotdroit.com/2021/12/blog-post_77.html

الفرع الرابع: إجراء الاعتراض الفوري

نصت المادة (36) من القرار بقانون رقم 10 لسنة 2018، على هذا الإجراء حيث جاء فيها أنه" للمحكمة المختصة أن تقوم بمنح الإذن الفوري بالاعتراض لمحتوى اتصالات، وتسجيلها أو نسخها وفق طلب النائب العام أو أحد مساعديه، ويتضمن قرار المحكمة جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والأفعال الموجبة له، ومدته. 2. تكون مدة الاعتراض في الفقرة (1) من هذه المادة، لا تزيد على ثلاثة أشهر من بداية تاريخ الشروع الفعلي في إنجازه، قابلة للتمديد مرة واحدة فقط. 3. يتعين على الجهة المكلفة بتنفيذ إذن الاعتراض إعلام النيابة العامة بالتاريخ الفعلي لانطلاق عملية الاعتراض، والتنسيق معها بخصوص اتخاذ التدابير اللازمة لحسن سيرها".

وبالنسبة للدخول غير المصرح به فقد جرى تنظيمه في المادة (33/أ/1) من قانون الجرائم الالكترونية، والتي جاء فيها "للمدعي العام المختص أو المحكمة ... إصدار أمر إزالة أو حظر أو إيقاف أو تعطيل أو تسجيل أو اعتراض خط سير البيانات أو أي منشور أو محتوى أو منع الوصول إليه أو حظر المستخدم أو الناشر مؤقتاً خلال المدة المحددة في القرار، وذلك بعد الحصول على إذن من المدعي العام المختص أو المحكمة المختصة، ولو لم ينص عليه صراحة باعتباره يدخل في نطاق التفتيش بمعناه القانوني ويندرج تحت مفهومه لما تقتضيه مصلحة وظروف التحقيق والكشف عن الحقيقة في الجرائم المعلوماتية[119].

المبحث الثاني: الدليل الرقمي وحجيته في الإثبات

إن النظرة للواقع الجديد للتقنيات الرقمية كونها ذات مدلول حقيقي ومؤثر في العالم المعاصر والمستقبلي، فما تنتجه تلك التقنية يؤدي دوراً لا نستطيع تجاهله حتى في المجتمعات بطيئة النمو في هذا المجال [120].

---

[119] أنظر المادة (33/أ/1) من القانون رقم 17 لسنة 2023، قانون الجرائم الالكترونية الصادر بتاريخ 2023/8/13، وكذلك المادة (7/أ) من القانون المذكور.

[120] الشقيرات، رزق الله، الصعوبات الناشئة في تطبيق أحكام جرائم الذم والقدح والتحقير عبر شبكة الإنترنت: دراسة مقارنة، رسالة ماجستير–جامعة عمان العربية، الأردن، 2009، ص126.

من جانبه أسهم القضاء المقارن بدوره في تشكيل ملامح الأدلة الرقمية في الجرائم الالكترونية المرتكبة عبر الانترنت بمجرد قبوله له ليكون مصدرا يلهم القاضي للإدانة كما البراءة في أحكامه، إلا أنه لا يمنع من الإقرار بدور علماء التقنية المؤثر هنا، فاعتماد قاضي الموضوع على الخبير الرقمي كما لو كان موضوع الخبرة قضية تتعلق بموضوع تقليدي، فهذا تحول خطير في مسار الخبرة، الأمر الذي يحد من إرساء تقليد مفادهُ أن كل ما يبديه الخبير الرقمي يعد حقيقة تجبر قاضي الموضوع على تقبله.

ويرى الباحث أن البحث في نطاق هذا النوع من الأدلة يعتريه صعوبة في رصد أسلوب بحد ذاته يمكنه أن يقدم منطقاً قانونياً نستطيع عبره رصد المعيار المفقود للدليل الرقمي، ويعود ذلك لعدم الاستقرار القانوني في آلية التعامل مع الأدلة الرقمية.

انطلاقاً من ذلك سنتناول في هذا المبحث، ماهية الدليل الرقمي (المطلب الأول)، وحجية الدليل الرقمي في الإثبات (المطلب الثاني).

المطلب الأول: ماهية الدليل الرقمي

سنتعرض في هذا المطلب لبيان وتحديد مفهوم الدليل الرقمي بكل جوانبه، وهذا بتعريفه وتحديد خصائصه ثم أنواعه.

أولاً: مفهوم الدليل الرقمي

الدليل الرقمي لغوياً

يقصد ب "الدليل" لغويا ما يستدلُّ به، ويقال أدلَّ، وفلاناً يدلُّ فلان، والدليل أي المرشد، وجمعه أدلّة[121]، ويقصد به أيضاً البرهان، بحيث يقال أقام الدليل أي بيّنَ وبرهنَ[122].

أما "الرقمي" هي أسم منسوب للدليل، واصلها رقم أي علامات الأعداد المعروفة 1،2...، وأيضا عدد وجمعها أعداد[123].

---

[121] الرازي، محمد بن أبي بكر، مختار الصحاح، دار الرسالة، الكويت، 1983، ص 209.

[122] المنجد الأبجدي، دار المشرق، لبنان، 1967 ص 446.

[123] الرازي، محمد بن أبي بكر، مرجع سابق، ص49.

الدليل الرقمي اصطلاحاً

يعرف الدليل في صورته المتعارف عليها أنه: "الجزء المادي الذي يؤدي إلى اقتناع قاضي الموضوع بارتكاب الشخص لجريمته على وجه اليقين" [124]، أما الدليل الجنائي يعرف بأنه " هو كل واقعة مادية أو معنوية تؤدي إلى إثبات وقوع الجريمة، أو تحديد شخصية مرتكبيها، أو إثبات ارتكابه لها سواء تم ذلك مباشرة أو عن طريق غير مباشر"[125].

أما فيما يتعلق بالدليل الرقمي فقد تنوعت التعريفات والمفاهيم له بين الفقهاء، إذ يرى جانب منهم أنه "مجموعة من المجالات والذبذبات المغناطيسية أو النبضات الكهربائية التي يمكن تجميعها وتحليلها باستخدام تطبيقات وبرامج خاصة؛ لتظهر في صور أو فيديوهات أو تسجيلات صوتية" [126].

ويرى جانب آخر أن الأدلة الرقمية" هي مجموعة من المعلومات تنسجم مع الفعل والمنطق ويأخذ بها العلم، ويتم الاستعانة بالدليل الرقمي بواسطة إجراءات قانونية وعلمية، من خلال ترجمة البيانات المخزنة في أجهزة الحاسوب وملحقاته، وشبكات الاتصال ويمكن الاستناد إليها في أيَّ مرحلة من مراحل التحقيق أو المحاكمة عند وقوع أي نوع من أنواع الجرائم الالكترونية" [127].

أما محكمة النقض المصرية عرفته بأنه: "أية معلومات إلكترونية ذات القيمة الإثباتية المخزنة أو المنقولة أو المأخوذة من جهاز الكمبيوتر أو شبكة المعلومات أو ما شابه ذلك، ويمكن تحليلها وتجميعها بواسطة أجهزة أو تطبيقات تقنية خاصة"[128].

---

[124] الشقيرات، رزق الله، مرجع سابق، ص114.

[125] طاهري، عبد المطلب. الإثبات الجنائي بالأدلة الرقمية، رسالة ماجستير – جامعة المسيلة، 2015، الجزائر، ص3.

[126] الحوامدة، لورنس. حجية الأدلة الرقمية في الإثبات الجنائي: دراسة تحليلية مقارنة، مجلة البحوث الفقهية والقانونية، العدد36، المملكة العربية السعودية، 2021، ص895.

[127] البشري، محمد الأمين. الأدلة الجنائية الرقمية، مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، السعودية، 2002، ص102.

[128] محكمة النقض المصرية، الطعن رقم 2093، السنة القضائية 89، جلسة بتاريخ 2020/6/13.

في حين لم يورد المشرع الأردني تعريفاً للدليل الرقمي بل تركه للفقه القانوني، وعليه عرّف الفقه الأردني الدليل الرقمي بعدة تعريفات تدور جميعها حول نفس الفكرة وإن اختلفت في ألفاظها، ومن هذه التعريفات، هو" الأدلة المشتقة من أو بواسطة النظم البرمجية المعلوماتية الحاسوبية، وأجهزة ومعدات وأدوات الحاسب الآلي، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علمياً أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور وأشكال وأصوات، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها" [129].

