جـامعـــة النجاح الوطنية

كليـــة الدراســـات العليـــا

التفتيش في الجرائم الإلكترونية: دراسة تحليلية مقارنة

إعداد

نادين محمود محمد الشايب

إشراف

د. أحمد برّاك

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون العام، من كلية الدراسات العليا، في جامعة النجاح الوطنية، نابلس- فلسطين.

2023

التفتيش في الجرائم الإلكترونية: دراسة تحليلية مقارنة

إعداد

نادين محمود محمد الشايب

نوقشت هذه الرسالة بتاريخ 2023/2/19 م، وأجيزت:

د. أحمد برّاك	
المشرف الرئيسي	التوقيع
د. مصطفى عبد الباقي	
الممتحن الخارجي	التوقيع
د. نور عدس	
الممتحن الداخلي	التوقيع

الاهداء

أهدي هذا العمل المتواضع إلى نفسي أولاً...

وإلى كل من زرع الشوك في طريق دراستي وإلى كل من اعتبرتهم سنداً وعوناً لي ذات يوم... وإلى كل من راهن على فشلي... فلولا وجودكم لما استطعت الوصول إلى هنا ولما أحسست بمتعة النجاح.. لذا أهديكم هذا العمل..

الشكر والتقدير

الشكر والثناء لله عز وجل على نعمة الصبر والقدرة على تحقيق الأهداف وإنجاز هذا العمل...

وأتقدم بالشكر إلى الدكتور أحمد برّاك الذي تفضّل بإشرافه على هذا البحث والدكتورة نور عدس والدكتور مصطفى عبد الباقي على ما قدموه لي من توجيه وإرشاد لإتمام هذا البحث.

الإقرار

أنا الموقع أدناه مقدم الرسالة التي تحمل عنوان:

التفتيش في الجرائم الإلكترونية: دراسة تحليلية مقارنة

أقر بأن ما اشتملت عليه هذه الرسالة هي نتاج جهدي الخاص، باستثناء ما تمت الإشارة اليه حيثما ورد، وأن هذه الرسالة ككل أو أي جزء منها لم يقدم من قبل لنيل أية درجة أو لقب علمي أو بحثي لدى أية مؤسسة تعليمية أو بحثية أخرى.

اسم الطالب: _____

التوقيع: _____

التاريخ: _____

فهرس المحتويات

التفتيش في الجرائم الإلكترونية: دراسة تحليلية مقارنة

اعداد

نادين محمود محمد الشايب

إشراف

د. أحمد برّاك

الملخص

تعد الجرائم الإلكترونية من الجرائم المستحدثة التي تتمتع بخصوصية تقنية مما جعلها تحتاج إلى اتّباع طرق خاصّة للتعامل معها والتنقيب عن أدلتها وجمعها، فجاءت هذه الدراسة لتتناول هذه الجرائم والبحث فيها من ناحية كيفية إجراء التفتيش عليها، فإجراء التفتيش بشكلٍ عام هو أحد إجراءات التحقيق الابتدائي الذي يهدف إلى الكشف عن الحقيقة من خلال البحث والتنقيب عن الأدلة.

وتظهر أهمية هذه الدراسة في الكشف عن كيفية إجراء التفتيش في الجرائم الإلكترونية من قبل الجهات المختصّة التي تتمتع بخبرة تقنية عالية للتعامل مع هذه الجرائم وكذلك إبراز الطرق التي تتبعها في الحصول على الأدلة الناجمة عن هذه الجرائم وضبطها والمحافظة عليها.

وتمثلت إشكالية هذه الدراسة حول فيما إذا استطاع المشرع في القرار بقانون بشأن الجرائم الإلكترونية أن ينظم إجراء التفتيش في الجرائم الإلكترونية بطريقة فاعلة لملاحقة هذه الجرائم، وتمحورت أهداف الدراسة في تبيان المقصود بإجراء التفتيش في الجرائم الإلكترونية وأهم الشروط الواجب توافرها عند إجرائه وكذلك آلية القيام به وكيفية جمع الأدلة وضبطها وحفظها والصعوبات التي يتم مواجهتها أثناء القيام به.

وفي سبيل إجراء هذه الدراسة وتحقيق أهدافها اتبعت الباحثة المنهج الوصف التحليلي المقارن والقائم على تحليل النصوص القانونية المنظمة لإجراء التفتيش في الجرائم الإلكترونية والمقارنة ما بين التشريعين الفلسطيني والمصري وذلك في محاولة لإيجاد أوجه التشابه والاختلاف بينهما.

وتوصلت الدراسة إلى أن إجراء التفتيش في الجرائم الإلكترونية بحاجة إلى المزيد من التنظيم الإجرائي كونه من أهم وأخطر إجراءات التحقيق لما يساعد في الكشف عن الجريمة واثباتها، إذ إن القوانين الموجودة سواء القوانين الإجرائية أو تلك القوانين التي تنظم الجرائم الإلكترونية تعاني من قصور في تنظيم هذا الإجراء.

الكلمات المفتاحية: الجرائم الإلكترونية، التفتيش الإلكتروني، الإثبات الجنائي، الأدلة الإلكترونية.

المقدمة

شهد العالم تطوراً ملحوظاً في المجال التكنولوجي وخاصة في وسائل الاتصال الحديثة المختلفة، وساهمت هذه الوسائل في إحداث ثورة كبيرة أطلق عليها مسمى الثورة المعلوماتية وذلك نتيجة الاستخدام الواسع لهذه الوسائل فلم تعد مقصورةً على فئات معينة بل أصبحت جميع فئات المجتمع تستخدم هذه الوسائل، ونتيجةً لهذا التوسع الكبير ظهرت لنا جرائم مستحدثة بسبب قيام بعض الفئات بإساءة استخدام هذه الوسائل كارتكاب أفعال مجرمة عن طريق شبكات الانترنت[1].

ونظراً لازدياد هذه الجرائم المستحدثة في العالم–والتي أطلق عليها عدة مسميات كالجرائم المعلوماتية والجرائم الإلكترونية– تضافرت الجهود الدولية ووضعت اتفاقية بودابست لعام 2001 والتي تضمنت مجموعة من المبادئ العامة التي تتعلق بالتعاون الدولي في مكافحة الجرائم الإلكترونية[2]، كما وتم إبرام الاتفاقية العربية والتي جاءت بعنوان الاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات، وشرعت بعض الدول إلى إصدار تشريعات جنائية لمواجهة هذه الجرائم والبعض الآخر سعى إلى القيام بتعديلات على تشريعاتها القائمة بما يتناسب مع هذه الجرائم من تجريمها وملاحقتها ووضع العقوبات المناسبة لها.

وتعد فلسطين من الدول التي عملت على إصدار تشريع جنائي لمواجهة هذه الجرائم فقامت بإصدار القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتضمن هذا القرار بقانون أحكاماً تنظم أنواع هذه الجرائم وكيفية الحد منها ومتابعتها وملاحقة مرتكبيها ومعاقبتهم وكذلك الإجراءات التي تتبع في مثل هذه الجرائم كون أنه من الصعب تطبيق النصوص التقليدية على مثل هذه الجرائم وخاصة النصوص التقليدية المتعلقة بإجراء التفتيش والواردة في قانون الإجراءات الجزائية، فالجرائم الإلكترونية أكثر حساسة من الجرائم التقليدية العادية حيث يتم التعامل فيها مع معلومات وأدلة

[1] إبراهيم، خالد ممدوح: **الجرائم المعلوماتية**، الطبعة الثانية، الاسكندرية – مصر: دار الفكر الجامعي، 2019، ص 5.

[2] الديربي، عبد العال وإسماعيل، محمد صادق: **الجرائم الإلكترونية دراسة قضائية مقارنة**، الطبعة الأولى، القاهرة – مصر: المركز القومي للإصدارات القانونية، 2012، ص 8.

معنوية وبالتالي حتى يتم كشفها وإجراء التفتيش فيها وإثباتها لا بد من استخدام إجراءات وطرق وتقنيات حديثة خاصّة بها تختلف عن الإجراءات العادية.

وفي الحقيقة إن الجريمة الإلكترونية أو الجريمة المعلوماتية تضم أشكالاً وأنماطاً مختلفة من الأفعال الإجرامية، وكما أي جريمة فإنه عند حدوثها واكتشافها تقوم السلطات المختصة باتخاذ عدة إجراءات فتبدأ بإجراء البحث والتحري عنها وجمع المعلومات عنها وعن مرتكبها حتى يتسنى إقامة دعوى جزائية ضد مرتكبها ومعاقبته على أفعاله المجرمة وتمر هذه الدعوى بمرحلتي التحقيق الابتدائي والتحقيق النهائي (المحاكمة)، وتعد مرحلة التحقيق الابتدائي أخطر هذه المراحل إذ يتم فيها اتخاذ إجراءات مختلفة منها ما يهدف إلى الإمساك بالمتهم بارتكاب الجريمة كإجراء القبض عليه، ومنها ما هو يهدف إلى جمع الأدلة حول الجريمة ومن ثم التوصل إلى الحقيقة كإجراء الاستجواب و إجراء التفتيش، ويتعرض الفرد في مرحلة التحقيق الابتدائي إلى العديد من الإجراءات التي قد تمس بحريته المكفولة بالدستور ولعل أهم هذه الإجراءات وأكثرها خطورة إجراء التفتيش كونه إجراء يقوم بالبحث والتنقيب عن الأدلة في مستودع السر، ولأن إجراء التفتيش قائم على تماس مباشر مع حقوق الفرد وحرياته التي كفلها له الدستور تم تنظيم أحكامه ووضع قيود وضوابط عليه من شأنها أن تؤدي إلى خلق توازن بين مصلحة المجتمع في معاقبة المتهم من جهة ومصلحة الفرد وحماية حقوقه وحرياته من جهة أخرى[1].

أهمية الدراسة

تعد الجرائم الإلكترونية من قبيل الجرائم المستجدة والحديثة في المجتمع والتي ظهرت نتيجة التطور والتقدم التكنولوجي الحاصل في العالم والانتشار الواسع لاستخدام الأجهزة الإلكترونية، لهذا فإن طبيعة الجرائم الإلكترونية ومحلها تختلف عن الجرائم العادية مما جعلها محطّ أنظار سواء من قبل الدول لوضع التشريعات الجنائية لتنظيم أحكامها أو من قبل فقهاء القانون الجنائي للبحث فيها وتناولها في كتبهم

[1] الطوالبة، علي حسن محمد: **التفتيش الجنائي على نظم الحاسوب والإنترنت**، البحرين: جامعة العلوم التطبيقية، 2010، ص11.

القانونية، ولعل موضوع إجراء التفتيش في الجرائم الإلكترونية والصعوبات المصاحبة لهذا الإجراء له أهمية من الناحية النظرية والعملية فمن الناحية النظرية تكمن هذه الأهمية في التعرف على إجراء التفتيش في الجرائم الإلكترونية وأهم القواعد التي يتم اتباعها عند إجرائه وبيان مدى اختلاف طبيعة التفتيش على الدليل الإلكتروني عن طبيعة التفتيش على الدليل المادي، والتعرف على السلطات المختصة بالقيام بهذا الإجراء، أما عن الأهمية العملية كون أن هذه الدراسة جاءت لتبحث في جزئية مهمة وحساسة من موضوع التفتيش ألا وهو إجراء التفتيش على الأجهزة الإلكترونية المختلفة والذي يستهدف أدلة غالباً ما تكون غير محسوسة باعتبارها بيانات ومعلومات لذا فإن الأهمية العملية تكمن في تسليط الضوء حول كيفية تعامل السلطات المختصة بالتفتيش مع هذه الأدلة والمهارات التقنية والفنية التي تستخدمها في سبيل تحصيل الأدلة الإلكترونية ومدى التزامها في إحداث التوازن بين تحقيق المصلحة العامّة وحماية خصوصية وحقوق المتهم.

أهداف الدراسة

تسعى الباحثة من خلال هذه الدراسة إلى تحقيق عدة أهداف والمتمثلة فيما يلي:

1. التعرف على الأحكام الموضوعية المتعلقة بالجرائم الإلكترونية من حيث المقصود بها وأركانها ومحلها.
2. توضيح الآلية المتبعة في إجراء التفتيش في الجرائم الإلكترونية وأهم الشروط الواجب توافرها عند إجرائه.
3. معرفة كيفية ضبط الأدلة والتصرف بها من قبل السلطة المختصة.
4. بيان مدى قوة الدليل الإلكتروني وقيمته في الإثبات الجنائي.
5. إبراز أهم الصعوبات التي تواجه السلطات المختصة عند إجراء التفتيش في الجرائم الإلكترونية.

إشكالية الدراسة

إن إجراءات التحقيق التي تقوم بها السلطات المختصة بما فيها إجراء التفتيش تهدف إلى ملاحقة الجريمة والوصول إلى فاعلها الحقيقي واتخاذ بحقه الإجراءات اللازمة ولكن مع توافر ضمانات قانونية له، وبما أننا أمام جرائم مستحدثة خلت القوانين السارية من نصوص تعالجها خاصة من الناحية الإجرائية كان لا بد من إصدار تشريع يعالج هذه الجريمة استناداً للمبدأ القائل" لا جريمة ولا عقوبة إلا بنص" وهو ما جرى فعلاً وتم إصدار القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات واحتوى على بعض النصوص التي تعالج موضوع الجرائم الإلكترونية من الناحية الإجرائية كنص المادة 52 من القرار بقانون والتي تحدثت عن إجراء التفتيش والآلية المتبعة عند إجرائه على الأجهزة الإلكترونية، ومن هنا ظهرت لدينا إشكالية هذه الدراسة والتي تكمن في هل استطاع المشرع في القرار بقانون بشأن الجرائم الإلكترونية أن ينظم إجراء التفتيش في الجرائم الإلكترونية بطريقة فاعلة لملاحقة هذه الجرائم؟

أسئلة الدراسة

تتفرع عن الإشكالية الرئيسية عدة تساؤلات فرعية والتي تتمثل فيما يلي:

1. هل يعتبر تنظيم إجراء التفتيش في الجرائم الإلكترونية في القرار بقانون كافياً في ظل غياب تنظيمه بنصوص إجرائية في قانون الإجراءات الجزائية؟
2. هل نجح القرار بقانون في عملية تنظيم ضبط الأدلة المتحصلة عن إجراء التفتيش؟ وكيف يتم التغلب على الصعوبات التي قد تحول دون ضبطها؟
3. بما إن الجريمة الإلكترونية هي جريمة عابرة للحدود فكيف يتم التعامل مع مثل هذه الجرائم إذا ما حصلت ؟ وما هي الآلية المتبعة لإجراء التفتيش فيها؟ وهل توفق القرار بقانون في تنظيم ذلك؟ أم جاء قاصراً ولا يلبي هذه الغاية؟

نطاق الدراسة

تناولت هذه الدراسة موضوع الجرائم الإلكترونية وآلية إجراء التفتيش التي تتم فيها وكيفية ضبط الأدلة والتعامل معها والتحفظ عليها وحمايتها من التلف والضياع، وذلك في ضوء القانون الفلسطيني وخاصة القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وبالمقارنة مع القانون المصري، ومع التطرق إلى الاتفاقيات الدولية والإقليمية ذات العلاقة بالجرائم الإلكترونية.

منهجية الدراسة

لغايات الإجابة على محاور الدراسة المختلفة فإن الباحثة اعتمدت في هذه الدراسة المنهج الوصفي التحليلي المقارن، إذ إنها ستستعين بالمراجع القانونية المختلفة التي توصف ظاهرة الجرائم الإلكترونية وتوضحها وتبين ماهيتها، ومن ثم الوقوف على النصوص القانونية في القانون التشريعات الفلسطينية المتعلقة بإجراء التفتيش في الجرائم العادية والجرائم الإلكترونية وتحليلها ومقارنتها مع التشريع المصري وكذلك الاسترشاد والإشارة إلى بعض مواقف القوانين العربية.

الدراسات السابقة

1. **التفتيش عن الدليل في الجرائم المعلوماتية**، للباحث الدكتور أسامة بن غانم العبيدي، المجلة العربية للدراسات الأمنية والتدريب، مجلد 29، العدد 2013/58.

وهدفت هذه الدراسة إلى دراسة موضوع التفتيش عن الدليل المعلوماتي في الجرائم الإلكترونية فتناولت ماهية التفتيش من حيث تعريفه وشروطه وبطلانه، كما وتحدثت عن مدى قابلية مكونات الحاسوب الآلي لإجراء التفتيش عليها، وإجراء التفتيش وكيفية ضبط الدليل والمعيقات التي تقف أمام السلطات المختصة في إجراء ذلك.

2. **التفتيش في الجرائم الإلكترونية في التشريع الفلسطيني، دراسة تحليلية مقارنة بالتشريع العماني،** للباحث الدكتور أحمد حسنية، مركز جيل البحث العلمي، العدد28/سبتمبر/2018.

عمل الباحث في هذه الدراسة على تسليط الضوء على إجراء التفتيش في الجرائم الإلكترونية، كون أن هذا الإجراء هو أخطر إجراءات التحقيق الابتدائي لما له من تأثير على الحقوق والحريات، وتناول في دراسته ماهية التفتيش لنظم الحاسوب الآلي من حيث مفهومه وأنواعه والخصوصية التي يتمتع بها إجراء التفتيش للحاسوب الآلي، كما وتحدث عن إجراء التفتيش في الجرائم الإلكترونية بشكل عام وعن أهم القيود التي تحيط بهذا الإجراء والصعوبات التي تواجه السلطات عند إجرائه.

3. **الجرائم الإلكترونية (التجريم والملاحقة والإثبات)**، للباحث الدكتور عبد اللطيف ربايعة، جامعة النجاح الوطنية، فلسطين، 2016.

عالج الباحث في هذه الدراسة موضوع كيفية مواجهة القانون الجنائي الفلسطيني للجرائم الإلكترونية، فهدفت الدراسة إلى التعريف بالجرائم الإلكترونية وتبيان خصائصها ومحلها، وكيفية ملاحقتها ومتابعتها عند حدوثها وكذلك إثباتها، والإجراءات المتبعة في التحري والتفتيش والضبط فيها، وطالب في دراسته بضرورة إقرار قانون من شأنه معالجة الجرائم الإلكترونية من حيث التجريم ووجود قواعد إجرائية يتم اتباعها عند حدوث مثل هذه الجرائم.

4. **الجرائم الإلكترونية في التشريع الفلسطيني، دراسة تحليلية مقارنة،** للباحث يوسف خليل يوسف العفيفي، الجامعة الإسلامية، غزة – فلسطين، 2013.

تناول الباحث في دراسته الجريمة الإلكترونية من حيث مفهومها وطبيعتها القانونية والقواعد الموضوعية لهذه الجرائم وهي أركان الجريمة الإلكترونية، كما وتطرق في دراسته إلى القواعد الإجرائية للجرائم الإلكترونية فتحدث عن الجريمة الإلكترونية منذ لحظة اكتشافها والبدء بالتحري والاستدلال عنها، والمراحل

التي تمر فيها بعد ذلك وهي مرحلة إجراء التحقيق الابتدائي ومرحلة التحقيق النهائي والإجراءات التي يتم اتباعها في هاتين المرحلتين.

5. **وسائل البحث والتحري عن الجرائم الإلكترونية**، للباحث أدهم باسم نمر بغدادي، جامعة النجاح الوطنية، فلسطين، 2018.

جاءت هذه الدراسة لتتناول موضوع الوسائل التي يتم اتباعها من قبل السلطات المختصة في عمليات البحث والتحري عن الجرائم الإلكترونية، وذلك في ظل غياب تشريع خاص بهذه الجرائم وعجز التشريعات التقليدية على مواجهتها، وتحدث في دراسته حول الجرائم الإلكترونية من حيث تعريفها وخصائصها وأركانها، ثم تطرق إلى وسائل البحث والتحري في هذه الجرائم وكيفية إجراء التحقيق فيها بما فيه إجراء التفتيش والضبط وكذلك آليات التحقيق في الجرائم الإلكترونية والواردة في الاتفاقيات الدولية.

إن الدراسات السابقة وغيرها من الدراسات جاءت تعالج موضوع الجرائم الإلكترونية من الناحية الموضوعية من حيث مفهومها وخصائصها وأركانها ومحلها، وكذلك من الناحية الإجرائية من حيث إجراءات البحث والتحري والتحقيق الابتدائي والنهائي، ومعظم هذه الدراسات جاءت قبل صدور القرار بقانون بشأن الجرائم الإلكترونية، أي قبل وجود تشريع يجرم وينظم الجرائم الإلكترونية، لذا تختص دراستي بالحديث عن جزئية هامّة في موضوع الجرائم الإلكترونية من الناحية الإجرائية ألا وهي إجراء التفتيش في الجرائم الإلكترونية، حيث سأتحدث حول مدى فعالية القرار بقانون في تنظيمه لموضوع التفتيش في الجرائم الإلكترونية وفيما إذا كان هناك أي اختلاف عن إجراء التفتيش في الجرائم العادية التقليدية، وكيفية إجراء التفتيش والضبط للأدلة المعلوماتية.

خطة الدراسة

ستعتمد الباحثة لإتمام هذه الدراسة وتحقيق الهدف منها إلى تقسيمها على النحو الآتي:

المبحث التمهيدي: مفهوم الجرائم الإلكترونية

المطلب الأول: تعريف الجرائم الإلكترونية

المطلب الثاني: القواعد الموضوعية للجرائم الإلكترونية

الفصل الأول: ماهية التفتيش في الجرائم الإلكترونية

المبحث الأول: تعريف التفتيش في الجرائم الإلكترونية

المبحث الثاني: شروط التفتيش في الجرائم الإلكترونية

الفصل الثاني: كيفية إجراء التفتيش في الجرائم الإلكترونية

المبحث الأول: الآلية المتبعة عند إجراء التفتيش في الجرائم الإلكترونية

المبحث الثاني: ضبط الأدلة المتحصلة عن إجراء التفتيش في الجرائم الإلكترونية

الفصل التمهيدي

مفهوم الجرائم الإلكترونية

شهد العالم تطوراً وتقدماً تكنولوجياً في شتّى مناحي الحياة، وخاصة في وسائل تكنولوجيا المعلومات والتي انتشرت بشكل كبير في الآونة الأخيرة، ونظراً للاستخدام الواسع لهذه الوسائل ظهرت لدينا جرائم جديدة سمّيت بالجرائم الإلكترونية وهي تختلف عن الجرائم التقليدية، وأضحت هذه الجرائم تؤثر بشكل سلبي وخطير على المجتمع، ونتعرف على هذه الجرائم من خلال تقسيم هذا المبحث إلى مطلبين:

المطلب الأول: تعريف الجرائم الإلكترونية.

المطلب الثاني: القواعد الموضوعية للجرائم الإلكترونية.

المطلب الأول: تعريف الجرائم الإلكترونية

تعددت التسميات التي جرى إطلاقها على هذه الجرائم منها الجرائم الإلكترونية والجرائم المعلوماتية، والجريمة السيبرانية وجريمة إساءة استخدام الحاسوب وجرائم التقنية العالمية، ويعود السبب في الجدل حول تسمية هذه الجرائم إلى كونها جرائم حديثة ويختلف النظر إليها من دولة لأخرى بحسب مقدار استخدام هذه الدولة للتكنولوجيا ووسائلها، فهناك دول متقدمة ومتطورة بشكل كبير في مجال استخدامها كالولايات المتحدة الأمريكية ودول أوروبا ودول أقل تقدماً وتطوراً في استخدامها كالدول العربية، وللإحاطة بالمقصود في الجرائم الإلكترونية فإنه سنتحدث في هذا المطلب حول تعريفها تشريعياً وفقهياً.

الفرع الأول: تعريف الجرائم الإلكترونية تشريعياً

نظراً لكون هذه الجرائم جديدة وحديثة فإن مختلف الدول قامت بإصدار قوانين من شأنها تنظيم هذه الجرائم من حيث الأفعال التي تعد مجرّمة والعقوبات التي تترتب عليها، وفلسطين شأنها شأن هذه الدول قامت بإصدار القرار بقانون رقم 10 لسنة 2018 الذي تحدث عن الجرائم الإلكترونية وجرائم الاتصالات

وتكنولوجيا المعلومات وما تعلق بها إلا أنه خلى من تعريف واضح للجرائم الإلكترونية، ولم يكن المشرع الفلسطيني وحده الذي لم يضع تعريفاً واضحاً للجريمة الإلكترونية فالمشرع المصري أيضاً في قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 لم ينص على تعريف واضح للجريمة الإلكترونية، كذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات خلت من أي تعريف للجريمة الإلكترونية وسار على دربها العديد من قوانين الدول العربية مثل القانون الأردني والقانون البحريني.

هناك تشريعات بعض الدول العربية تناولت المقصود بالجريمة الإلكترونية، كالتشريع الكويتي والذي عرّفها بأنها "هي كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون"[1]، وكذلك التشريع السعودي الذي نص على "أنها هي كل فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[2]، وعند النظر في التعاريف السابقة نجد أن كل من المشرع الكويتي والمشرع السعودي قد اعتمدا على معيار وسيلة ارتكاب الجريمة في توضيح مفهوم الجريمة الإلكترونية، وهو معيار منتقد فقهياً إذ لا يمكن الاعتماد عليه لوحده كون أن الجريمة الإلكترونية لا يتم اقترافها باستخدام الحاسوب فقط وإنما يوجد وسائل أخرى غيره، ومن التشريعات العربية أيضاً التي نصّت على تعريف الجريمة الالكترونية التشريع السوري وهو برأيي قد أصاب في تعريفه كونه جمع بين معيار الوسيلة ومعيار محل الجريمة كما أن تعريفه حاول فيه احتواء جميع أنواع الجرائم الالكترونية التي قد يتم ارتكابها حيث قال: "أن الجريمة الالكترونية تعني جريمة ترتكب باستخدام الأجهزة الحاسوبية أو الشبكة أو تقع على المنظومات المعلوماتية أو الشبكة"[3].

[1] مادة 1 من قانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات الكويتي.

[2] مادة 1 من نظام مكافحة الجرائم المعلوماتية السعودي الصادر في العام 2007.

[3] مادة 1 من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري لسنة 2012.

الفرع الثاني: تعريف الجريمة الإلكترونية فقهياً

تولى الفقه مهمة وضع التعريفات المختلفة للجريمة الإلكترونية وأطلق البعض منهم عليها تسمية الجرائم المعلوماتية وكذلك جرائم الكمبيوتر إلا أنه يعاب على هذه التسميات أنها تقتصر على جزئيات معينة كمسمّى جرائم الكمبيوتر فهو يدل على أن الجرائم ترتكب على الكمبيوترات فقط، وهذا غير صحيح إذ إن الجرائم تطال أجهزة أخرى غير الكمبيوتر كأجهزة الاتصالات وغيرها.

وتعددت المفاهيم التي وضعها الفقهاء إذ كل منهم اتجه في تعريفه للجرائم الإلكترونية بحسب الزاوية التي ينظر منها لذلك تنوعت المعايير التي ارتكزوا عليها والتي تمثلت بما يلي:

1. فمنهم من استند في تعريفه على موضوع الجريمة بحيث اعتمد على معيار المعلومات باعتبارها محلاً للجريمة، ومن هذه التعريفات أن الجرائم الإلكترونية تعني: "نشاط موجّه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحوّل عن طريقه"[1]، وكذلك التعريف الصّادر عن مكتب المحاسبة العامة في الولايات المتحدة الأمريكية G.O.A بأنها "الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيداً من الناحية التقنية مثل تعديل الحاسوب"[2].
2. ومنهم من استند إلى أداة أو وسيلة ارتكاب الجريمة وانطلق أصحاب هذا المعيار من أن هذه الجرائم يتم ارتكابها باستخدام الكمبيوتر أي أنه الوسيلة التي تؤدي إلى حدوث الجرائم، لكن برأيي أنه ليس من المنطق أن يقتصر تعريف جرائم بالاستناد إلى الوسيلة لوحدها فالجرائم الإلكترونية لا يتم ارتكابها فقط باستخدام الكمبيوتر وإنما يمكن أن تقع باستخدام وسائل أخرى، ومن الأمثلة على التعاريف التي استندت على الأداة فقط بأن الجرائم الإلكترونية هي" كل فعل إجرامي يستخدم الكمبيوتر في ارتكابه

[1] عيّاد، سامي علي حامد: **الجريمة المعلوماتية واجرام الانترنت** ، الاسكندرية – مصر : دار الفكر الجامعي ، 2007 ، ص 27.

[2] حسنية، أحمد أسامة : *الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية* ، **مجلة جامعة الأزهر** ، غزة–فلسطين ، مج 19 ، 2017 ، ص 5 .

كأداة رئيسية"[1]، أو حسب ما عرّفها الفقيه الألماني تاديمان بأنها: " هي كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي"[2].

3. ومنهم من استند إلى الشخص الفاعل، بحيث يتوافر لدى مرتكب الجريمة المعرفة الفنية في الحاسوب ومكوناته حتى يتسنى له ارتكاب الجريمة، ويرى في ذلك الفقيه David Thompson أن الجريمة الإلكترونية هي" جريمة تتطلب لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية النظام المعلوماتي"[3]، ورأى آخرون بأنها: " أي فعل مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لارتكابه والتحقيق فيه وملاحقته قضائياً"[4]، وتنتقد هذه التعريفات وغيرها ممن يستندون على معيار الفاعل لأنها تركز على فاعل الجريمة والذي يجب أن يكون على دراية ومعرفة بالتقنيات ولكن في الحقيقة ليس شرطاً أن يكون كذلك إذ يمكن لأي شخص عادي أن يقوم بارتكاب جريمة إلكترونية وهو لا يملك أدنى معلومات تقنية كأن يقوم بارتكاب جريمة ابتزاز وتهديد لشخص آخر.