ثانياً: خصائص الدليل الرقمي

تستند خصائص الدليل الرقمي إلى البيئة التي نشأ فيها وهي البيئة الافتراضية العالم الافتراضي، وتتمثل هذه البيئة في جهاز الكمبيوتر بكل مكوناته المادية والبرمجية، ومنه انعكست هذه البيئة الافتراضية على طبيعة هذا الدليل، فأصبح يتصف بعدة خصائص ميزته عن الدليل التقليدي (المادي)، وهو ما سنتناوله تالياً:

1. يعد الدليل الرقمي دليلاً علمياً؛ فهو يحتاج إلى البيئة التقنية التي يتكون فيها، ومن هذا فإن ما ينطبق على الدليل العلمي ينطبق على الدليل الرقمي، غير أنه يجب ألا يحيد الدليل العلمي عن منطقه، ويجب أن لا يتعارض مع القواعد العلمية السليمة [130].
2. الأدلة الرقمية في الجرائم الالكترونية هي أدلة ذات طبيعة تقنية، فهي ليست كالأدلة المادية، فالتقنية هي التي تنتج هذه الأدلة مما يسمح بمصادرة الأدلة الرقمية. فإطلاق الصفة الرقمية تعني وجوب وجود توافق بين الدليل المرصود وبين البيئة التي يقبع فيها [131].

يدل هذا الأمر على أنه لا وجود للدليل الرقمي في الجرائم الالكترونية خارج البيئة التقنية، وإنما ليكون هناك دليلاً رقمياً يجب أن يكون مستنبطا من بيئته التي يتمحور بها وهي البيئة التقنية.

---

[129] حماة الحق – محامي الأردن، حجية الدليل الإلكتروني في القضايا الجزائية، https://jordan-lawyer.com/2021/11/02/authentic-electronic-evidence-in-criminal-cases/

[130] الشقيرات، عبدالله، مرجع سابق، ص128.

[131] طاهري، عبد المطلب، مرجع سابق، ص8.

3. الدليل الرقمي متطور ومتنوع في الجرائم الالكترونية، يشمل مصطلح الدليل الرقمي في الجرائم الالكترونية كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقميا، أي أن يكون بينها وبين الجريمة الالكترونية رابط من نوع ما أو أن تتصل بالهيمنة على النحو الذي يجد هذه الرابطة بينها وبين مرتكب هذه الجريمة، حيث يعد الاعتراف بالدليل الرقمي في الجرائم المرتكبة عبر الانترنت كونه من الأدلة المتطورة بطبيعتها، والتي لا تمتاز بالجمود والتبعية للتطور المتواصل في البيئة الرقمية، وذلك كله يستدعي دقة كبيرة من حيث التعامل مع هذه النوعية من الأدلة، وأي منها يكون مقبولا أو غير مقبولا لدى المحاكم [132].
4. التخلص من الأدلة الرقمية أمر صعب للغاية، لا يعد موضوع التخلص من الدليل الرقمي في الجريمة الالكترونية باستخدام خاصية التخلص من الملفات في الحاسوب أو الانترنت من العوائق التي تحول دون استرجاع الملفات المذكورة، حيث تتوافر برمجيات ذات طبيعة رقمية يمكن بواسطتها استرداد كافة الملفات التي تم حذفها من جهاز الحاسوب وذلك بسبب الثقة في التكنولوجيا حيث إن التقنية تستطيع القيام بتحقيق الخيال الإنساني بلا حدود [133].
5. الدليل الرقمي دليلاً عابراً للحدود وهذا يعني أنه لا ينحصر في بقعة جغرافيا محدّدة أو دولة معينة كما الحال في الأدلة التقليدية، بل قد يوجد الدليل الرقمي بأكثر من مكان سواء داخل أو خارج حدود الدولة؛ ويعود ذلك لارتباطه بالبيئة الافتراضية التي تغطي مساحة واسعة تعدى حدود الدولة الواحدة، فشبكة الإنترنت وسيلة اتصال أساسية عالمية، تتعدى كل حدود الدول عبر تبادل المعلومات والبيانات بين مستخدميها الأمر الذي يسهل عملية انتقال الدليل الرقمي من دولة لأخرى بدقة وسرعة [134].

ثالثاً: أنواع الأدلة الرقمية

تتنوع الأدلة الرقمية باختلاف أنواع البيانات أو المعلومات والأرقام داخل الوسائل الالكترونية في العالم الافتراضي، وعليه سنتناول في هذا البند أنواع الأدلة الرقمية.

---

[132] سعيداني، نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير– جامعة الحاج لخضر – باتنة –، كلية الحقوق والعلوم السياسية، الجزائر، 2013، ص 124.

[133] حنفي، حازم محمد، الدليل الإلكتروني ودوره في المجال الجنائي، ط1، دار النهضة العربية، 2017، ص19–22

[134] الحوامدة، لورنس، مرجع سابق، ص899.

النوع الأول: دليل أجهزة التقنيات الرقمية

هناك رأي لجانب من الفقهاء أن ما يتم إنشاؤه تلقائيًا في الأجهزة الالكترونية كأدلة رقمية دون تدخل بشري، أي أن الإنسان لم ينشئ هذه الأدلة، مثل: "سجلات الهاتف المحمول، فواتير أجهزة الحاسب الآلي"، وهناك أدلة رقمية يتم حفظها عبر إدخالها في جهاز الحاسب الآلي كالبيانات والمعلومات التي تم إدخالها، ثم معالجتها من خلال برامج معدّة لذلك [135].

ويرى جانب آخر أنَّ هناك سجلات تمَّ حفظ جزء منها عبر الإدخال إلى الحاسوب وجزء أخر تم إنشاؤه من خلال الحاسب الآلي وعلى سبيل المثال: "رسائل البريد الإلكتروني" حيث يكتبها الشخص بنفسه، ومن ثم يقوم الجهاز بإكمال بياناتها مثل: توقيت الإرسال وحفظها في البريد المرسل [136].

يرى الباحث أن هذا الدليل يمكن أن يكون وسيلة لإثبات الجرائم الإلكترونية، ويمكن للقاضي الاعتماد عليه للوصول إلى الحقيقة.

النوع الثاني: أدلة لم يتم إعدادها لتكون وسيلة للإثبات في الجرائم الالكترونية

إن هذا النوع من الأدلة الرقمية يتكون دون إرادة من مستخدم الجهاز أو الشبكة العنكبوتية، ويقصد به أنَّ المستخدم لهذه الوسائل التقنية قد يخلف أثراً لهذا النوع من الأدلة دون قصد إحداث هذا الدليل أو ذلك الأثر [137].

وعلى سبيل المثال **البصمة الالكترونية**، حيث يُخلق هذا الدليل عند استخدام جهاز الحاسوب أو الإنترنت من سجلات أو بيانات تم تسجيلها عند إرسال أو استقبال الرسائل أو المكالمات سواء عبر الحاسوب أو الإنترنت أي أن هذه الأدلة لا يتم حفظها من قبل المستخدم، بل تقوم الأجهزة

---

[135] الحلبي، خالد عياد. إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص 230.

[136] يوسف، أمير فرج. الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، ط1، مكتبة الوفاء القانونية، مصر، 2016، ص290.

[137] يوسف، فرج، مرجع سابق، ص290.

التقنية بحفظ البيانات من تلقاء نفسها ولو مضى فترة من الوقت على إجراء العملية؛ لذلك فإنَّ كل الإجراءات التي تتم بواسطة هذه الأجهزة أو الشبكة العنكبوتية يمكن ضبطها كأدلة من قبل المحققين عبر استخدام برامج تقنية خاصة لهذه الغاية [138].

من هذا يمكن ملاحظة أن النوع الأول من الأدلة يتميز بسهولة الحصول عليه من قبل الأجهزة المختصة، فهو دليل جاهز أصلا ليكون دليل إثبات على الوقائع التي يتضمنها كما يمكن الاحتفاظ به كدليل إثبات كما هو الحال في الأدلة التقليدية، أما النوع الثاني فإنه لا يمكن الحصول عليه إلا عن طريق اتباع الوسائل التقنية الخاصة بذلك، أي أنه لا بد من الاستعانة بأهل الخبرة أو استخدام تقنيات خاصة، كما يمتاز بصعوبة حفظه ويتطلب لحفظه تقنيات وآليات خاصة.

المطلب الثاني: حجية الدليل الرقمي في الاثبات في الجرائم الالكترونية

أولاً: مشروعية الدليل الرقمي

تستند إدانة المتهم في جريمة إلى أدلة تم الحصول عليها من مصادر مشروعة ووفقاً لقواعد النزاهة واحترام الضوابط والإجراءات المنصوص عليها في القانون، أما إذا تم الحصول على هذا الدليل من الوسائل الالكترونية بوسائل وطرق غير مشروعة أصبح الدليل باطلا، ويحق للمحكمة المختصة القضاء ببطلانه من تلقاء نفسها، إذا تعلق البطلان بالنظام العام كما أن الدليل الباطل بطلاناً مطلقاً لا يصلح للمحكمة أن تبني عليه قرار الإدانة بحق المتهم [139].

كما تتضمن مشروعية الدليل الرقمي أيضاً اقتناع القاضي وتكوين عقيدته بقرار الإدانة للمتهم، خاصة عندما تكون الأدلة الرقمية المستند إليها في الواقعة مشروعة ومبنية على إجراءات سليمة، مما يترتب عليه أنه لا يجوز للقاضي أن يبني قراره بالإدانة للمتهم على ما قد رآه بنفسه في غير قاعة المحكمة أو بناء على إجراء معيب وباطل فالقناعة الوجدانية للقاضي يجب أن تكون مشروعة ومبنية على أدلة وبينات مطابقة لواقع الدعوى وغير مخالفة للقانون [140].