4. هناك من جمع المعايير وحاول وضع تعريفاً جامعاً وأكثر شمولية حتى يتم تفادي الانتقادات الموجهة للمعايير السابقة ومن هذه التعاريف ما وضعه مؤتمر الأمم العاشر لمنع الجريمة ومعاقبة المجرمين وهو: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية والجريمة تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[5]وكذلك التعريف الذي وضع من جانب الفقه المصري وهو أن الجرائم الإلكترونية تعني: كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات ويلحق ضرراً بمكونات الحاسوب وشبكات الاتصال الخاصة به والتي يحميها قانون العقوبات ويفرض لها عقاباً ويكون الهدف من ذلك الاعتداء على الأموال المادية أو

---

[1] فكري، أيمن عبد الله: **الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية**، الرياض – السعودية : مكتبة القانون والاقتصاد، 2014، ص 93.

[2] حجازي، عبدالفتاح بيومي: **مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي**، الطبعة الأولى، الاسكندرية– مصر: دار الفكر الجامعي، 2006، ص24 .

[3] الملط، أحمد خليفة: **الجرائم المعلوماتية "دراسة مقارنة"**، الطبعة الثانية، الاسكندرية– مصر: دار الفكر الجامعي، 2006، ص 86.

[4] حسين، سامي جلال فقي: **التفتيش في الجرائم المعلوماتية " دراسة تحليلية"**، مصر: دار الكتب القانونية، 2011، ص 21.

[5] حسنية، أحمد أسامة: **الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية**، مرجع سابق، ص 7 .

المعنوية[1]، وهناك من حاول وضع تعريف للجريمة الإلكترونية قد يكون أقرب للشمولية والوضوح وهو:" كل فعل أو امتناع عن فعل بشكل عمدي مخالف لأحكام القانون يرتكبه شخص أو أكثر عبر جهاز إلكتروني مما يتسبب هذا الفعل أو الامتناع ضرر للغير يستوجب إيقاع العقوبة المناسبة على الفاعل وتعويض مادي عادل"[2].

في الحقيقة إن عدم وجود تعريف شامل للجريمة الإلكترونية يعود إلى تنوّع واختلاف الجرائم الإلكترونية فهناك جرائم تستهدف البيانات والمعلومات وشبكات الانترنت مثل تزييف البيانات أو محوها، وجرائم أخرى يكون الانترنت والحاسب الآلي هما الوسيلة التي يتم ارتكاب الجرائم من خلالها مثل جرائم التجارة الالكترونية وجرائم التشهير والابتزاز والإرهاب[3]، بالتالي هذه الجرائم في تطور مستمر ويظهر منها أنواع جديدة كلما تقدم الزمن وتطورت الوسائل التكنولوجية لذا من الصعب وضع تعريف ثابت لها ومتفق عليه.

المطلب الثاني: القواعد الموضوعية للجرائم الإلكترونية

حتى نتعرف أكثر حول هذه الجريمة فإنه لا بد من البحث في القواعد الموضوعية التي تقوم عليها الجرائم الإلكترونية، وهي تتمثل في أركان الجرائم الإلكترونية ومحلها.

الفرع الأول: أركان الجرائم الإلكترونية

إنّ الجريمة بشكل عام حتى تقوم لا بد من توافر أركان أساسية لها وهما:1-الرّكن الشرعي ويتمثل بوجود النص القانوني الذي يحدد الفعل المجرّم ويفرض عليه عقوبة،2-الرّكن المادي وهو المظهر الخارجي للجريمة والذي يتمثل في النشاط أو السلوك والنتيجة والعلاقة السببية بينهما،3-الرّكن المعنوي وهو الإرادة

---

[1] العريان، محمد علي: **الجرائم المعلوماتية**، الاسكندرية – مصر: دار الجامعة الجديدة للنشر، 2004، ص 45 .

[2] العفيفي يوسف خليل يوسف: **الجرائم الإلكترونية في التشريع الفلسطيني دراسة تحليلية مقارنة**، رسالة ماجستير، الجامعة الإسلامية: غزة- فلسطين، 2013، ص 13.

[3] برّاك، أحمد وجرادة، عبدالقادر: **الجرائم الإلكترونية في التشريع الفلسطيني "دراسة تحليلية تأصيلية مقارنة"**، رام الله-فلسطين: دار الشروق للنشر والتوزيع ، 2019، ص 33+34.

الخاطئة التي تتمثل في النشاط الصّادر من شخص متمتعاً بالأهلية الجنائية ويكون مسؤولاً عن أعماله[1]، وبالتالي فإن الجريمة الإلكترونية يلزم لها هذه الأركان حتى تكون جريمة قائمة وموجودة.

أولاً: الرّكن الشرعي للجريمة الإلكترونية

ويقوم الرّكن الشرعي على وجود نص قانوني مكتوب يجرّم الفعل المرتكب ويفرض عليه عقوبة مناسبة استناداً لمبدأ الشرعية "لا جريمة ولا عقوبة إلا بنص القانون"، وكذلك على انتفاء قيام سبب من أسباب التبرير والإباحة، إذ يعدّ القانون هو المصدر للتجريم والعقاب فهو يحدد الأفعال التي تعتبر من قبيل الجرائم ويحدد لها عقوبة تلائمها من خلال نصوصه التشريعية.

إن الجرائم الإلكترونية كونها جرائم حديثة في المجتمعات فإن وضع نصوص خاصّة لها وإصدار تشريعات لتنظمها أمراً ليس بالسهل وعلى الرغم من ذلك سعت الدول إلى وضع قوانين لتنظمها مثل فلسطين ومصر التي عملت على إصدار قوانين خاصة تعمل على تنظيم الجرائم الإلكترونية، وهناك دول أخرى قامت بتعديل نصوص قوانينها لتتلائم مع هذه الجرائم وتجرم الأفعال التي تعتبر من قبيل الجرائم الإلكترونية ووضع العقوبات المناسبة لها.

واحتوى كل من القرار بقانون الفلسطيني رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وقانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 على مجموعة من النصوص القانونية منها ما هو موضوعي والتي تبيّن الأفعال التي تشكّل جرائم إلكترونية والعقوبات المناسبة لها، ومنها ما هو إجرائي بحيث تناولت بعض الإجراءات التي يتم اتخاذها عند الكشف عن جريمة إلكترونية وملاحقتها وجمع الأدلة فيها ومن هذه الإجراءات إجراء التفتيش.

[1] الحلبي، محمد علي السالم: **شرح قانون العقوبات– القسم العام–**، عمّان–الأردن: دار الثقافة للنشر والتوزيع، 2011، ص 102.

وتسري أحكام القرار بقانون الفلسطيني على أي من الجرائم المنصوص عليها فيه فيما إذا ارتكبت هذه الجرائم كلياً أو جزئياً داخل فلسطين أو خارجها أو حتى امتد أثرها داخل فلسطين وسواء أكان الفاعل أصليّاً أم شريكاً أم محرضاً أم متدخلاً شريطة أن تكون الجريمة المرتكبة معاقباً عليها خارج فلسطين مع ضرورة المبادئ العامّة الواردة في قانون العقوبات النافذ[1]، أما أحكام القانون المصري مع عدم الإخلال بما ورد في قانون العقوبات المصري في الباب الأول منه[2]فإنه تسري أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها في هذا القانون متى كان الفعل معاقباً عليه في الدول التي وقع فيها تحت أي وصف قانوني[3].

والسؤال هنا ماذا عن حالة ارتكاب جرائم منصوص عليها في قوانين أخرى سواء قانون العقوبات أو غيرها من القوانين الجنائية وتم ارتكاب هذه الجرائم بالاستعانة بوسائل تكنولوجية؟

الإجابة بالطبع حتى لو لم تكن القوانين المتعلقة بالجرائم الإلكترونية قد نصّت عليها فإنه في هذه الحالة تعتبر جريمة قائمة ويتم المعاقبة عليها وذلك سنداً للمادة 65 من القرار بقانون الفلسطيني بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات[4]والمادة 27 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018، **ونرى هنا** أن المشرع حاول اعتبار أن كافة الأفعال المجرمة التي يتم ارتكابها باستخدام الوسائل التكنولوجية حتى لو لم ينص عليها في القوانين المتعلقة بالجرائم الإلكترونية هي تشكّل جرائم طالما تم النص عليها في القوانين النافذة الأخرى.

---

[1] المادة 2 من القرار بقانون الفلسطيني رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] المادة 1 من قانون العقوبات المصري رقم 58 لسنة 1937 والمعدّل لسنة 2021" تسري أحكام هذا القانون على كل من يرتكب في القطر المصري جريمة من الجرائم المنصوص عليها فيه".

[3] المادة 3 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.

[4] كانت تحمل رقم المادة 45 وأصبحت تحمل رقم 65 بموجب القرار بقانون رقم38 لسنة 2021 والذي عدّل القرار بقانون رقم10 لسنة 2018.

ويمكن القول أن النصوص القانونيّة التي تعالج الجرائم الإلكترونية تتصف باتّساع دائرة التجريم لأنها عادةً ما تحوي مصطلحات فضفاضة وواسعة تتناسب مع طبيعة وخصوصية الجريمة الإلكترونية، الأمر الذي يساعد القاضي الجنائي في إعطاءه سلطة يتمكن من خلالها إسقاط القاعدة القانونية على عدد أكبر من الجرائم والتي تتميز بتطورها السريع مع مرور الزمن[1].

ثانياً: الرّكن المادي للجريمة الإلكترونية

ويقصد بالرّكن المادي للجريمة بشكل عام هو المظهر الخارجي للجريمة أي النشاط أو السلوك الجرمي (سواء أكان هذا السلوك إيجابي أو سلبي)[2] الذي يقوم به الجاني ويبرز للعالم الخارجي.

ويختلف الرّكن المادي في الجرائم الإلكترونية عن الجرائم التقليدية العاديّة حيث إن هذه الأخيرة يكون فيها عبارة عن اعتداء على ماديّات محسوسة تظهر للعالم الخارجي[3]، بينما يكون الرّكن المادي في الجرائم الإلكترونية عبارة عن اعتداء على بيانات ومعلومات تكون مخزنة على ذاكرة حاسوب أو أنظمة معلوماتية أو على شبكات أو مواقع إلكترونية...إلخ، بالتالي تعتبر طبيعتها بأنها غير محسوسة أو ملموسة.

ويتكون الرّكن المادي في الجريمة الإلكترونية من ثلاثة عناصر وهي أ-السلوك الجرمي ب- النتيجة الجرمية ج- العلاقة السببية[4].

---

[1] المصري، نداء نائل فايز: **خصوصية الجرائم المعلوماتية**، رسالة ماجستير، جامعة النجاح الوطنية، نابلس-فلسطين، 2017، ص 13.

[2] عبد الستّار، فوزية: **شرح قانون العقوبات القسم العام**، القاهرة-مصر: دار النهضة العربية، 1987، ص23.

[3] العجمي، عبدالله دغش: **المشكلات العملية والقانونية للجرائم الإلكترونية**، رسالة ماجستير، جامعة الشرق الأوسط، عمّان-الأردن ، 2014، ص26.

[4] نجم، محمد صبحي: **قانون العقوبات القسم العام النظرية العامة للجريمة**، الطبعة الخامسة، عمّان-الأردن: دار الثقافة للنشر والتوزيع، 2014، ص208.

أ. السلوك الجرمي: وهو القيام بفعل أو الامتناع عن القيام بفعل وهو الذي يبرز الجريمة إلى حيّز الوجود، إذ يشكّل السلوك الإنساني الإرادي المحظور والمجرّم[1]، ويمثل السلوك الجرمي القاسم المشترك بين جميع أنواع الجرائم إذ لا يمكن تصوّر قيام جريمة دون وجود السلوك الجرمي، لذلك يعتبر السلوك الجرمي أهم عناصر الركن المادي[2].

ويتمثل السلوك الجرمي في الجرائم الإلكترونية بأنه يكون نشاط تقني بحيث يتم استخدام الوسائل التكنولوجية المختلفة كالحاسوب وشبكة الإنترنت لارتكاب هذه الجرائم وبالتالي يجب توافر بيئة رقمية واتصال في شبكة الإنترنت عند ارتكابها[3]، ويشترط في السلوك الجرمي في الجرائم الإلكترونية معرفة بداية النشاط والشروع فيه ونتيجته، فعلى الرغم من أن القانون لا يعاقب على الأعمال التحضيرية إلا أنه يصعب في الجرائم الإلكترونية الفصل بين الأعمال التحضيرية والبدء في النشاط الإجرامي فمثلاً شراء برامج الاختراق ومعدات لفك الشيفرة وكلمات السرّ تعتبر أعمال تشكّل بحد ذاتها جريمة يعاقب عليها القانون لذا فإن الجرائم الإلكترونية تختلف عن الجرائم التقليدية في المعاقبة على الأعمال التحضيرية[4]، وأكد المشرع (الفلسطيني والمصري) على تجريم الأعمال التحضيرية التي تسبق ارتكاب الجرائم الإلكترونية وفرض العقوبة عليها[5] واعتبر هذه الأعمال جريمة مستقلة قائمة بحد ذاتها.

---

[1] الحلبي، محمد علي السالم: **شرح قانون العقوبات**، مرجع سابق، ص136.

[2] برّاك، أحمد وجرادة، عبدالقادر: **الجرائم الإلكترونية في التشريع الفلسطيني**، مرجع سابق، ص58.

[3] هروال، نبيلة هبة: **جرائم الإنترنت "دراسة مقارنة"**، رسالة دكتوراة ، جامعة أبي بكر بلقايد، تلمان– الجزائر، 2013–2014، ص58.

[4] أبو الرب، نبيل محمود فريد: **مفهوم الجرائم المعلوماتية وتحدياتها التشريعية في فلسطين**، رسالة ماجستير، جامعة النجاح الوطنية، نابلس–فلسطين، 2018، ص28+29.

[5] المادة 26 من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات الفلسطيني:" كل من حاز بغرض الاستخدام جهازاً أو برنامجاً أو أي بيانات إلكترونية معدّة أو كلمة سر أو تراميز دخول أو قدمها أو أنتجها أو وزعها أو استوردها أو صدرها أو روّج لها وذلك بغرض اقتراف أي من الجرائم المنصوص عليها في هذا القرار بقانون، المادة 22 من قانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات: " ... كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدّر أو تداول بأي صورة من صور التداول أي أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو بيانات مماثلة بدون تصريح من الجهاز أو مسوّغ من الواقع أو القانون وثبت أن ذلك السلوك كان بغرض استخدام أي منها في ارتكاب أو تسهيل ارتكاب أي جريمة من الجرائم المنصوص عليها في هذا القانون أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء".