---

[138] طاهري، عبد المطلب، مرجع سابق، ص8.

[139] الجسمي، خالد مصطفى. الإثبات الجنائي بالأدلة الرقمية، مجلة القانون المغربي، دار السلام للطباعة والنشر، المغرب، 2017، ع34، ص33.

[140] الحوامدة، لورانس. مرجع سابق. ص907.

ودليل على ما سبق ذكره فقد قضت محكمة النقض المصرية بما يلي: " لمحكمة الموضوع أن تستمد اقتناعها بثبوت الجريمة مِنْ أي دليل تطمئن إليه، ما دام له مأخذه الصحيح مِنَ الأوراق" [141]. وقضت أيضاً بأن "تقدير الدليل هو صلاحية لمحكمة الموضوع، بحيث تستطيع بسط سلطتها على الأخذ من أي بيئة أو قرينة ترتاح إليها" [142].

إذ أفرد المشرع الفلسطيني باباً متخصصاً لمعالجة مسائل البطلان في قانون الإجراءات الجزائية الفلسطيني وهو "الباب الرابع من الكتاب الخامس"، ورتب على عدم مراعاة أحكام القانون المتعلقة بأي إجراء جوهري البطلان، كما نظم المشرع الفلسطيني أحكام البطلان المتعلق بالنظام العام إذا كان راجعا لعدم مراعاة أحكام القانون المتعلقة بتشكيل المحكمة أو ولايتها أو باختصاصها من حيث نوع الجريمة[143].

ومن الجدير بالذكر أن المشرع الفلسطيني اعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو نظم المعلومات أو الموقع الالكتروني أو البيانات والمعلومات الالكترونية من أدلة الإثبات وفقا للمادة (38) من ذات القرار بقانون كما ظهرت في السنوات الأخيرة العديد من التشريعات الوطنية التي تهدف إلى تنظيم وتطوير البنية الأساسية القانونية لتطبيق المعاملات الالكترونية مع إرساء مبادئ قانونية للقواعد والمعايير المتعلقة بتوثيق وسلامة المراسلات والسجلات الالكترونية، والتي تتمثل أساسًا في الاعتراف بحجية الملفات ذات المدلول التقني، والإقرار بحجية التوقيع الالكتروني، ومعادلته بالتوقيع اليدوي باعتباره دليلا للإثبات، والتخلي بالتدريج عن أية قيود تحد من الإنترنت في البيئة التقنية، ومنها في فلسطين القرار بقانون رقم (15) لسنة 2017م بشأن المعاملات الالكترونية، وقانون المعاملات الالكتروني الأردني رقم 17 لسنة 2023، وقانون التوقيع الالكتروني المصري رقم 15 لسنة 2004، حيث اتفقت نصوص هذه القوانين على إعطاء المحررات الالكترونية حجية كاملة في الإثبات إذا استوفت الشروط القانونية [144].

---

[141] انظر: قرار نقض مصري رقم 10349 لسنة 88 قضائية بتاريخ 2021/2/6م

[142] انظر: قرار نقض مصري رقم 7834 لسنة 90 قضائية بتاريخ 2021/2/6م

[143] انظر: المواد (479-474) من قانون الإجراءات الجزائية الفلسطيني 3 لسنة 2001.

[144] الحجار وبشير، عدنان وفايز، الأدلة الرقمية وإثبات الجرائم السيبرانية ما بين التأصيل والتأويل، مجلة جامعة الاستقلال للأبحاث، المجلد 6، العدد 1، 2021، ص132.

ومن هذا المنطلق نستطيع تعريف مشروعية الدليل هو أن يكون الدليل معترف به، أي أن يجيز القانون للقاضي الاستناد إليه لتكوين عقيدته للحكم بالإدانة.

ثانياً: سلطة القاضي في تقدير الدليل الرقمي

يخضع تقدير الأدلة الرقمية لصلاحية المحكمة المختصة، وفي سبيل اقتناعها بالدليل الرقمي الذي تم الحصول عليه من الوسائط الالكترونية، تشرع المحكمة بفحص الدليل الرقمي والتأكد منه عبر طرحه في جلسة المحاكمة لمناقشته بحضور أطراف الخصومة في الجرائم الالكترونية وذلك في سبيل الوصول للحقيقة التي تُرضي ضمير القاضي وقناعته، وعليه لم يلزم المُشرع القاضي بالأخذ بدليل رقمي محدد، بل مَنحهُ القانون سلطة تقديرية لوزن الأدلة الرقمية كما الحال في الأدلة المتعارف عليها التي تقدم في الدعوى الجزائية [145].

ويرى بعض الفقهاء أنه يشترط في الدليل الرقمي حتى يكون له الحجيَّة في الإثباتات الجنائية أن تكون مخرجاته الالكترونية مشروعة وموافقة للقانون، كما يجب أن تكون يقينية وتم تحصيلها بوسائل مشروعة، كذلك لا بُدَّ مِنْ مناقشة الأدلة الرقمية في جلسة المحاكمة بحضور أطراف الخصومة في الجريمة الالكترونية، كي يصل القاضي المختص لليقين التام بالمخرجات الالكترونية وما ينتج عنها من أدلة رقمية، ويقوم أيضاً بإدراك هذه المخرجات بحواسه حتى يستطيع أن يربط هذه المخرجات بوقائع الدعوى المعروضة عليه" [146].

وعليه سنتناول أبرز الاتجاهات في مجال الإثبات، ومدى صلاحية القاضي في تقدير الأدلة في كل اتجاه على النحو الآتي:

1- نظام الإثبات الحر

في هذا النظام لا يحدد القانون طرقاً محددة للإثبات يلتزم بها القاضي إذ يترك حرية الإثبات لأطراف الخصومة في أن يقدموا ما يرون أنه مناسب لإقناع القاضي، هذا من جهة ومن جهة

---

[145] الجسمي، خالد مصطفى، مرجع سابق، ص38.

[146] الحوامدة، لورانس، مرجع سابق، ص 925.

أخرى يترك للقاضي الحرية الكاملة في قبول أي دليل أو استبعاده بناء على اقتناعه الصميم [147].

تخضع الأدلة كيفما كانت لسلطة القاضي التقديرية، وعلى الرغم من توفر شروط صحة الأدلة إلا أن القاضي له الحق في أن يستبعده تحت مبرر عدم الاقتناع وكما هو معلوم أن نظام الإثبات الحر مبدئياً لا يتعارض مع فكرة الدليل الإلكتروني الجنائي بل ينسجم معها سواء عندما يتعلق الأمر بإثبات جريمة تقليدية أو جريمة مرتكبة عبر الوسائط الالكترونية [148]. وأخذ بهذا النظام العديد من الدول مثل: الأردن، مصر، سوريا، ولبنان، وفرنسا.

2- نظام الإثبات المقيد

يستند هذا الاتجاه إلى عدم منح القاضي السلطة التقديرية للدليل بغض النظر عن نوعه تقليدي أم رقمي، أي أن القاضي لا يَملُك تقدير حجية الدليل بالمطلق، فالقانون يحدّد للقاضي ماهية الدليل ونوعه والقيمة القانونية له وحجيته في الإثبات، فلا يوجد قيمة قانونية للدليل إلا إذا نص عليه القانون واعتبره ضمن القائمة[149].

وعليه يمكننا القول إن مجرد الحصول على الأدلة الرقمية وتقديمها إلى القضاء لا يكفي لاعتمادها كدليل على الإدانة، فالطبيعة الفنية للأدلة الرقمية تمكن من العبث به على نحو يمكن معه أن يحيد عن الحقيقة دون أن يكون هناك أي قدرة لغير المتخصص إدراك ذلك، كما أن نسبة الخطأ في إجراءات الحصول على دليل صادق في الإخبار عن الحقيقة تبدو عالية في مثل هذا النوع من الأدلة ولهذا تثور فكرة الشك في مصداقيتها كأدلة للإثبات [150].

3- نظام الإثبات المختلط

يجمع هذا النظام بين النظامين السابقين ذكرهما، حيث أن نظام الإثبات أعطى القاضي سلطة التقدير لقبوله الدليل في بعض أدلة الإثبات كالأدلة الرقمية، وفي أدلة أخرى لم يكن للقاضي إلا

---

[147] بنار، مراد، مرجع سابق، ص 167.

[148] النوازلي، إدريس، موقف القضاء من الجريمة الإلكترونية، مقال منشور بمنشورات كلية العلوم القانونية والاقتصادية والاجتماعية، مراكش، سلسلة الندوات والأيام الدراسية، المغرب، 2010، ص103.

[149] حوامدة، لورانس، مرجع سابق، ص926.

[150] بنار، مراد، مرجع سابق، ص168.