وللسلوك الجرمي صورتين: وهما السلوك الإيجابي والسلوك السلبي، ويقصد بالسلوك الإيجابي هو ذلك الفعل أو النشاط الذي يقوم به الجاني مستخدماً فيه أحد أعضاء جسمه(اليد أو الرجل) لإحداث أثر خارجي، ويشترط في هذا النشاط أن يكون صادراً عن إرادة حرّة واعية[1]ويتطلب مجهوداً بدنياً كبيراً، أما السلوك الإيجابي في الجرائم الإلكترونية يختلف عن الجرائم العادية إذ إنه يتطلب أن يتم الفعل أو النشاط بالاعتماد على عقل الجاني ومستخدماً مجهوداً بدنياً بسيطاً[2]، فمثلاً عندما يقوم الجاني بتدمير البيانات أو حذفها أو التلاعب فيها على أحد الأنظمة المعلوماتية فإنه يحتاج إلى استخدام ذكائه لاختراق النظام ومن ثم يستخدم يده للقيام بالضغط على الأزرار أو اللمس على الشاشة لإعطاء الأوامر للجهاز الإلكتروني للحذف أو تغيير المعلومات أو...إلخ[3].

أما السلوك السلبي فهو عبارة عن السلوك الذي يفرضه القانون ويوجبه ولكن يمتنع الشخص المكلف به عن القيام به مما يؤدي امتناعه إلى ارتكاب جريمة[4].

ويمكن القول أن السلوك السلبي هو نادر الحدوث في الجرائم الإلكترونية، ولكن يمكن تصورّه في أن يكون هناك موظف مسؤول عن حماية المعلومات والبيانات ويتعمّد هذا الموظف في عدم حمايتها أو المحافظة عليها من الاختراق كأن لا يقوم بتشغيل برامج الحماية فيؤدي ذلك إلى ارتكاب جريمة إلكترونية[5]، وبالرجوع إلى القرار بقانون بشأن الجرائم الإلكترونية الفلسطيني نجد أنه لم ينص صراحةً على الجريمة الإلكترونية التي تقع بصورة السلوك السلبي على الرغم من أنه أورد في المادة 61منه أنه يتوجب على أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها أن تعمل على اتخاذ الإجراءات والتدابير الأمنية والوقائية اللازمة لحماية كافة أنظمتها المعلوماتية، مواقعها الإلكترونية، شبكاتها المعلوماتية، البيانات

---

[1] الحلبي، محمد علي السالم: **شرح قانون العقوبات**، مرجع سابق، ص137.

[2] محمود، عبدالله ذيب و درّاج، أسامة اسماعيل: **الوجيز في الجرائم الإلكترونية "القواعد الموضوعية والإجرائية"**، عمّان– الأردن: دار الثقافة للنشر والتوزيع، 2022، ص46.

[3] العجمي، عبدالله دغش: **المشكلات العملية والقانونية للجرائم الإلكترونية**، مرجع سابق، ص27.

[4] نجم، محمد صبحي: **قانون العقوبات القسم العام النظرية العامة للجريمة**، مرجع سابق، ص210.

[5] برّاك، أحمد وجرادة، عبد القادر: **الجرائم الإلكترونية في التشريع الفلسطيني**، مرجع سابق، ص60.

والمعلومات الإلكترونية الخاصة بها، إلا أنه لم يجرم سلوك عدم الالتزام ولم يشير إلى العقوبة المفروضة في هذه الحالة على عكس القانون المصري الذي نص في المادة 29 من قانون مكافحة جرائم تقنية المعلومات المصري على أنه كل مسؤول عن إدارة موقع أو حساب خاص أو بريد إلكتروني أو نظام معلوماتي لم يتخذ التدابير والاحتياطات التأمينية مما عرّض أو تسبب في إهماله في تعرّض أياً منها لإحدى الجرائم المنصوص عليها في هذا القانون فإنه يعتبر بامتناعه هذا مرتكباً لجريمة إلكترونية، وبالتالي نرى هنا أن المشرع المصري جرّم السلوك السلبي وفرض له عقوبة مناسبة.

واستناداً لما سبق نرى أن السلوك أو النشاط الجرمي سواء أكان سلوكاً إيجابياً أو سلبياً دائماً ما يتطلب وجود وسيلة تكنولوجية كجهاز إلكتروني واتصال بشبكة الإنترنت وبيئة تقنية حاضنة للقيام بهذا النشاط[1]، فيتم التعامل مع أشياء غير ملموسة وهي البيانات والمعلومات التي يتم معالجتها من خلال جمعها أو تعديلها أو نقلها أو محوها أو نشرها أو حجب الوصول إليها أو القيام بإيقاف عمل الأجهزة أو تدمير الأنظمة أو التطبيقات أو تعديلها أو بأي طريقة من شأنها أن تشكّل جريمة إلكترونية.

ب. النتيجة الجرمية: وتتمثل في الآثار التي تترتب على السلوك الجرمي المرتكب سواء أكان هذا السلوك إيجابي أم سلبي، بالتالي هي تشكّل الضرر الذي ينتج عن السلوك الجرمي ويقع على الحق أو المصلحة المقررة لها حماية من المشرع[2].

وتقسم الجرائم بحسب مدى تطلب حدوث نتيجة إلى جرائم الخطر وجرائم الضرر، فجرائم الخطر تعني أنها هي الجرائم التي لا يشترط فيها تحقق نتيجة جرمية معينة إذ يكفي فيها ارتكاب السلوك الجرمي بغض

[1] العجمي، عبدالله دغش: **المشكلات العملية والقانونية للجرائم الإلكترونية**، مرجع سابق، ص27.

[2] برّاك، أحمد وجرادة، عبدالقادر: **الجرائم الإلكترونية في التشريع الفلسطيني**، مرجع سابق، ص61.

النظر عن النتيجة، أما جرائم الضرر فهي الجرائم التي تتطلب تحقق نتيجة جرمية معينة بعد ارتكاب السلوك الجرمي[1].

والجرائم الإلكترونية يمكن أن تكون جرائم من قبيل جرائم الخطر بحيث لا يعتدّ فيما إذا تحققت النتيجة أم لا، إذ إنه بمجرد ارتكاب السلوك الجرمي يعتبر الفاعل مرتكباً للجريمة الإلكترونية بغض النظر عن تحقق الجريمة، فمثلاً مجرد الدخول غير المشروع أو الاختراق لأحد الأنظمة المعلوماتية من قبل شخص غير مسموح له بالدخول ودون إحداث أي تغيير في البيانات فإنه يعتبر دخوله واختراقه هو جريمة بحد ذاتها حتى لو لم تتحقق النتيجة التي كان يبغيها، وجرائم من قبيل جرائم الضرر والتي يشترط فيها تحقيق نتيجة مثل بعض صور جرائم الإرهاب الإلكتروني والتي تتطلب تحقيق نتيجة معينة[2].

ويترتب على النتيجة الجرمية للجرائم الإلكترونية آثار عديدة، فيمكن أن تكون آثاراً مادية تتمثل بالضرر الذي يلحق بالمجني عليه نتيجة فقدانه للبيانات والمعلومات التي تم تدميرها وإتلافها، أو خسائر مادية تلحق بشركة ما بسبب الاعتداء على بيانات ومعلومات أنظمتها والتغيير والتلاعب فيها، أو آثاراً معنوية كالتشهير بشخص على المواقع الإلكترونية ونشر صوره ومعلومات خاصة به، أو آثاراً قانونية فالاعتداء يكون على مصلحة محمية بموجب القانون بالتالي إن ارتكاب السلوك الجرمي والاعتداء على بيانات أو معلومات شخص ما وسرقتها فإنه يترتب عليه اعتداء على حق الملكية المكفول بالقانون[3].

---

[1] المناعسة، أسامة أحمد و الزعبي، جلال محمد: **جرائم تقنية نظم المعلومات الإلكترونية "دراسة مقارنة"**، عمان– الأردن: دار الثقافة للنشر والتوزيع، 2017، ص56.

[2] العبيدي، صدام حسين ياسين: **جرائم الانترنت وعقوباتها في الشريعة الإسلامية والقوانين الوضعيّة**، الطبعة الأولى، مصر: المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع،2019،ص234.

[3] محمود، عبدالله ذيب ودرّاج، أسامة اسماعيل: **الوجيز في الجرائم الإلكترونية**، مرجع سابق، ص48+49.

وفي الحقيقة لا تقتصر النتيجة الجرمية في الجريمة الإلكترونية في ترتيب الآثار على العالم الافتراضي الخيالي، وإنما يمكن أن تمتد الآثار إلى العالم الحقيقي كأن يتم ارتكاب جريمة عادية تقليدية باستخدام إحدى الوسائل التكنولوجية ليتم سرقة بيانات عميل وسرقة أمواله وسحبها من حسابه المصرفي[1].

ج. العلاقة السببية: وهي العلاقة التي تربط بين السلوك أو النشاط الجرمي المرتكب والتي من خلالها يثبت بأن بسبب هذا السلوك قد حصلت هذه النتيجة وترتب الضرر.

ونظراً للإشكاليات التي قد تحدث عند إثبات العلاقة السببية بين السلوك الجرمي والنتيجة فقد وضع الفقه عدة نظريات لتحديد معيار العلاقة السببية بين السلوك والنتيجة والتي تتمثل فيما يلي:-

1. نظرية السبب الأقوى (السبب المباشر): وتقوم هذه النظرية على أن السبب الأقوى أو المباشر أو الأساسي في حدوث النتيجة هو السبب الذي يؤخذ به وأن أي أسباب أخرى هي مجرد عوامل مساعدة[2].
2. نظرية تعادل الأسباب: وتقوم على أنه هناك مجموعة من الأسباب التي أدت إلى حدوث النتيجة ولكن يكون فعل الجاني هو المسؤول عن حدوث النتيجة مهما تعددت هذه الأسباب التي تبعت فعله، وتم انتقاد هذه النظرية كونها تحمّل الفاعل الأول المسؤولية كافة عن الجريمة حتى لو كان فعله ضئيل[3].
3. نظرية السبب الملائم أو السبب الكافي: وتقوم على أن العلاقة السببية تثبت بين السلوك والنتيجة وفقاً للمجرى العادي للأمور لتحقيق النتيجة[4]، فالسلوك الجرمي وفقاً للمجريات العادية هو أدى إلى تحقيق

---

[1] محمود، عبدالله ذيب ودرّاج، أسامة اسماعيل: **الوجيز في الجرائم الإلكترونية**، مرجع سابق، ص50.

[2] المصري، نداء نائل فايز: **خصوصية الجرائم المعلوماتية**، مرجع سابق، ص18.

[3] الحلبي، محمد علي السالم: **شرح قانون العقوبات**، مرجع سابق، ص146.

[4] المناعسة، أسامة أحمد و الزعبي، جلال محمد: **جرائم تقنية نظم المعلومات الإلكترونية**، مرجع سابق، ص59.

النتيجة لذا هناك علاقة سببية ربطت بين السلوك والنتيجة، وبمجرد حصول أفعال غير متوقعة فإن العلاقة السببية تنقطع بالتالي عدم وجود ربط بين سلوك الفاعل والنتيجة لذلك لا يعتبر هو المسؤول[1].

أما فيما يتعلق بالجرائم الإلكترونية فهي كالجرائم الأخرى إذ يجب توافر العلاقة السببية التي تربط بين السلوك الجرمي والنتيجة التي تم إحداثها، وأما عن المعيار لإثبات العلاقة السببية بين السلوك والنتيجة فهو أمر متروك للفقه والقضاء[2] وهي تحدد حسب مجريات الأحداث والظروف التي أحاطت بالجريمة.

وتتحقق العلاقة السببية في الجرائم الإلكترونية عند القيام بالسلوك الجرمي المتمثل في الوصول إلى بيانات ومعلومات يحظر عليه الوصول إليها وباستخدام جهاز إلكتروني متصلاً بالإنترنت، ومن ثم يقوم بنشر هذه البيانات أو المعلومات كأن يتم اختراق جهاز خاص بفتاة أو اختراق إحدى حساباتها على مواقع التواصل الاجتماعي ومن ثم تهديدها ونشر صورها ومحادثاتها، لذلك نربط السلوك المتمثل بالاختراق بالنتيجة المتمثلة بالتشهير بالفتاة وإلحاق الضرر بها وبسمعتها.

ثالثاً: الرّكن المعنوي للجريمة الإلكترونية

يقصد به "القوة النفسية التي تكشف عن إرادة الجاني وموقفه الباطني من تحقيق العدوان في الجريمة"[3].

ويتمثل الرّكن المعنوي بالقصد الجنائي العام:

أ. العلم: وهو أن يكون الجاني عالماً بكافة العناصر الأساسية للجريمة[4]، وللعلم في الجريمة نوعان هما: العلم بالوقائع المادية المكونة للجريمة بحيث يكون الجاني عالماً بكافة الظروف التي تجعل من عمل يبدو ظاهره مشروع لكنه يشكّل جريمة، والعلم بالتكييف أي العلم بتكييف القانون لهذه الوقائع

---

[1] الحلبي، محمد علي السالم: **شرح قانون العقوبات**، مرجع سابق، ص146.

[2] المصري، نداء نائل فايز: **خصوصية الجرائم المعلوماتية**، مرجع سابق، ص19.

[3] أحمد، طارق عفيفي صادق: **الجرائم الإلكترونية جرائم الهاتف المحمول" دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي**، الطبعة الأولى، القاهرة– مصر: المركز القومي للإصدارات القانونية، 2015، ص53.

[4] عطا الله، إمام حسنين: **جرائم تقنية المعلومات في التشريعات والصكوك العربية**، الرياض–السعودية: دار جامعة نايف للنشر، 2017، ص150.

والمسؤولية الجزائية التي يرتبها عليها[1]، وبذلك تقوم المسؤولية الجنائية على الشخص طالما هو عالماً بهذه الوقائع وما يترتب عليها من آثار.

وهناك حالات قد لا تقوم فيها المسؤولية الجنائية على الشخص إذا صدر منه السلوك الذي يشكّل جريمة لكن من غير قصد أو بصورة خاطئة كأن يقوم بالدخول إلى نظام معلوماتي أو موقع إلكتروني كان يعتقد أن الدخول إليه مشروعاً أو كان قد سبق له الاشتراك للدخول إليه وانتهى اشتراكه دون أن يعلم أو يتنبّه لذلك، فإذا قام بعد ذلك بالخروج فوراً بعد الشعور بخطئه ودون أن يكون قد تلاعب بالبيانات أو أحدث أي تغيير، فإن المسؤولية الجنائية لا تقوم عليه ولا يمكن تصوّر قيام الجريمة لانتفاء القصد وذلك لأن الغلط والخطأ هو أمر جوهري ينفي القصد الجنائي[2].