الالتزام بالنص القانوني الذي يحدد القيمة والحجية للدليل، كدولة اليابان الآخذة بنظام الإثبات المختلط عدت الأدلة الجنائية التقليدية (كالشهادة، وأقوال المتهم والقرائن والخبرة) هي أداة قانونية، وليس للقاضي سلطة تقديرية فيها؛ لأن القانون هو الذي يمنح هذه الأدلة القيمة والحجة القانونية [151].

وفيما يتعلق بمدى تكييف أدلة الاثبات المتعارف عليها قانونياً كالشهادة، والدليل الرقمي على وجه الخصوص نستطيع أن نتصور أنه بحال حرر أحدهم خطابا على حسابه على تويتر فإنه يمكن اتخاذ هذا الخطاب كاعتراف منه على نفسه أو على غيره[152].

ولكننا نرى أن الأدلة الرقمية هي أدلة إثبات قائمة بذاتها لا تنطوي تحت أحد أدلة الإثبات المتعارف عليها، وهنا تثور المشكلة الحقيقة أننا في حاجة ملحة لوجود نص تشريعي لتعريف محدد للدليل الرقمي ومشروعيته وحجيته وإثره ينظمها القانون كدليل إثبات قائم بذاته حتى لا نتركها لأهواء القضاة وسلطتهم التقديرية.

حيث جاء قرار بقانون رقم (10) لعام 2018 بشأن الجرائم الالكترونية في المادة (37) أنه "يعتبر الدليل الناتج بأي وسيلة من وسائل التكنولوجيا المعلوماتية أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الالكترونية أو البيانات والمعلومات الالكترونية من أدلة الإثبات".

أما عن موقف المشرع الأردني من الدليل الإلكتروني كوسيلة اثبات في المسائل الجزائية، بالنظر لحداثة الدليل الإلكتروني في مسائل الإثبات فلا يوجد نص صريح في قانون أصول المحاكمات الجزائية الأردني على إدراج الدليل الإلكتروني ضمن وسائل الإثبات الجزائي، إلا أنه يفهم من نص (المادة147/2) من قانون أصول المحاكمات الجزائية "تقام البينة في الجنايات والجنح والمخالفات بجميع طرق الإثبات ويحكم القاضي قناعته الشخصية أن أدلة الإثبات الجزائي غير حسب محددة على سبيل الحصر إلا ما ذكره المشرع صراحة بالنسبة لبعض الجرائم الأمر الذي يعني جواز الاستناد إلى الدليل الإلكتروني في إثبات المسائل الجزائية شريطة أن تتوافر فيه شروط صحة أدلة الإثبات واقتناع القاضي بهذا الدليل .

---

[151] حوامدة، لورانس، ص627.

[152] مركز هردو لدعم التعبير الرقمي. الجريمة الإلكترونية وحجية الدليل الرقمي في الاثبات الجنائي، مصر، 2014، ص26.

وتأكيداً على ذلك قضت محكمة التمييز الأردنية بالحكم رقم 651 لسنة 2013 الصادر بتاريخ 2014 /7/10 بأنه: "يستفاد من (المادة 147) من قانون أصول المحاكمات الجزائية أنها أمدت محكمة الموضوع في المسائل الجزائية بالحرية الكاملة في الاقتناع بالأدلة المقدمة إليها دون رقابة عليها من محكمة التمييز في هذه المسألة الموضوعية ما دام أن النتيجة التي توصلت إليها لها ما يؤيدها في بينات الدعوى وتتفق مع العقل والمنطق."[153]

كذلك نصت المادة (88) من قانون أصول المحاكمات الجزائية الأردني على أن " للمدعي العام أن يضبط لدى مكاتب البريد كافة الخطابات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق كافة الرسائل البرقية كما يجوز له مراقبة المحادثات الهاتفية متى كان لذلك فائدة في إظهار الحقيقة والمحادثات الهاتفية ما هي إلا دليل إلكتروني فهذا دليل على قبول الأدلة الالكترونية كوسائل إثبات في المسائل الجزائية". [154]

وعلى المستوى الفلسطيني فقد بين القرار بقانون رقم (10) بشأن 2018م بشأن الجريمة الالكترونية في المادة (37) أنه "يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الالكترونية أو البيانات والمعلومات الالكترونية من أدلة الإثبات".

وباستعراض القوانين ذات العلاقة في فلسطين، فقد نص قانون البينات في المواد المدنية والتجارية رقم (4) لسنة 2001، على سريان أحكام الفصل المتعلقة بالسندات غير الموقع عليها، وهي من الأدلة الكتابية على وثائق نظم الحاسب الآلي. هذا يعني أن المشرع قد ساوى في الإثبات بين الوثيقة المادية المكتوبة والوثيقة الرقمية المكتوبة على الكمبيوتر.

أما قانون الإجراءات الجزائية فقد نص على أن تقام البيئة في الدعاوى الجزائية بجميع طرق الإثبات إلا إذا نص القانون على طريقة معينة للإثبات، وهذا يعني أن الإثبات بالوثائق الالكترونية جائز في الدعاوى الجزائية طالما لم ينص القانون على طريقة معينة للإثبات، وطالما اقتنع القاضي بالدليل.

---

[153] منشور على الموقع التالي: https://jordan-lawyer.com/2021/11/02/authentic-electronic-evidence-in-criminal-cases/، تاريخ الزيارة: 2023/10/15، ساعة الزيارة: 15:35.

[154] أنظر المادة (88) من قانون أصول المحاكمات الجزائية الأردني لعام 1961، وفق آخر التعديلات.

وعلى الرغم من ذلك، فإن معظم القضاة وأعضاء النيابة العامة يجهلون حيثيات المعلومات الأساسية الضرورية المتعلقة في الجرائم الالكترونية وكيفية التحقيق فيها وإثباتها ويفتقرون إلى التدريب المناسب والكافي، وبالتالي يترددون في الأخذ بالأدلة الرقمية لإثبات الجرائم الالكترونية [155].

أما بالنسبة لمشروع قانون المعاملات الالكترونية لسنة 2010، فقد تضمن تعريفات لعدد من المصطلحات، حيث عرف البيانات الالكترونية بأنها بيانات ممثلة أو مرمزة الكترونياً سواءً على شكل نص أو رمز أو صوت أو صور أو غيرها. كما عرف السجل الإلكتروني بأنه: "مجموعة من المعلومات التي تشكل وصفاً لحالة تتعلق بشخص أو شيء ما ويتم إنشاؤها أو نقلها أو تسلمها أو تخزينها بوسائل إلكترونية".

وبما أننا بصدد الحديث عن المعاملة الالكترونية فقد نص المشروع صراحة على أن يكون للمعاملات والتوقيعات الالكترونية أثرها القانوني ولا يشوبها أي عوائق وقابلة للتنفيذ شأنها في ذلك شأن الوثائق والمستندات الخطية بموجب أحكام التشريعات النافذة من حيث الزامها لأطرافها أو صلاحيتها في الإثبات. كما نص في ذلك اعتبار الصورة المنسوخة على الورق من رسالة البيانات الالكترونية الرسمية حجة على الكافة بالقدر الذي تكون فيه مطابقة لأصل هذه الرسالة. ويلاحظ على هذه النصوص أنها ركزت على العقود والتوقيعات الالكترونية. ويحق لنا التساؤل حول البيانات الالكترونية الأخرى من قبيل ملفات السجل وبيانات التعريف وغيرها ما إذا كانت مشمولة أم لا؟

المبحث الثالث: ضمانات المتهم والإشكاليات العملية للتحقيق الابتدائي في الجرائم الالكترونية

بما أن التحقيق يسعى إلى بناء العدالة في المجتمع وخلق المساواة من منطق القواعد التشريعية للتجريم والعقاب وفقاً لظروف وملابسات كل مادة، فقد أحيطت مرحلة التحقيق بسلسلة من الضمانات وإن اختلفت من تشريع لآخر من حيث المقدار، إلا أنها اتفقت عند ملاحقة المتهم أمام الجهات المختصة وجود ضمانات إجرائية تؤدي في ذات الوقت الى شعور القائمين بالتحقيق الاطمئنان في تنفيذ لمهامه، ومن هذا المنطلق سوف نتناول بهذا المبحث ضمانات المتهم في

[155] عبد الباقي، مصطفى، مرجع سابق، ص293.

المطلب الأول، على أن نخصص المطلب الثاني للحديث عن انتهاك الحق في الخصوصية باعتباره أحد أبرز الإشكالات العملية التي تواجه التحقيق الابتدائي في الجرائم الالكترونية.

المطلب الأول: ضمانات المتهم خلال مرحلة التحقيق الابتدائي

أولاً: مراعاة مبدأ أن الأصل في الإنسان البراءة

إن الافتراض العام لبراءة المتهم هو حق أساسي وهو أحد الأصول الراسخة فيه، وأحد أركان مفهوم المحاكمة العادلة في الدعوى القضائية ضد المتهم، وعليه أرست التشريعات المعاصرة هذا المبدأ كضمانه للمتهم باعتباره بريئا حتى تثبت إدانته بحكم قضائي نهائي أمام محكمة قانونية وعادلة، فلا بد من التأكد من قيامه بارتكاب الجريمة فقرينة البراءة من المبادئ الأساسية لحماية حقوق المتهم أمام العدالة الجنائية واحترامها [156]. ولترسيخ هذا المبدأ أقر المشرع بعد إلزام المتهم بتقديم ما يثبت براءته، بل إن سلطة التحقيق هي الملزمة بتقديم هذا الإثبات على ما تنسبه إليه من فعل مجرم، وهذا الحق كرسته كافة التشريعات الدولية والوطنية.