ب. الإرادة: ويقصد بها القدرة الكاملة والحرّة للشخص المتمتع بالأهلية الجنائية لتوجيه نفسه لارتكاب فعل أو سلوك أو نشاط معيّن أو إلى عدم القيام به والامتناع عنه دون أن يكون عليه أي ضغط أو إكراه أو إجبار من أي جهة لدفعه للقيام بالنشاط[3]، لذلك يسعى الجاني من خلال توجيه نفسه وبإرادته لارتكاب السلوك أو النشاط لتحقيق نتيجة معينة وبالتالي تكون نيته الإجرامية قائمة[4].

على الرغم من أن غالبية الجرائم الإلكترونية تتم بصورة قصدية وعمدية[5]، والتي تتطلب توافر القصد الجنائي العام–العلم والإرادة– إلا أنه هناك بعض الجرائم الإلكترونية لا تقتصر على توافر القصد الجنائي العام فحسب بل يتطلب أيضاً توافر القصد الجنائي الخاص والذي يقصد به توجه إرادة الشخص لتحقيق غاية أبعد من الغاية التي يقوم عليها القصد الجنائي العام، ويشترط في القصد الجنائي الخاص توافر وقيام

---

[1] البرايسة، حسين محمد فلاح: **الركن المعنوي للجرائم الإلكترونية وفقاً لقانون العقوبات الأردني**، رسالة ماجستير، جامعة الشرق الأوسط، عمان– الأردن، 2021،ص78.

[2] بخي، فاطمة الزهراء: **إجراءات التحقيق في الجريمة الإلكترونية**، رسالة ماجستير، جامعة المسيلة، الجزائر، 2013–2014، ص36.

[3] الحلبي، محمد علي السالم: **شرح قانون العقوبات**، مرجع سابق، ص186.

[4] بغدادي، أدهم باسم نمر: **وسائل البحث والتحري عن الجرائم الإلكترونية**، رسالة ماجستير، جامعة النجاح الوطنية، نابلس–فلسطين، 2018، ص24.

[5] بغدادي، أدهم باسم نمر: **وسائل البحث والتحري عن الجرائم الإلكترونية**، مرجع سابق، ص24.

القصد الجنائي العام وذكر الغاية أو الهدف الأبعد واشتراطه ضمن النص القانوني حتى يصبح قصداً جنائياً خاصاً[1]، ومن الأمثلة على الجرائم التي تتطلب قصداً جنائياً خاصاً جرائم التزوير الإلكتروني والتي يكون فيها القصد الجنائي العام المتمثل في علم الجاني بمخالفته للقانون وتتجه إرادته لارتكاب السلوك المجرم، أما القصد الجنائي الخاص فهو يتمثل في نية الجاني للغش في استخدام المستند المزوّر من أجل تغيير الحقيقة وكذلك نيته لإحداث ضرر للغير سواء أكان هذا الضرر احتمالياً أم فعلياً[2].

لذلك يمكن القول بأنه لا بدّ من أن يكون الجاني عالماً بأنه يقوم بنشاط إجرامي أو أن يكون عالماً بأن فعله هو يشكّل جريمة وأن تتجه إرادته الحرّة الكاملة إلى القيام بهذه الأفعال لتحقيق نتيجة معينة[3].

الفرع الثاني: محل الجرائم الإلكترونية

يمكن أن تقع الجريمة الإلكترونية على ثلاثة عناصر أساسية فإما أن تكون على إحداها أو عليها جميعاً وتصنف هذه العناصر إلى: الأشخاص، المعلومات، الأجهزة [4].

أولاً: الأشخاص

تحتل الجرائم الإلكترونية الواقعة على الأشخاص نسبة كبيرة من هذه الجرائم إذ تكون موجهة ضد أشخاص معينين أو ضد جهات معينة كالحكومة أو هيئة أو مؤسسة[5]، وتختلف الجرائم الإلكترونية عن الجرائم العادية، إذ تتميز هذه الأخيرة بوجود اعتداء مادي موجّه ضدّ المجني عليه من قبل الجاني، أما الجرائم الإلكترونية يقوم الجاني فيها بالاعتداء على المجني عليه ليس اعتداءً مادياً فقط وإنّما يمكن أن يكون أيضاً اعتداءً معنوياً والذي يتمثل بالشتائم والقذف والتشهير ونشر معلومات وأفكار مغلوطة وكاذبة والاعتداء على

[1] محمود، عبدالله ذيب و درّاج، أسامة اسماعيل: **الوجيز في الجرائم الإلكترونية**، مرجع سابق، ص53.

[2] المصري، نداء نائل فايز: **خصوصية الجرائم المعلوماتية**، مرجع سابق، ص44.

[3] العبيدي، صدام حسين ياسين: **جرائم الانترنت وعقوباتها في الشريعة الإسلامية والقوانين الوضعية**، مرجع سابق ، ص80.

[4] حسنية ، أحمد أسامة : **الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية**، مرجع سابق ، ص 12.

[5] حسنية ، أحمد أسامة : **الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية**، مرجع سابق ، ص 12.

الملكية الفكرية للأسماء وغير ذلك من صور الاعتداء، وينتج عن الاعتداء في الجرائم الإلكترونية أضراراً معنوية تلحق بالمجني عليه[1].

وأورد القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات الفلسطيني العديد من الجرائم ضد الأشخاص منها ما نصّت عليه المادة 15 منه عندما يقوم شخص باستخدام الشبكة الإلكترونية أو أحد الأجهزة الإلكترونية بتهديد آخر أو يقوم بابتزازه حتى يقوم بفعل أو امتناع عن فعل حتى لو كان هذا الفعل أو الامتناع عنه مشروعاً وأكدت على ذلك محكمة النقض بقولها "...فإن استخدام الشبكة الإلكترونية في تهديد شخص حتى ولو كان مشروعاً يعاقب أي يعتبر هذا الفعل جريمة يعاقب عليها القانون"[2]، وأيضاً ما ورد في المادة 16 من قام قصداً باستخدام الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات بإرسال ما هو مسموع أو مقروء أو مرئي ويتضمن أعمالاً إباحية أو تتعلق بالاستغلال الجنسي للأشخاص سواء أكانوا فوق الثامنة عشر من عمرهم أو أقل، وكذلك من يقوم بإنشاء، إعداد، حفظ، معالجة، عرض، طباعة، نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على الأشخاص خاصة لمن هم دون الثامنة عشر من عمرهم، وفي الواقع لا يقتصر الاعتداء على الأشخاص من الناحية المعنوية فقط من تهديد وابتزاز والتعرض لهم وإنما يمكن أن يصل الاعتداء على أموالهم كسرقتها أو اختلاسها أو الاستيلاء على أموال منقولة لهم أو سندات أو تواقيع إلكترونية وذلك بالاستعانة بالطرق الاحتيالية سواء اسم كاذب أو صفة احتيالية[3].

أما بالنسبة لقانون مكافحة جرائم تقنية المعلومات المصري فقد أورد أيضاً وتحدث عن العديد من الجرائم الإلكترونية التي تقع على الأشخاص ومن الأمثلة عليها ما ورد في المادة 25 منه القيام بالاعتداء على أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهك حرمة الحياة الخاصة أو قام بإرسال عدد

---

[1] طه ، وليد: **التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست:** مصر، ص 18.

[2] نقض/جزاء فلسطيني رقم 2019/171.

[3] مادتي 13+14 من القرار بقانون الفلسطيني رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

كبير من الرسائل الإلكترونية لشخص دون رضاه أو القيام وعن طريق الشبكة المعلوماتية أو باستخدام إحدى وسائل تقنية المعلومات نشر معلومات أو أخبار أو صور تنتهك خصوصية أي شخص دون رضاه سواء أكانت هذه المعلومات المنشورة صحيحة أو غير صحيحة، وكذلك ما ورد في المادة 26 العمل على معالجة معطيات شخصية للغير وبواسطة برنامج معلوماتي أو تقنية معلوماتية لربطها بمحتوى منافٍ للآداب العامة أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه.

ثانياً: المعلومات

تشكل الجرائم الموجهة ضد البيانات والمعلومات أكثر خطورة كونها يتعدى أثرها ليشمل المجتمع ككل من أشخاص ومؤسسات وغير ذلك، ويترتب على مثل هذه الجرائم تأثيرين وهما:

أ. التأثير السلبي: إذ يتم الدخول واختراق أنظمة المعلومات بصورة غير مشروعة ولكن دون أن يتم إجراء أي تعديل أو تغيير بالبيانات، وطالما أن الشخص غير مصرح له بالدخول لقاعدة البيانات وقام باختراقها بصورة غير مشروعة فهو مرتكب لجريمة[1]، ومن الأمثلة على مثل هذه الجرائم ذات التأثير السلبي ما ورد في القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات الفلسطيني أن كل من دخل عمداً دون وجه حق بأي وسيلة موقعاً إلكترونياً أو نظاماً أو شبكة إلكترونية أو وسيلة تكنولوجيا معلومات أو جزء منها أو تجاوز الدخول المصرح به أو استمر في التواجد بها بعد علمه بذلك سواء أكانت تلك البيانات لمؤسسة معينة كبنك مثلاً أو بيانات حكومية فإن ذلك يشكل جريمة ويعاقب بالحبس أو بالغرامة[2]، وكذلك قيام الشخص عمداً بفك بيانات مشفرة في حالات غير مصرح بها قانوناً[3]، ومن الأمثلة أيضاً ما ورد في قانون مكافحة جرائم تقنية المعلومات المصري قيام الشخص الجاني عمداً بالدخول غير المشروع أو عن طريق الخطأ غير العمدي وبقي

[1] طه، وليد: **التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابيست**، مرجع سابق، ص 19.

[2] مادة 4 من القرار بقانون الفلسطيني رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[3] مادة 8 من القرار بقانون الفلسطيني رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

بدون وجه حق على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه[1]، كما أنه يمكن لشخص يكون متمتعاً بحق يخوّل له الدخول إلى موقع أو حساب خاص أو نظام معلوماتي ولكنه يقوم بالتعدي على هذا الحق من حيث الزمان ومستوى الدخول وبالتالي يصبح مرتكباً لجريمة إلكترونية بمجرد حدوث هذا التجاوز أو التعدي[2].

ب. التأثير الايجابي: إذ لا يكتفي الشخص بالدخول والاختراق لقاعدة البيانات والأنظمة بل يقوم بإجراء تعديلات وتغييرات على البيانات ويهدف من وراء ذلك جني فائدة مادية ومعنوية لنفسه والإضرار المادي والمعنوي بالجهة التي تعود لها البيانات[3]، ونذكر أمثلة على ذلك ما أوردتها المواد 3/4 و11و 12 من القرار بقانون بشان الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات الفلسطيني وهي الدخول والاختراق لقواعد البيانات بقصد التعديل والتغيير فيها وذلك من خلال حذفها أو إضافتها أو إفشاؤها أو إتلافها أو نقلها أو نسخها أو نشرها وكذلك التلاعب والتزوير فيها وفي أي مستندات إلكترونية رسمية تابعة للدولة أو هيئات أو مؤسسات عامة، أو استعمال مستندات رسمية مزورة أو أنشأ بيانات توقيع إلكتروني رسمي لا يحق له الحصول عليه، أو قام بالوصول دون وجه حق إلى بيانات وأرقام وعمل على التلاعب فيها، وما ورد أيضاً في قانون مكافحة جرائم تقنية المعلومات المصري في المادة 17منه القيام بجريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية وذلك من خلال إتلاف أو تعطيل أو تعديل مسار أو إلغاء كلياً أو جزئياً متعمداً وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه أياً كانت الوسيلة التي استخدمت في الجريمة.

---

[1] مادة 14 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.

[2] مادة 15 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.

[3] طه، وليد : **التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابيست**، مرجع سابق ، ص 20.

ثالثاً: الأجهزة

تستهدف هذه الجرائم بشكل أساسي الأجهزة الإلكترونية بغرض تعطيلها أو اتلافها أو التأثير عليها أو التغيير في المعلومات والبيانات الموجودة فيها، ومن الأساليب المتبعة في هذه الجرائم استخدام الفايروسات والتي تعد من قبيل البرامج الخبيثة الضارة التي تدمر الأجهزة الإلكترونية[1].

ومما يعد من قبيل الجرائم الإلكترونية ضد الأجهزة قيام الشخص الجاني بتعطيل وإعاقة الوصول إلى الأجهزة والبرامج أو البيانات أو المعلومات على هذه الأجهزة وذلك باستخدام الشبكة الإلكترونية أو أحد وسائل تكنولوجيا المعلومات[2]، وأيضاً إذا قام بإنتاج أو إدخال عن طريق الشبكة الإلكترونية أو أحد الأجهزة الإلكترونية ما من شأنه إيقافها عن العمل أو تعطيلها أو إتلاف البرامج أو حذفها أو تعديلها[3]، وكذلك القيام بجريمة اعتراض غير المشروع وبدون وجه حق للمعلومات أو البيانات أو لكل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسوب الآلي وما في حكمها[4].

[1] حسنية، أحمد أسامة: **الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية**، مرجع سابق، ص 12و13.

[2] مادة 5 من القرار بقانون الفلسطيني رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[3] مادة 6 من القرار بقانون الفلسطيني رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[4] مادة 16 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.

الفصل الأول

ماهية التفتيش في الجرائم الإلكترونية

إن الغاية من إجراء التفتيش الكشف عن الجريمة التي تم ارتكابها ومن ثم التنقيب عن الأدلة المتعلقة بهذه الجريمة من أجل الوصول إلى إثباتها وبالتالي نسبتها إلى مرتكبها، فالتفتيش هو من أخطر الإجراءات التي تقوم بها سلطة التحقيق لما فيه من مساس مباشر بالحياة الخاصة للإنسان؛ لذلك يجب على السلطات المختصة عند القيام به مراعاة الضمانات الواجب توافرها عند إجراء التفتيش حتى يتم المحافظة على حقوق الانسان وحرياته الأساسية وخصوصية أسراره، ولعلّ ما يهمنا في إجراء التفتيش هو التفتيش الذي يتم في الجرائم الإلكترونية، لذلك يتمتع التفتيش في الجرائم الإلكترونية بخصوصية أكثر من الجرائم الأخرى، كونه يجري على الوسائل التكنولوجية الحديثة والتي يتم فيها تخزين معلومات الناس وأسرارهم، لذا نتحدث في هذا الفصل حول ماهيّة إجراء التفتيش في الجرائم الإلكترونية وذلك من خلال تقسيمه على النحو الآتي:

المبحث الأول: تعريف التفتيش في الجرائم الإلكترونية

المبحث الثاني: شروط التفتيش في الجرائم الإلكترونية

المبحث الأول: تعريف التفتيش في الجرائم الإلكترونية

يعدّ التفتيش إجراء يتم فيه البحث عن الأدلة وضبطها من أجل كشف الحقيقة، ونظراً لخطورة وحساسية هذا الإجراء كونه ماسّ بحقوق وحريات الأشخاص فقد اتفقت جميع دساتير العالم على ضرورة صون هذه الحقوق وأن لا يتم المساس بها إلا وفقاً لما يقرره القانون ونرى كذلك أن الدساتير شددت على ضرورة وجود أمر قضائي مسبب وبالكيفية التي حددها القانون، وعلى الرغم من النص على وجوب إصدار مذكرة قانونية للتفتيش وخاصة عند تفتيش المساكن إلا أنّ المشرعين الفلسطيني والمصري أوردا حالات على

سبيل الحصر يجوز فيها الدخول للمساكن وتفتيشها، إذ تعتبر حالات استثنائية وفي حالات ضرورية يتم اللجوء إليها[1]، ونتعرف في هذا المبحث على إجراء التفتيش من خلال مطلبين:

المطلب الأول: المقصود بالتفتيش في الجرائم الإلكترونية.

المطلب الثاني: الطبيعة القانونية للتفتيش في الجرائم الإلكترونية.

المطلب الأول: المقصود بالتفتيش في الجرائم الإلكترونية

ويقصد بالتفتيش **لغةً:** "هو مصدر للفعل فتّش بمعنى الطلب والبحث وفتّش الشيء فتشاً وفتّشه تفتيشاً مثله"[2]، أما **اصطلاحاً** فهو" عبارة عن البحث عن الأدلة والأشياء المتعلقة بوقوع الجريمة في مسكن المشتكى عليه أو البحث عنها في ملابسه أو الأشياء التي يرتديها أو الأدوات التي يستعملها"[3].

وللتفتيش عدة صور والتي تتمثل فيما يلي:

1. **التفتيش الإداري:** هو "الإجراء التحفظي الذي يتم بمعرفة الموظفين أو من في حكمهم، وذلك بقصد تحقيق أهداف إدارية عامة"[4]، إذ إنّه لا علاقة له بأدلة جريمة معينة ولا يدخل ضمن مجال إجراءات التحقيق فهو ليس تفتيشاً بالمعنى القانوني وللتفتيش الإداري عدة صور وهي: أ- فقد يكون تفتيشاً إدارياً جائزاً بنص القانون للحيلولة دون وقوع الجرائم أو لاكتشافها إن كانت وقعت ومن الأمثلة على

---

[1] مادة 48 من قانون الاجراءات الجزائية الفلسطيني "لا يجوز دخول المنازل من السطات المختصة بدون مذكرة إلا في إحدى الحالات التالية:1- طلب المساعدة من الداخل 2-حالة الحريق أو الغرق 3-إذا كان هناك جريمة متلبساً بها 4- في حالة تعقب شخص يجب القبض عليه أو شخص فر من مكان أوقف فيه بوجه مشروع " ، مادة 45 من قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950 "لا يجوز لرجال السلطة الدخول في أي محل مسكون إلا في الأحوال المبينة في القانون أو في حالة طلب المساعدة من الداخل أو حالة الحريق أو الغرق أو ما شابه ذلك".

[2] لسان العرب – ابن منظور – الجزء 6 – ص 325.

[3] الكساسبة، فهد يوسف والطراونة ، مصطفى ، *الضوابط القانونية للتفتيش بغير إذن في القانونين الأردني والمصري " دراسة مقارنة* " ، **مجلة علوم الشريعة والقانون** ، مج 42، ع 2/ 2015 ، ص 713.

[4] حسين ، سامي جلال فقي: **التفتيش في الجرائم المعلوماتية**، مرجع سابق ، ص 75 .

ذلك التفتيش الذي يحصل على المتهم عند دخوله للسجن[1]، ب- التفتيش الإداري اتفاقاً: كالتفتيش اليومي الذي يخضع له العاملين بالمصانع عند مغادرتهم لأماكن عملهم[2]، ج- التفتيش الإداري بحكم الضرورة: كإجراء التفتيش الذي يقوم به رجل الإسعاف لجيوب الشخص المصاب للتعرف على هويته ويعد هذا الإجراء غير مخالف للقانون لأنه لا يعد تفتيشاً الذي يعتبر من أعمال التحقيق[3].

2. **التفتيش الوقائي:** وهذا النوع من التفتيش يأخذ صفتين: أ- فإما أن يكون إجراء من إجراءات التحقيق للبحث عن أدلة جريمة معينة، ب- أو إجراء للمحافظة على الأمن من خلال تجريد الشخص مما قد يحمله معه من أسلحة أو أدوات قد يستخدمها لإيذاء نفسه أو إلحاق الأذى بغيره، وتعتبر الصفة الثانية ليست من أعمال التحقيق بل مجرد إجراء احتياطي وقائي لمنع الشخص من إيذاء نفسه أو غيره، وهذا النوع من التفتيش لا يحتاج إلى وجود نص قانوني ليبيح القيام به فهو مجرد إجراء تستوجبه الضرورة للحفاظ على الأمن، وبالتالي لا يتطلب هذا التفتيش القيام بإجراء القبض القانوني كما أنه لا ينبغي أن يكون القائم بهذا التفتيش هو من مأموري الضبط القضائي[4].

3. **التفتيش القضائي:** وهذا النوع من التفتيش هو محض دراستنا فالتفتيش القضائي من الناحية القانونية، نجد أن المشرع لم يضع تعريفاً واضحاً له فلو رجعنا لقانون الاجراءات الجزائية الفلسطيني من المادة 39 إلى المادة 52 والتي تناولت أحكام التفتيش نجد أنها لم تتطرق إلى توضيح المقصود بالتفتيش بشكل مباشر، كما أن قانون الإجراءات الجنائية المصري لم يضع تعريفاً واضحاً للتفتيش القضائي واقتصر فقط على تعريف أحد أنواع التفتيش القضائي ألا وهو تفتيش المنازل بحيث عرّفه بأنه: " عمل من أعمال التحقيق ولا يجوز الالتجاء إليه إلا بمقتضى أمر من قاضي التحقيق بناءً على اتهام موجه

---

[1] الشهاوي، قدري عبدالفتاح: **مناط التفتيش قيوده وضوابطه في التشريع المصري، العربي، الأجنبي**، الطبعة الأولى، القاهرة-مصر: دار النهضة العربية، 2006، ص 28و34.

[2] الشهاوي، قدري عبدالفتاح: **مناط التفتيش قيوده وضوابطه**، مرجع سابق، ص 36.

[3] الشواربي، عبدالحميد: **إذن التفتيش في ضوء القضاء والفقه**، الإسكندرية-مصر: منشأة المعارف، ص 103.

[4] الشهاوي، قدري عبد الفتاح: **مناط التفتيش قيوده وضوابطه**، مرجع سابق، ص 25.

إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها أو إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة"[1].

لذلك حاول فقهاء القانون الجنائي وضع مفهوم للتفتيش القضائي والتي تنوعت ولكنها حتماً كانت تصب في معنى واحد ومن بين هذه المفاهيم ما وضعه الدكتور جلال ثروت بأنه: "اطلاع على محل له حرمة خاصة بحثاً عن دليل يفيد التحقيق"[2]، وكذلك التعريف التي وضعته الدكتورة فوزية عبد الستار أن التفتيش: هو عبارة عن إجراء من إجراءات التحقيق الابتدائي الذي يهدف للتوصل إلى أدلة الجريمة التي تم ارتكابها فعلاً ويتم ذلك بالبحث والتنقيب عن هذه الأدلة في مستودع السر[3].

ولعل أفضل تعريف ما وضعه الدكتور عبد المهيمن بكر والذي يعد تعريفاً جامعاً إذ عرّف التفتيش القضائي على أنه: إجراء من إجراءات التحقيق والذي لا تجوز مباشرته أو الإذن به إلا بشأن جناية أو جنحة وقعت للبحث عن دليل يفيد في كشف الحقيقة حيال شخص كانت دلائل كافية على اتهامه فيها بوصفه فاعلاً أو شريكاً أو على أنه حائز لأشياء استعملت في الجريمة أو نتجت عنها أو تعلقت بها ويقوم بهذا الإجراء سلطة حددها القانون في محل له حرمة لأنه مستودع الحق في سر الإنسان وتباشر هذه السلطة هذا الإجراء لأن ضرورة التحقيق تقتضيه سواء رضي به من يباشر حياله أو لم يرضى[4].

لذا إن التفتيش يجري على كل ما يتعلق بالشخص المشتبه به بارتكاب الجريمة فيمكن أن يتم تفتيش الشخص ذاته، وأمتعته، والأشياء المتعلقة به، وكذلك الأماكن سواء تعود ملكيتها له أو تواجد فيها، ويعود

---

[1] مادة 91 من قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950 المعدّل.

[2] ثروت، جلال: **نظم الاجراءات الجنائية**، مصر: دار الجامعة الجديدة، 2003 ، ص 438.

[3] عبد الستار، فوزية : **شرح قانون الاجراءات الجنائية وفقاً لأحدث التعديلات** ، القاهرة – مصر ، دار النهضة العربية ، 2010 ، ص 293.

[4] غانم، محمد علي مصطفى: **تفتيش المسكن في قانون الاجراءات الجزائية الفلسطيني دراسة مقارنة**، رسالة ماجستير، جامعة النجاح الوطنية، نابلس–فلسطين، ص 3 وما بعدها.

الهدف من وراء هذا الإجراء إلى إمكانية الكشف عن الجريمة المرتكبة والتأكد من حصولها فعلاً ومن ثم الوصول إلى مرتكبها ونسبتها له وضبط كافة الأشياء المتعلقة والمتحصلة من هذه الجريمة.

أما عن المقصود بالتفتيش في الجرائم الإلكترونية فهو لا يختلف عن التعاريف السابقة التي توضح المقصود بالتفتيش القضائي، فهذه التعريفات تعتبر أن التفتيش إجراءً قضائياً يتم من خلاله الاطلاع على حرمة مكان أو محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه، كما أن الهدف من إجراء التفتيش القضائي هو البحث عن الأدلة والحصول عليها وبغض النظر عن طبيعتها، بالتالي يمكن أن تكون هذه الأدلة عبارة عن أدلة إلكترونية[1]، لذلك يعرّف التفتيش في الجرائم الإلكترونية على أنه: عملية بحث وتنقيب في وعاء السر بقصد ضبط ما يفيد في كشف الحقيقة، فالهدف من إجراء التفتيش في الجرائم الإلكترونية هو الوصول إلى أدلة مادية أو معنوية تفيد في كشف الحقيقة وكشف المتهم ونسب الجريمة إليه[2]، أو هو" الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو نظمه أو الإنترنت"[3].

ويتمتع التفتيش في الجرائم بشكل عام سواء الجرائم الإلكترونية أو العادية بعدة خصائص هي:

1. الجبر والإكراه: إذ إنّ إجراء التفتيش فيه قدر من الإكراه بحيث يكون بغير إرادة الشخص أو رضائه، وبالتالي هو إجراء يتم فيه التعرض لحرية المتهم الشخصية وانتهاك لحقه في الاحتفاظ بأسراره، وفي حالة عدم رضوخ المتهم لإجراء التفتيش عليه أو بدت منه أي مقاومة أثناء التفتيش فإنه يمكن للقائم بالتفتيش أن يتخذ أي إجراء من شأنه أن يمكّنه من إتمام مهمته حتى لو اضطر إلى اللجوء إلى القوة

[1] حسين، سامي جلال فقي: **التفتيش في الجرائم المعلوماتية**، مرجع سابق ، ص 52.

[2] العبيدي، أسامة بن غانم : *التفتيش عن الدليل في الجرائم المعلوماتية*، **المجلة العربية للدراسات الأمنية والتدريب** ، مج29،ع58 ، ص 87.

[3] الطوالبة، علي حسن محمد: **التفتيش الجنائي على نظم الحاسوب والإنترنت**، البحرين، 2010 ، ص 21.

وصد مقاومة المتهم، لذلك أي تفتيش لا يتمتع بهذه الخاصية فهو لا يعدّ تفتيشاً وإنما يمكن أن يتخذ طابعاً آخر[1].

وتطبيقاً على ذلك فقد نصّ قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 على " يتعيّن على المقيم في المنزل أو المسؤول عن المكان المراد تفتيشه أن يسمح بالدخول إليه وأن يقدم التسهيلات اللازمة فإذا رفض السماح بدخوله جاز لمأمور الضبط القضائي تنفيذ ذلك بالقوة"[2] وكذلك نص على " لمأموري الضبط القضائي في حالة قيامهم بواجباتهم أثناء عملية التفتيش أن يستعينوا بقوات الشرطة أو القوة العسكرية إذا لزم الأمر"[3]، كما ونص قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950 على " لمأموري الضبط القضائي في حالة قيامهم بواجباتهم أن يستعينوا مباشرة بالقوة العسكرية"[4].

2. المساس بالحق في الحياة الخاصة: إذ يعدّ إجراء التفتيش من الإجراءات الماسّة بحرمة الشخص وحرمة مسكنه وحقوقه وحرياته، ويكون هذا الإجراء من أجل تحقيق مصلحة المجتمع في الدفاع ضد الجريمة، بحيث لا يمكن المساس بحق الشخص وحرياته إلا إذا وجد سبب يؤدي إلى وجوب المساس بهم ألا وهو وقوع جريمة ووجود قرائن قوية على أن صاحب هذا الحق هو فاعل أو شريك في هذه الجريمة، لذا يعتبر إجراء التفتيش قيداً على حرمة أو حصانة الشخص الذاتية وقيداً على حرمة أسراره الشخصية[5].

---

[1] ملالحة، عبدالرحمن عوض رجا وفتيحة، عمارة: *التفتيش إجراء تحقيق بين القانون الفلسطيني والجزائري*، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، مج5، ع2/2020 ، ص 1342.

[2] مادة 42 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

[3] مادة 49 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

[4] مادة 60 من قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950.

[5] الشواربي، عبد الحميد : **إذن التفتيش**، مرجع سابق، ص10.

وتأكيداً على ما سبق فقد نصّت المادة 39 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001: "دخول المنازل وتفتيشها عمل من أعمال التحقيق لا يتم إلا بمذكرة من قبل النيابة العامة أو في حضورها وبناءً على اتهام موجّه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها أو لوجود قرائن قوية على أنه يحوز أشياء تتعلق بالجريمة"، وكذلك المادة 49 من قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950: " إذا قامت أثناء تفتيش منزل المتهم قرائن قوية ضد المتهم أو شخص موجود فيه على أنه يخفي معه شيئاً يفيد في كشف الحقيقة جاز لمأمور الضبط القضائي أن يفتشه".

3. البحث عن الأدلة المادية للجريمة: فالهدف الأساسي من إجراء التفتيش هو ضبط الأدلة سواء كانت أدلة مادية أو أدلة قولية، فإذا لم تتوافر هذه الألة فإنه لا محل للتفتيش[1]، كما أنه لا يمكن إدانة أي شخص دون وجود دليل يثبت أنه من قام بارتكاب الجريمة، بالتالي يعدّ إجراء التفتيش وسيلة مهمّة للبحث عن الأدلة للجريمة ومن ثم ضبطها[2].