لذلك توصل المشرع الفلسطيني إلى ضمان عام يتمتع به المتهم أثناء إجراءات الدعوى الجزائية وهو ما تنص عليه المادة (14) من القانون الأساسي الفلسطيني: "المتهم بريء حتى تثبت إدانته...."، وبهذه القواعد الدستورية أصبح المتهم محاطاً بسياج من الضمانات ضد أي تعسفٍ أو تجاوز قد يمارس ضده.

ثانياً: حق المتهم في الصمت

الصمت هو أحد الحقوق العامة للمتهم، وهو حرية الشخص في الكلام أو الامتناع عنه ، فإذا كان للمدعى عليه الحق في المساهمة الإيجابية في الإثبات عن طريق حقه في تقديم الأدلة التي تشخص الاتهام المنسوب إليه، ويمكنه أيضاً التزام الصمت دون توضيح أنه اعتراف بالتهمة، ومن ثم إثبات الإدانة، فإن حق صمت المدعى عليه هو حق أصيل من حقوقه فلا يلزم أو يجبر

---

[156] المليح، عبد الله، صحّة الإجراءات الجزائية وأثرها في مواجهة الجريمة، أكاديمية شرطة دبي، الإمارات، 2015، ص83.

الشخص على الكلام أمام مأمور الضبط القضائي أو سلطة التحقيق فهو يمثل الضمانة الحقيقية للمتهم، الذي يجب أن يسمح له بمساحة حرة في تنظيم دفاعه كيفما يريد، ولو بالصمت دون أن يستنتج من هذا الصمت دليلا على سلامة ما ينسب إليه من اتهام [157].

تناول مشرعنا الفلسطيني هذه الضمانة في المادة (97) من قانون الإجراءات الجزائية بقولها: "للمتهم الحق في الصمت وعدم الإجابة على الأسئلة الموجهة إليه"، كما نصت المادة (217) من ذات القانون على أن "للمتهم الحق في الصمت ولا يفسر صمته أو امتناعه عن الإجابة اعتراف منه".

كما تناولها المشرع الأردني في المادة (77) من قانون اصول المحاكمات الجزائية " على قاضي التحقيق أن يراعي مبدأ حرية إرادة المدعى عليه أثناء استجوابه وأن يتأكد من أنه يدلي بإفادته بعيدا عن كل تأثير خارجي عليه سواء أكان معنويا أم ماديا".

ثالثاً: استعانة المتهم بمحام

يعتبر هذا الحق من حقوق الدفاع التي تعتبر ضمانة قانونية المشتكى في مرحلة التحقيق الابتدائي وضمانة أساسية لتحقيق العدالة، ولا يجوز حرمانه من حق الاستعانة بمحامٍ مهما كانت الظروف والأسباب[158].

وفي هذا جاءت المادة (64) من قانون المحاماة المصري رقم (17) لسنة 1983 [159] أنه على المحامي تقديم المساعدة القضائية للمواطن غير القادر وغيره في الحالات المنصوص عليها في القانون، وأن يؤدي واجبه عمن يندب بذات العناية التي يبذلها بحال كان موكلا ولا يجق للمحامي المنتدب التنحي عن مواصلة الدفاع إلا باستئذان المحكمة التي يتولى أمامها الدفاع، وعليه أن يستمر بالحضور حتى يقبل تنحيه وتعيين آخر، فتوجيه تهمة للمتهم من شأنه أن يوقع في نفسه الاضطراب، ولو كان بريئا لأن موقف الاتهام بذاته ذو رهبة قد يسئ معها المتهم حُسن دفاعه عن نفسه، ولذلك من الطبيعي أن يتم اللجوء لمحامي يساعده في دفاعه عن نفسه، حيث يتقدم

---

[157] المليح، المرجع السابق، ص92.

[158] صباح، صباح ناطق. ضمانات التحقيق مع الأحداث في مرحلة ما قبل المحاكمة في القانونين الأردني والعراقي، رسالة ماجستير–جامعة الشرق الأوسط، الأردن، 2017، ص93.

المحامي في الدفاع عن المتهم عبر إبداء الطلبات والدفوع وتسجيلها في المحضر أو طلب سماعا لشهود وطلب ندب الخبراء لإجراء المعاينة غير أنه لا يحق له المناقشة للشهود بل له الحق في إبداء رأيه. [160].

ولم يكتفي المشرع الفلسطيني بالنص على هذه الضمانة وإنما أوجب على المحقق تنبيه المتهم إلى حقه بالاستعانة بمحام وأن يتم تدوين هذا التنبيه بالمحضر وهذا ما نصت عليه المادة (69) من قانون الإجراءات الجزائية الفلسطيني" يجب على وكيل النيابة ... ويخبره أنه من حقه الاستعانة بمحام". كما جاء في المادة (102) من قانون الإجراءات الجزائية الفلسطيني الفقرة (1) أنه: "يحق لكل من الخصوم الاستعانة بمحام أثناء التحقيق"، وأيضاً المادة (123) يكون لكل موقوف حق الاتصال بذويه والاستعانة بمحام".

رابعاً: تدوين التحقيق

يعد التحقيق الابتدائي الذي يجريه المدعي العام مع المتهم أحد الخطوات المهمة لحماية الوقائع والمعلومات من التداخل أو النسيان، ويجب أن يقوم بتدوين التحقيق كاتب يرافق المدعي العام في إجراءات التحقيق كافة[161]، حيث تقضي القواعد العامة في الاجراءات الجزائية وجوب تدوين الاجراءات المتبعة في التحقيق ضماناً لحق المتنازعين فيستطيع أياً منهم الرجوع إلى هذه الإجراءات[162].

وقد تطرقت معظم التشريعات الوطنية إلى ضرورة تدوين التحقيق، حيث نص قانون الإجراءات الجزائية الفلسطيني في المادة (58) على وجوب مرافقة وكيل النيابة كَاتباً لتدوين المحاضر ويوقعها معدة، حيث يصطحب وكيل النيابة العامة في جميع إجراءات التحقيق كاتباً لتدوين المحاضر ويوقعها معه، وذلك لأنه لا يمكن الاعتماد على ذاكرة المحقق لمعرفة الإجراءات والآلية التي تمت بها، والتدوين يمثل ضمانة للمتهم فمن خلال التدوين يستطيع الرجوع إلى محاضر الإجراءات وما تضمنه من أمور في غيابه أو حتى في حضوره للاطلاع عليها، وبعد

---

[160] الشعار، خالد، مرجع سابق، ص20.

[161] بني فضل، علاء، ضمانات المتهم أمام المحكمة الجنائية الدولية، رسالة ماجستير–جامعة النجاح الوطنية، فلسطين، 2011، ص55

[162] الصباح، صباح، مرجع سابق، ص87.

[162] قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950، المادة 24، وفق آخر التعديلات عام 2020.

ذلك يستطيع هو ومحاميه من إعداد دفاعه بشكل يمكنه من إثبات براءته مما نسب إليه هذا من جهة، ويمثل نوع من الرقابة على المحقق ذاته من جهة أخرى، بحيث يراعي الدقة في تدوين إجراءات التحقيق ومطابقتها للتحقيق والواقع[163].

كذلك قانون أصول المحاكمات الجزائية الأردني أوجب على استعانة المحقق بكاتب لتدوين إجراءات التحقيق في المـادة (70).

وقانون الإجـراءات الجنـائية المصـري في المادة (73) منه، أوجب على المحقق أن يصطحب معه في جميع إجراءات التحقيق كاتباً يوقع معه المحاضرة[164]. كما جاء في المادة (24) بالفقرة الثانية من ذات القانون أنه يجب أن يتم تثبيت كافة الإجـراءات التي قام بها مأمورو الضبط القضائي في المحاضر الموقع عليها منهم يبين فيها وقت اتخاذ هذه الإجراءات ومكان حدوثها وأن تشمل زيادة على ما تقدم توقيع الشهـود والخبـراء الذين سمعـوا وتـرسل المحاضر للنيابة العامة مع الاوراق والاشياء المضبوطة"[165].

وبالنظر للمشرع الفلسطيني تنص المادة (58) من قانون الإجراءات الجزائية الفلسطيني، يصطحب وكيل النيابة العامة في جميع إجراءات التحقيق كاتباً لتدوين المحاضر ويوقعها معه، ذلك لانه لا يمكن الاعتماد على ذاكرة المحقق لمعرفة الإجراءات والكيفية التي تمت بها، والتدوين يمثل ضمانة للمتهم فمن خلال التدوين يستطيع الرجوع إلى محاضر الإجراءات وما تضمنه من أمور في غيابه أو حتى في حضوره للإطلاع عليها، وبعد ذلك يستطيع هو ومحاميه من إعداد دفاعه بشكل يمكنه من إثبات براءته مما نسب إليه، هذا من جهة، ويمثل نوع من الرقابة على المحقق ذاته من جهة أخرى، بحيث يراعي الدقة في تدوين إجراءات التحقيق ومطابقتها للتحقيق والواقع.

خامساً: السرية في التحقيق

تعد سرية التحقيق من أهم الضمانات العامة الممنوحة للمتهم، والتي تضمن عدم الإساءة والتشهير بالمتهم قبل إدانته، وصدور الحكم نهائياً بحقه من جهة، وعدم تأثير الرأي العام على

---

[163] قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001، المادة 58.

[164] قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950، المادة 73، وفق آخر التعديلات عام 2020.

[165] قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950، المادة 24، وفق آخر التعديلات عام 2020.

مجريات التحقيق من جهة أخرى، دفعت هذه الأسباب المشرع على اعتبار السرية أحد سمات مرحلة التحقيق الابتدائي[166].

وبناءً عليه يجب على المحقق إبقاء مجريات التحقيق طي الكتمان بحيث تكون إجراءات ونتائج التحقيق من الأسرار والحرص على سريتها، وقد فطن المشرع إلى أهمية المحافظة على أسرار التحقيق وعدم إذاعتها، وبهذا الصدد جاء في المادة (75) من قانون الإجراءات الجنائية المصري[167] أنه تعتبر إجراءات التحقيق ونتائجها من الأسرار ويجب على قضاة التحقيق وأعضاء النيابة العامة ومساعديهم من كتاب وخبراء وغيرهم ممن لديهم صلة بالتحقيق عدم إفشائها ومن يخالف هذا يعاقب وفقا للمادة 310 من قانون العقوبات[168].

وبالنظر للمشرع الفلسطيني تنص المادة (16) من تعليمات النائب العام الفلسطيني ينبغي أن يكون المحقق كتوماً المجريات التحقيق ضماناً لسيرة في طريقه الطبيعي وتنص المادة (159) إجراءات جزائية فلسطيني: تكون إجراءات التحقيق ونتائجها من الأسرار التي لا يجوز إفشاؤها وتعتبر جريمة يعاقب عليها القانون.

أما عن المشرع الأردني نصت المادة (53) من قانون اصول المحاكمات الجزائية على : ".. بقى التحقيق سريا ما لم تحل الدعوى على قضاء الحكم...."

سادساً: حياد المحقق

يعد حياد المحققين من أهم الضمانات وأكثرها خطورة؛ إذ تشكل ركيزة أساسية لتكوين المحقق الجنائي موقفاً عقلياً ونفسياً يتحتم على المحقق الالتزام به فهو ضروي لتحقيق رسالة هذا التحقيق المتمثلة في المواءمة بين الضرورة الاجتماعية لضمان عقاب عادل للجرائم وبين المحافظة على مصالح وحريات المتهم، وهي في ظاهرها مسائل متعارضه في حقيقتها متوافقة غير أنه

---

[166] الأحمد، أحمد. المتهم ضماناته وحقوقه في الاستجواب والتوقيف "الحبس الاحتياطي" في قانون الإجراءات الجزائية الفلسطيني "دراسة مقارنة"، رسالة ماجستير–جامعة النجاح الوطنية، فلسطين،2008، ص28.

[167] قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950، المادة 75، وفق آخر التعديلات عام 2020.

[168] سالم، عمر محمد. الوجيز في شرح قانون الإجراءات الجنائية، الجزء1، مركز جامعة القاهرة للتعليم المفتوح، 2007، ص 185

لا يستطيع ان يقوم بها من يفتقد الحيادية وذلك لأن القانون يكفلهُ بقيامه بدور الاتهام بالنسبة للمتهم فالحياد يعني عدم التحيز لاي من أطراف الدعوى إنما التحري للحق اينما كان[169] .

ومن هذا المنطلق نستطيع القول إنه لتحقيق أقصى ضمانات العدالة من الضروري الفصل بين سلطتي الاتهام والتحقيق، فيُسند التحقيق إلى سلطة قضاء التحقيق ويكون الاتهام من سلطة النيابة العامة، غير أن المشرع المصري لم يقر ذلك[170].

المطلب الثاني: الإشكاليات العملية للتحقيق الابتدائي

أولا: الخصوصية باعتبارها من أهم التحديات التي يوجهها التحقيق الإلكتروني

تجدر الإشارة إلى أن الخصوصية هي واحدة من أهم التحديات التي تواجه المحققين في الجرائم الالكترونية ولا يمكن بأي حال من الأحوال التغاضي عنها، أو إغفال خصوصية المتهم، ففي ظل نمو ملحوظ لتكنولوجيا المعلومات في الآونة الأخيرة، وضرورتها في حياة المجتمعات الديمقراطية يواجه المشرع وصانع القرار إشكالية الحفاظ على قيم المجتمع، وعلى حق مالك الحاسوب في الخصوصية، وحقه في سرية معلوماته الشخصية الموجودة عليه، وعدم خرقها بل وحمايتها وترتيباً على ما سبق فإن المحقق كثيراً ما يواجه أثناء بعض التحقيقات في الجرائم الالكترونية عدة عراقيل، تقف عقبة أمامه خاصة مع التزامه بالنصوص القانونية المتعلقة باحترام الحق في الخصوصية، والتي تختلف من دولة إلى أخرى.

وتجدر الإشارة أيضاً إلى أن نطاق الخصوصية بدأ في الانحسار خاصة في ظل التقدم التكنولوجي والحماية الأمنية، بالرغم من أن اتفاقية بودابست قد ألزمت الدول الأطراف على تطبيق النصوص الإجرائية المتعلقة بالتحقيق في الجريمة الالكترونية وجمع أدلتها بمراعاة حقوق الإنسان واحترام الحريات العامة، كما أن الاتفاقية أيضاً ألزمت دول الأعضاء بوضع التشريعات والنصوص التي تمكن السلطات المختصة من أن تطلب من المشترك تسليم معلومته الرقمية الضرورية التي يحوزها في جهاز الكمبيوتر الخاص به، وأي من أدوات تخزين

---

[169] نجم، محمد صبحي."الوجيز في قانون أصول المحاكمات الجزائية"، دار الثقافة للنشر والتوزيع، عمان، 2012، ص22.

[170] عبد الرؤوف مهدي. "شرح القواعد العامة للإجراءات الجنائية"، دار النهضة العربية، سنة 2017، ص 298

المعلومات وأيضاً وضع التشريعات اللازمة لكي تطلب السلطات المختصة من مزود الخدمة تقديم معلومات مشتركيها مثل: نوع الخدمة المقدمة له ومدة اشتراكه وهويته وعنوانه وقم هاتفه وغيرها من المعلومات الخاصة واللازمة للتحقيق في الجريمة الالكترونية [171].

ثانياً: المشكلات المتعلقة بجرائم الاعتداء على الحياة الخاصة للأفراد

إن الهدف الأساسي من تناول هذا الموضوع التعرض لتلك الجرائم التي يتعذر علينا مواجهتها بالنصوص التقليدية، ففي الأردن لا يوجد هناك قوانين خاصة لحماية الحياة الخاصة، وإنما هناك مجموعة من النصوص القانونية المتناثرة التي تنتشر في قانون العقوبات وقانون أصول المحاكمات الجزائية، ففي قانون العقوبات رقم (16) لسنة 1960م وتعديلاته، ورد بنص المادة (355) عقوبة من يقوم بإفشاء أسرار تحصل عليها بحكم وظيفته أو إبقاءها في حيازته بعد انتهاء عمله، ثم قام بإفشائها، وكذلك ورد بنص المادة (356) من قانون العقوبات لعام 1960، عقوبة من كان يعمل بمصلحة البرق والبريد ويقوم بالاطلاع على الرسائل والاستماع إلى المحادثات الهاتفية. وفي قانون أصول المحاكمات الجزائية الأردني رقم (9) لسنة 1961م وتعديلاته وردت عدة طرق قانونية تنظم عملية إلقاء القبض على المتهم وتفتيش بيته أو تفتيشه شخصياً واستجوابه بهدف عدم المساس بحريته الشخصية وحياته الخاصة المادة 348 مكررة.

إلا أنه وبعد أن أصدر المشرع الأردني قانون جرائم أنظمة المعلومات المؤقت رقم (17) لسنة 2023م، فقد أورد جرائم إلكترونية تتعلق بالخصوصية وبشكل خاص بالنسبة للشخصيات العامة أو البيانات المتصلة بالحياة الخاصة وتشمل جرائم الاعتداء على المعطيات السرية أو الخاصة، وجرائم الاعتداء على البيانات الشخصية المتعلقة بالحياة الخاصة.