---

[1] رشاد، نوال محمد: *التفتيش القضائي*، **مجلة البحوث القانونية والاقتصادية**، مج21،ع2012/36، ص 592.

[2] وتأكيداً على ضرورة البحث والتفتيش عن الأدلة التي تتعلق بالجريمة المرتكبة ومن ثم العمل على ضبطها ما ورد في المادة 1/50و2 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 :" 1-لا يجوز التفتيش إلا عن الأشياء الخاصة بالجريمة الجاري التحقيق بشأنها ومع ذلك إذا ظهر عرضاً أثناء التفتيش وجود أشياء تعد حيازتها في حد ذاتها جريمة، أو تفيد بكشف الحقيقة في جريمة أخرى جاز لمأمور الضبط القضائي ضبطها2- يتم ضبط جميع الأشياء التي يعثر عليها أثناء إجراء التفتيش والمتعلقة بالجريمة وتحرز وتحفظ وتثبت في محضر التفتيش وتحال إلى الجهات المختصة"، وكذلك المادة 50 من قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950 :" لا يجوز التفتيش إلا للبحث عن الأشياء الخاصة بالجريمة الجاري جمع الاستدلالات أو حصول التحقيق بشأنها ومع ذلك إذا ظهر عرضاً أثناء التفتيش وجود أشياء تعد حيازتها جريمة أو تفيد في كشف الحقيقة في جريمة أخرى جاز لمأمور الضبط القضائي أن يضبطها".

المطلب الثاني: الطبيعة القانونية للتفتيش في الجرائم الإلكترونية

حتى يتسنّى لنا الحديث عن الطبيعة القانونية للتفتيش في الجرائم الإلكترونية، فإنه لا بدّ من الرجوع إلى الطبيعة القانونية لإجراء التفتيش القضائي بشكلٍ عام، ومن ثم التطرق إلى الطبيعة القانونية للتفتيش في الجرائم الإلكترونية، إذ إنّ هنالك اختلاف فقهي حول تحديد الطبيعة القانونية للتفتيش وخرج هذا الاختلاف بانقسام الآراء إلى أربعة اتجاهات فقهية وهي على النحو الآتي:

الفرع الأول: معيار الهدف من إجراء التفتيش

ويرى أصحاب هذا الاتجاه أن الطبيعة القانونية للتفتيش يتم تحديدها من خلال الهدف من هذا الإجراء، فالهدف من إجراء التفتيش هو البحث عن الأدلة المتعلقة بالجريمة الجاري التحقيق بشأنها ومن ثم الحصول على هذه الأدلة وضبطها ومن ثم نسبتها إلى المتهم[1].

وبحسب رأي أصحاب هذا الاتجاه فإنه يعد التفتيش من أعمال التحقيق؛ "لأن أعمال التفتيش تتجه إلى البحث عن الأدلة وجمعها فكل عمل يبحث به المحقق عن دليل يعد من أعمال التحقيق إذ إنّ التحقيق هو العمل الموجّه إلى كشف الحقيقة"[2].

ويكون الهدف عادةً من إجراء التفتيش في الجرائم العادية التقليدية هو البحث عن الأدلة المادية كالبحث عن أداة الجريمة، أما الهدف من إجراء التفتيش في الجرائم الإلكترونية فيكون للبحث عن الأدلة المادية مثل الحاسوب أو الهاتف النقّال المستخدم في ارتكاب الجريمة، أو البحث عن الأدلة المعنوية كالبحث عن البيانات والمعلومات المتعلقة بالجريمة الإلكترونية المرتكبة.

---

[1] رشاد، نوال محمد: **التفتيش القضائي**، مرجع السابق، ص594.

[2] الحسيني، سامي حسني: **النظرية العامة للتفتيش في القانون المصري والمقارن**، القاهرة–مصر: دار النهضة العربية، 1972، ص55.

الفرع الثاني: معيار المرحلة التي تكون فيها الدعوى الجزائية

ويتعلق هذا المعيار بالوقت الذي جرى فيه إجراء التفتيش بحيث يرى مؤيدو هذا الاتجاه إلى أن الطبيعة القانونية لإجراء التفتيش يتحدد بحسب المرحلة التي تكون فيها الدعوى الجزائية، بالتالي إذا كان هذا الإجراء قد تم قبل فتح التحقيق فإنه يعدّ عملاً من أعمال الاستدلال أما إذا جرى بعد فتح التحقيق فإنه يعدّ من أعمال التحقيق الابتدائي[1]، ويواجه هذا الرأي انتقادات ومن بينها:

أ. إنّ أعمال الاستدلال يجب ألا تتضمن أي تعرض لحقوق الأفراد وحرياتهم أو حرمة مساكنهم دون أخذ إذن قضائي مسبق، لذلك إن صدور الإذن القضائي يعني حصول جريمة وبالتالي لا يمكن القول بأن إجراء التفتيش عمل من أعمال الاستدلال[2].

ب. لا يمكن الاعتماد على هذا المعيار في تحديد الطبيعة القانونية لإجراء التفتيش في الجرائم الإلكترونية؛ ويعود السبب في ذلك إلى أن هناك بعض الجرائم الإلكترونية تتطلب من الجهات المختصة القيام ببعض الإجراءات قبل إجراء التفتيش لضبط الأدلة ومن هذه الإجراءات التنصّت والتجسس المعلوماتي، وبالتالي لا يمكن في مثل هذه الحالة أن نطلق على هذا الإجراء بأنه عمل من أعمال الاستدلال وإنما هو من أعمال التحقيق[3].

---

[1] الحسيني، سامي حسني: **النظرية العامة للتفتيش**، مرجع سابق، ص55.

[2] حسين، سامي جلال فقي، **التفتيش في الجرائم المعلوماتية**، مرجع سابق، ص96.

[3] الطوالبة، علي حسن محمد: **التفتيش الجنائي على نظم الحاسوب والانترنت**، مرجع سابق، ص24.

الفرع الثالث: معيار صفة القائم بإجراء التفتيش القضائي

إذ يحدد أصحاب هذا الاتجاه الطبيعة القانونية لإجراء التفتيش من خلال صفة القائم بإجراء التفتيش، فإذا كان القائم بهذا الإجراء هو أحد أفراد السلطات المختصة حينئذٍ يكون إجراء التفتيش عملاً من أعمال التحقيق، أما إذا من قام به هو غير السلطات المختصة فلا يعد عملاً من أعمال التحقيق[1].

ويؤخذ على هذا المعيار بأن هناك حالات لا يشترط فيها إجراء التفتيش من قبل السلطات المختصة بالتحقيق وإنما يمكن ممارسة هذا الإجراء من قبل مأموري الضبط القضائي الذين يخضعون لقواعد معينة بحيث يمنحون فيها صفة سلطة التحقيق ويقوموا باتخاذ إجراءات التحقيق وليس إجراءات الاستدلال، ومن هذه الحالات حالتي:

أ. التلبس[2] وفي ذلك قضت محكمة النقض الفلسطينية على أنه (إذا توافرت حالة من حالات التلبس بالجريمة الواردة في المادة 26 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 فإن المشرع الفلسطيني في المادة 27 من هذا القانون أوجب على مأمور الضبط القضائي القيام بإجراءات معينة ومن ضمنها معاينة الآثار المادية للجريمة والتحفظ عليها)[3].

ب. التفويض من قبل السلطات المختصة بالتحقيق، حيث يقصد بالتفويض هو تكليف مأمور الضبط القضائي بعمل أو أكثر من أعمال التحقيق من قبل السلطة المختصة بالتحقيق ويعتبر العمل الذي يقوم به مأمور الضبط القضائي كأنه صادر من سلطة التحقيق نفسها كما أنه يتمتع هذا العمل بذات القيمة القانونية التي يتمتع بها العمل الصادر عن السلطة المختصة بالتحقيق، وقد أكد كل من المشرع

---

[1] قدواري، ابراهيم: **التفتيش في قانون الإجراءات الجزائية الجزائري**، رسالة ماجستير، جامعة محمد خيضر، الجزائر، 2015-2016،ص22.

[2] ما أكدت عليه كل من المادة 27 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 والمادة 31 من قانون الاجراءات الجنائية المصري رقم 150 لسنة 1950 وهو أنه يتوجب على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فوراً إلى مكان الجريمة ويعاين الآثار المادية لها ويتحفظ عليها ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة، وبذلك يمكن لمأمور الضبط القضائي أن يقوم بالتفتيش في حالة التلبس ويكون هذا التفتيش صحيحاً ويعتبر عملاً من أعمال التحقيق وكأن من قام به هو السلطة المختصة بالتحقيق.

[3] نقض/جزاء فلسطيني رقم 20لسنة2021.

الفلسطيني[1] والمشرع المصري[2] على إمكانية قيام السلطة المختصة بالتحقيق تفويض أحد أعضاء الضبط القضائي بالقيام بأي عمل من أعمال التحقيق فيما عدا الاستجواب في مواد الجنايات وبالتالي يمكن لأحد أعضاء مأموري الضبط القضائي القيام بإجراء التفتيش القضائي وبذلك يتمتع في حدود تفويضه بجميع السلطات المخولة للسلطة المختصة بالتحقيق.

لذا يمكن لأعضاء مأموري الضبط القضائي القيام بإجراء التفتيش على الأجهزة الإلكترونية والبرامج والدخول إلى قواعد البيانات بناءً على تفويض من السلطة المختصة بإجراء التفتيش وذلك استناداً إلى المادة1/52 من القرار بقانون رقم 10 لسنة 2018 الفلسطيني بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات: " للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة" والمادة 6 من قانون رقم 175 لسنة 2018 المصري بشأن مكافحة جرائم تقنية المعلومات: " لجهة التحقيق المختصة–بحسب الأحوال– أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين .... للبحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط".

الفرع الرابع: معيار مختلط يجمع عدة معايير في تحديد الطبيعة القانونية

ويستند أصحاب هذا الاتجاه إلى الجمع بين المعايير سالفة الذكر وهي الهدف من التفتيش والمرحلة التي يتم فيها وصفة القائم به[3]، ويعدّ إجراء التفتيش من إجراءات التحقيق عندما تقوم به السلطات المختصّة بالتحقيق الابتدائي وذلك بعد تحريك الدعوى الجزائية بهدف الكشف عن الحقيقة[4].

[1] للمزيد انظر المادة 55 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

[2] للمزيد انظر كل من المادة 70 و المادة 200 من قانون الاجراءات الجنائية المصري رقم 150 لسنة 1950.

[3] قدواري، ابراهيم: **التفتيش في قانون الاجراءات الجزائية الجزائري**، المرجع السابق، ص22.

[4] الحسيني، سامي حسني: **النظرية العامة للتفتيش**، مرجع سابق، ص55.

ترى الباحثة وبناءً على ما سبق فإن الاتجاه الأصح في تحديد الطبيعة القانونية للتفتيش في الجرائم الإلكترونية هو الاتجاه الرابع والذي يجمع بين عدة معايير واعتبر أن إجراء التفتيش هو عملاً من أعمال التحقيق والذي يكون بعد مباشرة الدعوى الجزائية وتحريكها من أجل تحقيق غرض محدد ألا وهو كشف الحقيقة.

المبحث الثاني: شروط التفتيش في الجرائم الإلكترونية

نظراً لخطورة إجراء التفتيش وكونه من إجراءات التحقيق التي تمسّ بالإنسان مباشرة وتنتهك حقوقه وحرياته ومستودع سره، فكان لا بدّ من أن يحاط هذا الإجراء بمجموعة من الشروط التي تضمن إجراؤه بالشكل الصحيح ولتحقيق الغاية منه بحيث لا يتم التعسف في إجرائه وعدم تجاوز حدوده، وحرصت الدساتير والقوانين الجزائية على ذلك ونصّت على مجموعة من الشروط الواجب توافرها عند إجراء التفتيش حتى يكون صحيحاً وهذه الشروط صنّفت إلى نوعين وهما شروط موضوعية وشروط شكلية، لذلك سنتعرف على هذه الشروط التي تحكم إجراء التفتيش من خلال تقسيم هذا المبحث إلى:-

المطلب الأول: الشروط الموضوعية للتفتيش في الجرائم الإلكترونية

المطلب الثاني: الشروط الشكلية للتفتيش في الجرائم الإلكترونية

المطلب الثالث: خصوصية التفتيش في الجرائم الإلكترونية العابرة للحدود

المطلب الأول: الشروط الموضوعية للتفتيش في الجرائم الإلكترونية

سنبحث في هذا المطلب كل من الشروط الموضوعية الواجب توافرها لإجراء التفتيش في الجرائم الإلكترونية، والتي تتمثل في: أ- وجوب توافر السبب لإجراء التفتيش ب- تحديد محل إجراء التفتيش.

الفرع الأول: وجوب توافر سبب إجراء التفتيش

ويقصد بالسبب في إجراء التفتيش هو الدافع أو المبرر الذي يدفع الجهة المختصة للقيام بإجراء التفتيش، ويعدّ سبب إجراء التفتيش من أهم الشروط الموضوعية التي وضعها المشرع وحرص على أن يكون إذن التفتيش الصّادر من السلطة المختصّة مسبباً[1]، ولا يمكن تحقيق هذا السبب إلا إذا وقعت جريمة إلكترونية وتم توجيه الاتهام إلى شخص أو مجموعة من الأشخاص بارتكابهم لهذه الجريمة وعلى أن تتوافر إمارات أو قرائن قوية على وجود محل الجريمة أو أدلة الجريمة المرتكبة لدى الشخص أو الأشخاص المراد تفتيشهم أو في المكان المتواجدين فيه، كما أنه يتوجب توافر غاية معينة أو هدف معيّن لإجراء التفتيش وتسعى الجهة المختصة إلى تحقيقه، ونبحث فيما يلي الأمور التي تؤدي لتحقيق السبب:

أولاً: وقوع جريمة إلكترونية

إنّ إجراءات التحقيق لا يمكن البدء فيها إلا بعد وقوع جريمة فعلاً، وبما أنّ إجراء التفتيش هو أحد إجراءات التحقيق الابتدائي فإنه لا يمكن القيام به لشخص معيّن أو لمكان محدد إلا إذا كانت هناك جريمة قد وقعت بالفعل سواء جناية أو جنحة وبالتالي لا يجوز إجراء التفتيش على جرائم لم تقع فعلاً وإنّما متوقع حدوثها مستقبلاً ولو تم إجراؤه فإنه يعتبر باطلاً وكل ما يترتب عليه من آثار أو نتائج تكون باطلة[2]؛ ويعود السبب في ذلك إلى أ- أنّ إجراء التفتيش ليس وسيلة للكشف عن الجرائم بل هو إجراء للبحث عن الأدلة لجريمة قد ارتكبت فعلاً. ب- أن الجريمة المستقبلية لا ينطوي عليها أي ضرر بالمجتمع كونها لم تنتج أي آثار بعد على أرض الواقع. ج- يمكن للجاني العدول عنها وبالتالي عدم وجود جريمة، ولهذا يعتبر شرط

---

[1] وهو ما أكدته المواد 2/52 من القرار بقانون رقم 10 لسنة 2018 الفلسطيني بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات: " يجب أن يكون أمر التفتيش مسبباً ومحدداً ...." و المادة 6 من قانون رقم 175 لسنة 2018 المصري بشأن مكافحة جرائم تقنية المعلومات: " لجهة التحقيق المختصة-بحسب الأحوال- أن تصدر أمراً مسبباً....، وفي كل الأحوال يجب أن يكون أمر جهة التحقيق المختصة مسبباً."