[171] مرعي، جمال. 2022، منشورات موقع حماه الحق، https://jordan-lawyer.com/2021/10/15/cyber-crime-investigation/

الخـــــاتمة

بات من الواضح تماماً المكانة الكبيرة والركيزة الأساسية التي أصبحت تحتلها الوسائل التكنولوجية وشبكات الانترنت ووسائل الاتصال الحديثة، في حياة الأشخاص داخل أي مجتمع من المجتمعات؛ نظرا لما حققاه من نقلة نوعية في حياة البشرية قاطبة، وما يقدمانه من خدمات، ناهيك عن السرعة والسهولة في التعامل بتلك التقنيات الحديثة، مما يجعل الشخص يسارع لاستخدامها بهدف توفير الوقت والجهد من جهة، ناهيك عما توفره هذه التقنيات من خصوصية يفترض أن يتمتع بها كل ما يلجأ للعالم الافتراضي في أي مجال من مجالات الحياة.

ولكن اللافت للنظر لدى الجميع أيضاً، أنه وعلى الرغم من الإيجابيات الكثيرة التي توفرها البيئة الافتراضية والتقدم التقني والتكنولوجي، ووسائل الاتصال والتواصل الحديثة، إلاّ أنها أصبحت تشكل مجالاً خصبا لارتكاب الأفعال الغير مشروعة، فيما بات يعرف بالجرائم الالكترونية.

الأمر الذي استدعى وبالضرورة، التدخل السريع من طرف المشرع في أي بلد لتطوير مجموعة من القوانين لمكافحة هذا النوع من الظواهر الإجرامية الحديثة، حيث أنها باتت تشكله من خطورة حقيقية تهدد حقوق الأفراد المادية والمعنوية، وما قد يترتب عليها من أضرار وخيمة يكون كل مستخدم لشبكات الانترنت ووسائل التواصل الحديثة معرضاً لها في أي وقت وبأي مكان.

النتائج:

وبناءً على ما سلف ذكره وشرحه، توصل الباحث في دراسته إلى مجموعة من النتائج أهمها:

1- باتت الجرائم الالكترونية تحتل ذات الخطورة التي تشكلها الجرائم التقليدية، بل وتفوقها في بعض الحالات.
2- يعاني التحقيق في الجرائم الإلكترونية بفلسطين من تدني مستوى أداء قسم التحقيق ممثلاً بوحدة الجرائم الالكترونية وأجهزة الشرطة المسؤولة، وذلك لغياب التدريب والتأهيل التقني والعلمي اللازم لمكافحة مثل هذه الجرائم.
3- لم يتطرق التشريع الفلسطيني لحماية الحق في الخصوصية في القوانين ذات العلاقة بالتحقيق في الجرائم الالكترونية. -في العمل القضائي الفلسطيني، لا تزال الأدلة الرقمية غريبة عن النظام القانوني الفلسطيني، وبالتالي غير معمول بها بشكل جدي حتى الآن، وذلك عائدٌ لكون أن القوانين الساري نفاذها في فلسطين لم تتطرق بشكل صريح وواضح لحجية الدليل الرقمي، ولم تأخذ به على سبيل الإلزام على الرغم من طبيعته العلمية والتقنية التي تعطيه مصداقية أكبر وأدق وتتلاءم وطبيعة الجريمة الالكترونية.
4- هناك نقص كبير في الكادر المؤهل من خبراء التحقيق الإلكتروني في فلسطين، لاسيما على مستوى مأموري الضبط القضائي الذين يضبطون أجهزة الكمبيوتر وأهزة الهاتف التي ارتكبت بواسطتها الجريمة الالكترونية. في مسرح الجريمة قبل إحالتها إلى الفرق المتخصصة في مراكز الشرطة.

بعد عرض النتائج المستخلصة من الدراسة، يوصي الباحث بما يلي:

1- ضرورة تحديث نصوص قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001، بما يتلاءم وخصوصية التحقيق الابتدائي في الجرائم الالكترونية، من حيث إجراءات التفتيش لتتلاءم وطبيعة الجريمة الالكترونية وأدوات ارتكابها، وطبيعة أدلة هذه الجرائم.
2- تقديم التدريب التكنولوجي المستمر لأعضاء وحدة الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، وكذلك القضاة المختصون وأفراد الشرطة، بالشكل الذي يجعلها

دائمة الاطلاع على مستجدات المجال التقني والتكنولوجي، للمساعدة في تحقيقاتها حول الجرائم الالكترونية.

3- إفراد نصوص قانونية في القرار بقانون رقم 10 لسنة 2018 وتعديله بما يتضمن إعطاء الدليل الرقمي حجية أكبر أمام القضاء الجزائي الفلسطيني.

4- إفراد تنظيم قانوني خاص لمسألة حماية الحق في الخصوصية على مستوى التشريع الفلسطيني، لاسيما إذا ما أخذنا بعين الاعتبار غياب هذا المضمون عن القرار بقانون رقم 10 لسنة 2018.

5- تعديل قانون الاجراءات الجزائية الفلسطيني من خلال تضمينه قواعد للتحقيق في الجرائم الإلكترونية، والتفتيش في أجهزة الكمبيوتر وأجهزة الاتصال الذكية بما يضمن فعالية ضبط وتحريز الأدلة الرقمية.

6- على مستوى مذكرات التفتيش الإلكتروني يجب تضمين نص القرار بقانون تعديلاً يتضمن تحديد نوع الملف المراد التفتيش فيه، أو اسم الملف، أو اسم البرنامج وذلك لحماية خصوصية الشخص المراد تفتيش الأجهزة الإلكترونية التي تعود ملكيتها لهذا الشخص، وكذلك تحديد نوع الأدلة المراد تفتيشها ونطاق التفتيش، كأن يتعلق بملفات صور، أو فيديوهات، أو رسائل، وليس كل محتويات المضبوط.

المصادر والمراجع

❖ قوانين

- قانون العقوبات رقم (16) لسنة 1960.
- قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001، وتعديلاته، منشور في جريدة الوقائع الفلسطينية – العدد 38، سبتمبر 2001، ص 94-225.
- القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية، منشور في جريدة الوقائع الفلسطينية – العدد 16، 2018/5/3، ص 8-24.
- قانون الجرائم الالكترونية الأردني رقم (17) لسنة 2023، منشور في الجريدة الرسمية رقم (5874)، ص 3579- 3598، منشور بتاريخ 2023/8/13.
- قانون رقم (175) لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، المصري، منشور في الجريدة الرسمية العدد 32 مكرر (ج) بتاريخ 2023/08/14.
- قانون البينات الفلسطيني رقم 4 لسنة 2001، منشور في جريدة الوقائع الفلسطينية – العدد 38، سبتمبر 2001، ص 226- 278.

❖ معاجم

- أنيس وآخرون، إبراهيم. 1973. المعجم الوسيط، ط1، دار المعارف، ج2، القاهرة.
- ابن منظور، لسان العرب، ط1، دار المعارف، ج4، القاهرة.

❖ الكتب

- إبراهيم خالد ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي – الإسكندرية، الطبعة الأولى، السنة 2009.
- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، الطبعة الثانية 2006.

- المضحكي، حنان ريحان مبارك، الجرائم المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، ط1، 2014.

- بن سليمان، عبد السلام. الإجرام المعلوماتي في التشريع المغربي: دراسة نقدية مقارنة في ضوء أداء الفقه وأحكام القضاء، ط1. دار الأمان. الرباط. المغرب، 2017.
- الجبور، محمد. (2012)، الوسيط في قانون العقوبات _ القسم العام، ط1، دار وائل، الأردن.
- حجازي، عبد الفتاح، الجوانب الإجرائية لأعمال التحقيق، دار النهضة العربية، القاهرة ط1.
- الحلبي، خالد عياد. (2011)، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع، الأردن.
- حنفي، حازم محمد. (2017)، الدليل الإلكتروني ودوره في المجال الجنائي، ط1، دار النهضة العربية
- خالد ممدوح إبراهيم.2009، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، ط1، الإسكندرية.
- الخيري، غسان، الطب العدلي والتحري الجنائي، دار الراية، الأردن، ط1، 2013.
- سالم، عمر محمد. (2007)، الوجيز في شرح قانون الإجراءات الجنائية، الجزء1، مركز جامعة القاهرة للتعليم المفتوح.

- شمسان الجيلي، الجرائم المستحدثة بطرق غير مشروعة لشبكة الإنترنت، دار النهضة العربية – القاهرة، السنة 2009.
- عبد الباقي مصطفى، شرح قانون الإجراءات الجزائية الفلسطيني (دراسة مقارنة)، وحدة البحث العلمي والنشر – جامعة بيرزيت، السنة.
- عبد الحميد، عائشة. 2022. الإطار القانوني والإجرائي للجنوح السيبراني للأطفال في ظل القانون رقم 15-12 في الجزائر.

- العزام، سهيل محمد. 2009. الوجيز في جرائم الإنترنت، ط1، المكتبة الوطنية، الأردن.
- مركز هردو لدعم التعبير الرقمي، التنظيم القانوني والجرائم الالكترونية ما بين أمن المعلومات وتقييد الحريات، القاهرة، مصر، 2018.
- المليح، عبد الله. (2015)، صحّة الإجراءات الجزائية وأثرها في مواجهة الجريمة، أكاديمية شرطة دبي، الإمارات.
- المومني عبد القادر، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع – عمان – الأردن، الطبعة الأولى، السنة 2012.
- نجم، محمد صبحي. (2012)"الوجيز في قانون أصول المحاكمات الجزائية"، دار الثقافة للنشر والتوزيع، عمان.
- عبد الرءوف مهدي. (2017). شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، مصر.
- محمود القرعان، الجرائم الالكترونية، دار وائل للنشر والتوزيع، الطبعة الأولى، الأردن، 2017.
- هروال، نبيلة. (2007). الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات :دراسة مقارنة، ط1، دار الفكر الجامعي، مصر.
- هشام رستم. (1992). قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة – مصر.
- يوسف، أمير فرج. (2016)، الإثبات الجنائي للجريمة الالكترونية والاختصاص القضائي بها، ط1، مكتبة الوفاء القانونية، مصر.
- مركز هردو لدعم التعبير الرقمي، التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات، القاهرة، مصر، 2018.

❖ **رسائل الماجستير والدكتوراة**

- الأحمد، أحمد. (2008). المتهم ضماناته وحقوقه في الاستجواب والتوقيف "الحبس الاحتياطي" في قانون الإجراءات الجزائية الفلسطيني "دراسة مقارنة"، رسالة ماجستير-جامعة النجاح الوطنية، فلسطين.
- أسامة مهمل، الإجرام السيبراني، رسالة ماجستير، كلية الحقوق والعلوم السياسية – جامعة بوضياف/الجزائر، 2017-2018.
- بخي، فاطمة الزهراء. 2014. إجراءات التحقيق في الجريمة الالكترونية، رسالة ماجستير: كلية الحقوق والعلوم السياسية-جامعة المسيلة.
- بنار، مراد. (2018). الجرائم المرتكبة عبر الوسائط الالكترونية، رسالة ماجستير – جامعة القاضي عياض، المغرب.
- بني فضل، علاء. (2011)، ضمانات المتهم أمام المحكمة الجنائية الدولية، رسالة ماجستير-جامعة النجاح الوطنية، فلسطين.
- ثنيان ناصر آل ثنيان. 2012. إثبات الجريمة الالكترونية: دراسة تأصيلية تطبيقية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، السعودية، ص108.
- سعيداني، نعيم. (2013)، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير-جامعة الحاج لخضر – باتنة -، كلية الحقوق والعلوم السياسية، الجزائر.
- الشعار، خالد. بدون سنة نشر. التحقيق الجنائي في الجرائم الالكترونية. بحث مقدم لاستيفاء متطلبات الحصول على درجة الدكتوراة في الحقوق، جامعة المنصورة.
- الشقيرات، رزق الله. (2009)، الصعوبات الناشئة في تطبيق أحكام جرائم الذم والقدح والتحقير عبر شبكة الإنترنت: دراسة مقارنة، رسالة ماجستير-جامعة عمان العربية، الأردن.
- صغير يوسف، الجريمة المرتكبة عبر الأنترنيت، مذكرة ماجستير في قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.

- طاهري، عبد المطلب. (2015)، الإثبات الجنائي بالأدلة الرقمية، رسالة ماجستير- جامعة المسيلة، الجزائر.
- العجمي، عبد الله.2014. المشكلات العلمية والقانونية للجرائم الالكترونية دراسة مقارنة، رسالة ماجستير-جامعة الشرق الأوسط، الأردن.
- فرغلي والمسماري، عبد الناصر ومحمد. 2007، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، جامعة نايف العربية للعلوم الأمنية، الرياض،2007.
- الكبيجي بهاء، مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة، رسالة ماجستير في القانون العام، جامعة الشرق الأوسط، السنة 2013.
- ميرغني، فيروز.2017. إجراءات التحري والضبط في الجريمة الالكترونية، أطروحة دكتوراه-جامعة شندي، السودان.

❖ **الدوريات**

- البشري، محمد الأمين. (2002)، الأدلة الجنائية الرقمية، مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، السعودية.
- الجسمي، خالد مصطفى.(2017)، الإثبات الجنائي بالأدلة الرقمية، مجلة القانون المغربي، دار السلام للطباعة والنشر، المغرب، ع34.
- الحوامدة، لورنس. (2021)، حجية الأدلة الرقمية في الإثبات الجنائي: دراسة تحليلية مقارنة، مجلة البحوث الفقهية والقانونية، العدد36، المملكة العربية السعودية.
- عبد الباقي، مصطفى. 2018. التحقيق في الجريمة الالكترونية وإثباتها في فلسطين: دراسة مقارنة، جامعة بيرزيت: دراسات علوم الشريعة والقانون، المجلد 45، عدد 4، ملحق 2.
- عثماني، عز الدين. 2018. إجراءات التحقيق والتفتيش في الجرائم الماسة أبنظمة الاتصال والمعلوماتية، دائرة البحوث والدراسات القانونية والسياسية - مخبر المؤسسات الدستورية والنظم السياسية (العدد الرابع – جانفي)، جامعة المسيلة، الجزائر.

- عطايا، ابراهيم. 2015. الجريمة الالكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية، العدد 30، الجزء الثاني.
- فاطمة زهرة بوعناد، "مكافحة الجريمة الالكترونية في التشريع الجزائري، " مجلة الندوة للدراسات القانونية، العدد الأول، (دون دار نشر)، الجزائر، 2013.
- معاشي، سميرة. (2011)، ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد 7، جامعة خيضرة بسكرة، الجزائر.
- النوازلي، إدريس. (2010)، موقف القضاء من الجريمة الالكترونية، مقال منشور بمنشورات كلية العلوم القانونية والاقتصادية والاجتماعية، مراكش، سلسلة الندوات والأيام الدراسية، المغرب.
- الحجار وبشير، عدنان وفايز (2021)، الأدلة الرقمية وإثبات الجرائم السيبرانية ما بين التأصيل والتأويل، مجلة جامعة الاستقلال للأبحاث، المجلد 6، العدد 1.

❖ **الندوات**

- بورشاق، زغودة. 2022. أسباب الجريمة الالكترونية من منظور سوسيو انثروبولوجي، جامعة المدية الجزائر، المؤتمر الدولي العلمي الافتراضي، برلين.
- بومدين وبن مزيان، إيمان وحنان. (2022). الجريمة الالكترونية بين دوافع ارتكابها واليات مواجهتها: الإستراتيجية الإمنية للدولة الجزائرية في مكافحة الجرائم الالكترونية أنموذج، المؤتمر الدولي العلمي الافتراضي.
- سلام، كرم سلام. (2022)، الجرائم الالكترونية في الفقه الإسلامي والقانون الوضعي، المؤتمر الدولي العلمي الافتراضي، برلين.

❖ **مراجع إلكترونية**

- طيب، ميرفت محمود. "الجريمة الالكترونية وأنواعها وأشكالها وأدواتها ودوافعها وطرق مكافحتها والعقوبات القانونية لها"، 2017، المصدر: جريدة وموقع غرب garbnews.net تاريخ نشرها، 2017/11/12، 8:56.
- شاهين، حسن. 2022. الجرائم الالكترونية في التشريع الفلسطيني، وكالة وطن للأنباء https://www.wattan.net/ar/news/370729.html
- مرعي، جمال. 2022، منشورات موقع حماه الحق، https://jordan-lawyer.com/2021/10/15/cyber-crime-investigation/
- حماة الحق - محامي الأردن، حجية الدليل الإلكتروني في القضايا الجزائية، https://jordan-lawyer.com/2021/11/02/authentic-electronic-evidence-in-criminal-cases/
- عقيدة، محمد أبو العلا، التحقيق وجمع الأدلة في مجال الجرائم الالكترونية، https://www.bibliotdroit.com/2021/12/blog-post_77.html

Abstract

Technological progress and clear development at the level of information and communication technology is one of the most important phenomena that have become of special interest in the daily life of people within any society, and Palestinian society is not far from this situation. Like other societies, the circle of daily use of the Internet has expanded as it is a means of communication in various aspects of life.

However, the many positives that information technology and the virtual world provide to people in any society have in turn led to many risks and resulted in new types of crimes, in what has become known as electronic crimes, and the latter have varied and multiplied in their forms and forms.

Investigating these electronic crimes and how to seize evidence that proves the commission of a criminal act is one of the recent and emerging issues in the Palestinian judiciary, especially if we take into consideration the first special legal regulation for this type of crime on the level of Palestine came in 2018.

The authority to investigate this type of crime is assumed by a special unit called the Electronic Crimes and Crimes Unit. Communications and Information Technology", all in accordance with special rules and procedures that distinguish the primary investigation of electronic crimes from the investigation of traditional crimes. These crimes are of modern methods and means that help in committing them, which necessitated confronting them with special procedures and means of proof, and undertaking the task of investigating them through specialized agencies.

Keywords: cybercrime, investigation of cybercrime, digital evidence.