[2] الجوخدار، حسن: **التحقيق الابتدائي في قانون أصول المحاكمات الجزائية "دراسة مقارنة "**، عمّان-الأردن: دار الثقافة للنشر والتوزيع ، 2008، ص131+132.

وقوع الجريمة فعلياً من الضمانات التي تحصر سلطات الجهة المختصة بالتفتيش وتحمي حريات الأفراد وحقوقهم وعدم المساس فيها.

ويتعيّن إجراء التفتيش بشكل عام في الجرائم التي تكون من قبيل الجناية أو الجنحة بحيث لا يمكن إجراء التفتيش في المخالفات وذلك لأن المخالفات هي من الجرائم البسيطة فلا يمكن أن يتم انتهاك والمساس بحرية وحقوق الأشخاص من أجل جريمة بسيطة[1]، وعبّر عن ذلك كل من المشرع الفلسطيني والمشرع المصري وأكدا على أنه لا يمكن إجراء التفتيش إلا في الجنايات والجنح[2]، أما عن القوانين المتعلقة بالجرائم الإلكترونية فلم ينص المشرع الفلسطيني والمشرع المصري على أن التفتيش في الجرائم الإلكترونية فقط في الجنايات والجنح و**نرى** أنه يفهم ضمنياً عدم قيامهم بالنص على ذلك يعود إلى أنّ كافة الجرائم الإلكترونية الواردة في هذه القوانين هي من قبيل الجنايات والجنح وبالتالي لا ضرورة في ذكر ذلك لأن التفتيش في الجرائم الإلكترونية هو أحد أنواع التفتيش في الجرائم ولذلك هو خاضع حتماً للقواعد العامة التي تحكم إجراء التفتيش.

ثانياً: توجيه اتهام لشخص أو مجموعة من الأشخاص بارتكاب جريمة إلكترونية أو الاشتراك في ارتكابها

حتى تتمكّن الجهات المختصة بإجراء التفتيش من القيام به فإنه لا بدّ من توجيه اتهام جدّي لشخص أو مجموعة من الأشخاص بارتكاب جريمة إلكترونية أو الاشتراك فيها، وعلى أن تكون هناك أدلة كافية على أن المتهم يحوز لديه أو في مسكنه أشياء تتعلق بالجريمة لكي يتم توجيه الاتهام له وانتهاك حق خصوصيته وتفتيش مستودع سرّه كإجراء التفتيش لهاتفه المحمول أو جهاز الحاسوب[3]، ويقصد بالدلائل

---

[1] الجوخدار، حسن: **التحقيق الابتدائي في قانون أصول المحاكمات الجزائية**، مرجع سابق، ص132.

[2] مادة 1/39 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 ومادة91 من قانون الإجراءات الجنائية رقم 150 لسنة 1950.

[3] الطوالبة، علي حسن: **التفتيش الجنائي على نظم الحاسوب والانترنت "دراسة مقارنة"**، إربد– الأردن: عالم الكتب الحديث، 2004،ص70.

الكافية في الجرائم الإلكترونية" مجموعة من المظاهر أو الإمارات المعيّنة القائمة على العقل والمنطق والخبرة الفنيّة والحرفية للمحقق والتي ترجّح نسبة الجريمة الإلكترونية إلى شخص معيّن باعتباره فاعلاً أصلياً أو شريكاً"[1]، ويمكن الاستدلال على أهمية وجود اتهام موجّه إلى شخص حتى يتم تفتيشه بشكل قانوني من خلال نصوص المواد مادة 39 من قانون الإجراءات الجزائية الفلسطيني والمادة 91 من قانون الإجراءات الجنائية المصري، حيث أكدت هذه المواد على أن إجراء التفتيش لا يتم إلا بناءً على اتهام موجّه إلى شخص بارتكابه جناية أو جنحة أو باشتراكه في ارتكابها إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة، وبالتالي تعد الدلائل الكافية على وجود اتهام موجّه للشخص هو شرطاً مهماً لا يمكن مباشرة التفتيش دون وجوده كون أن إجراء التفتيش يمس بحق مستودع السر لدى الشخص، لذلك توافر هذه الدلائل يؤدي إلى القيام بالإجراء بشكلٍ قانوني وصحيح.

وقضت محكمة النقض المصرية في ذلك " إنّ كل ما يشترط لصحة التفتيش الذي تجريه النيابة العامة أو تأذن بإجرائه في مسكن المتهم هو أن يكون رجل الضبط القضائي قد علم من تحرياته واستدلالاته أن جريمة معيّنة جناية أو جنحة قد وقعت من شخص معيّن وأن يكون هناك من الدلائل والإمارات الكافية والشبهات المقبولة ضد هذا الشخص بقدر يبرر تعرض التحقيق لحرمة مسكنه التي كفلها الدستور وحرّم على رجال السلطة دخوله إلا في الأحوال التي ينصّ عليها القانون"[2].

ثالثاً: وجود دلائل قوية على وجود محل الجريمة لدى الشخص المتهم بارتكاب الجريمة

إذ لا يكفي أن تكون هناك جريمة واتهام موجّه لشخص معيّن بارتكابه لهذه الجريمة وإنما يجب أن تتوافر أدلة معيّنة وقوية وقرائن كافية على وجود لدى الشخص المتهم أو في المكان المراد تفتيشه الأدوات المستخدمة في الجريمة أو أشياء قد تحصلت عن الجريمة أو وجود مستندات إلكترونية قد تفيد في كشف الحقيقة، وتكون وسيلة الحصول على هذه الدلائل والقرائن من خلال التحريات الجديّة التي تتم من قبل

[1] براهيمي، جمال: **التحقيق الجنائي في الجرائم الإلكترونية** ، رسالة دكتوراة ، جامعة مولود معمري، الجزائر، 2018، ص34.

[2] نقض /جزاء مصري، رقم 5769 لسنة 60 قضائية/ جلسة 1999/3/11/ قاعدة رقم 37 / صفحة 195.

مأموري الضبط القضائي خلال مرحلة الاستدلال وتخضع جديّة هذه القرائن ومدى كفايتها وصدقها إلى تقدير السلطة المختصّة بإصدار إذن التفتيش وتحت رقابة محكمة الموضوع[1].

وترى الباحثة هنا على الرغم من أن القرائن والدلائل تمتاز بسهولة اتلافها وتغييرها وإخفاؤها مما يؤدي إلى صعوبة التوصل إليها من قبل سلطات التحري والاستدلال وبالتالي فقدان السبب الذي يدفع إلى إجراء التفتيش، إلا أن توافرها يعتبر ضروري لصحة إجراء التفتيش وذلك حتى يتسنّى متابعة الجريمة والتحديد بدقة لما يتوجب إجراء التفتيش عليه.

رابعاً: الغاية من إجراء التفتيش

حتى يتم إجراء التفتيش بشكل صحيح فإنه لا بد من أن يكون من وراءه هدف أو غرض معيّن لتحقيقه، ويتمثل هذا الغرض في ضبط الأشياء التي تتعلق بالجريمة المرتكبة أو تفيد في كشف الحقيقة، لذلك يقع باطلاً أي إجراء تفتيش يكون خلافاً لما حدده الشرع[2].

ويكمن الهدف من إجراء التفتيش بشكل عام إلى ضبط الأدلة المادية المتحصلة من الجريمة كالسلاح المستخدم مثلاً في جريمة القتل، أما الهدف من إجراء التفتيش في الجرائم الإلكترونية لا يقتصر فقط على ضبط الأدلة المادية وانما يكون أيضاً للحصول على الأدلة المعلوماتية والتي تكون عبارة عن معلومات وبيانات ومستندات إلكترونية.

كما أن الهدف من وراء البحث عن الأدلة هو التوصل إلى أدلة إثبات وأدلة نفي فإما تثبت الجريمة على المتهم أو تنفي التهمّة عنه[3].

---

[1] براهيمي، جمال : **التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق ، ص 35.

[2] حجازي، عبدالفتاح بيومي: **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت**، الاسكندرية – مصر: دار الفكر الجامعي، 2006 ص 358.

[3] حسين، سامي جلال فقي: **التفتيش في الجرائم المعلوماتية**، مرجع سابق، ص127.

وهنا ترى الباحثة أنه يتوجب أن يكون الهدف من إجراء التفتيش حقيقي ويمكن أن يفيد التحقيق، إذ لا بد من أن تكون إجراءات التحري والاستدلال جدّية ومفيدة بحيث تحدد بشكل دقيق الوسائل التكنولوجية والأجهزة الإلكترونية المراد إجراء التفتيش عليها، وبذلك يتم ضمان عدم انتهاك حرمة وحقوق الأشخاص إلا لضبط أشياء معيّنة وتتعلق بالجريمة بشكل أساسي وتكون ضرورية لإظهار وكشف الحقيقة.

الفرع الثاني: تحديد محل إجراء التفتيش

ويقصد بمحل التفتيش هو مستودع سر الإنسان الذي يحتفظ فيه بالأشياء التي تتعلق به وتخصّه، وقد يكون هذا المستودع إما الشخص نفسه أو في مكان تابع له كالمسكن أو المركبة أو في الوسائل التكنولوجية التي له، لذلك يجري التفتيش على كل ما يتعلق بالجريمة سواء الأشخاص المتهمين أو الأماكن التي يمكن أن تتواجد فيها الأجهزة الإلكترونية أو وسائل تكنولوجيا المعلومات ذاتها ويتم تفتيشها والتنقيب عن أدلة الجريمة فيها[1]، وتتشابه الجريمة الإلكترونية مع الجريمة العادية التقليدية من ناحية تفتيش الأشخاص والأماكن، فالسلطة المختصة عندما تقوم بالتنقيب والبحث عن الأدلة يمكن أن تقوم بتفتيش الأشخاص للبحث عن أدلة متعلقة بالجريمة وكذلك تفتيش الأماكن كتفتيش منزل المتهم أو مكتبه، وتختلف الجريمة الإلكترونية عن الجريمة التقليدية العادية بأن هذه الأخيرة يكون محل التفتيش فيها دائماً هو الأدلة المادية أما الجرائم الإلكترونية فلا يقتصر البحث والتنقيب فيها عن الأدلة المادية بل يتم أيضاً البحث عن الأدلة المعنوية كالبيانات والمعلومات[2]، لذلك تتمثل عناصر محل التفتيش في الجرائم الإلكترونية بالأشخاص والأماكن ووسائل تكنولوجيا المعلومات، وقبل الخوض في الحديث عن هذه العناصر فإنه لا بد من تبيان الشروط الأساسية الواجب توافرها في محل إجراء التفتيش.

---

[1] البغو، ابتسام: **اجراءات المتابعة الجزائية في الجريمة المعلوماتية**، رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي، الجزائر،2015-2016، ص13+14.

[2] عربوز، فاطمة الزهراء: *التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية*، **مركز جيل البحث العلمي**، العدد34/2019، ص106.

أولاً: شروط محل إجراء التفتيش

أ. **أن يكون المحل معيّناً:** إذ لا بدّ من أن يكون محل التفتيش معيّناً ومحدداً، بحيث يتم تحديد محل التفتيش بناءً على وجود دلائل وقرائن تثبت أن هذا المحل أو الشيء المراد تفتيشه هو يتصل بالجريمة المرتكبة وأن إجراء التفتيش سيؤدي إلى الكشف عن الحقيقة وضبط الأدلة المتحصلة عن الجريمة، ويمكن أن يكون هذا المحل شخص أو أشخاص متهمين أو مشتركين بالجريمة ودلّت القرائن على أنّ لهم علاقة بالجريمة وبحوزتهم أدلة تتعلق بالجريمة، أو يمكن أن يكون المحل هو مكان أو عدة أماكن وأثبتت أيضاً القرائن والدلائل على وجود أدلة الجريمة فيها[1]، أو يمكن أن يكون المحل وسائل تكنولوجيا المعلومات والتي تتضمن معلومات وبيانات مختلفة متعلقة بالجريمة، وبالتالي يجب تحديد وتعيين الشخص أو المكان أو الوسيلة تعييناً نافياً للجهالة.

لذلك لا يمكن إجراء التفتيش على شخص غير محدد أو شخص لم تثبت الدلائل على علاقته بالجريمة أو على حيازته لأدلة الجريمة، كما أنه لا يمكن إجراء التفتيش على أماكن عشوائية دون تحديد الأماكن المتعلقة بالجريمة، وأخيراً لا يمكن إجراء التفتيش على مختلف وسائل تكنولوجيا أو إجراء بحث عام عليها وعلى معلومات وبيانات وملفات عشوائية، وتعود العبرة من هذا المنع إلى حماية حق الخصوصية من الانتهاكات من قبل السلطات المختصة، لذا إنّ أي إجراء تفتيش لمحل غير محدد يكون هذا الإجراء وما ينتج عنه باطلاً.

[1] غانم، محمد علي مصطفى: **تفتيش المسكن في قانون الاجراءات الجزائية الفلسطيني**، مرجع سابق، ص72-74.

ب. أن يكون محل التفتيش مما يجوز تفتيشه: فكما نعلم أنه في حالة توافر شروط التفتيش فإنه يمكن إجراؤه على أي محل يتضمن أدلة تفيد في الكشف عن الحقيقة، إلا أنه هناك حالات معيّنة لا يمكن فيها إجراء التفتيش وهي إذا كان محل التفتيش يتمتع بحصانة معيّنة منحه إياها القانون مما تشكّل هذه الحصانة عقبة تقف أمام السلطات المختصّة بإجراء التفتيش[1]، وتتمثل هذه الحصانة في ثلاثة أنواع هي:

- الحصانة الدبلوماسية: يتمتع المبعوثون الدبلوماسيون في أشخاصهم وأماكن إقامتهم ومقار أعمالهم ومراسلاتهم بحصانة دبلوماسية بحيث تمنحهم هذه الحصانة بأنهم لا يخضعون للإجراءات الجنائية في إقليم الدولة التي يكونوا مبعوثين إليها وتقتصر هذه الحصانة فقط خلال الفترة التي يتمتع بها المبعوث الدبلوماسي بالصفة الدبلوماسية[2]، وتشمل هذه الحصانة ما يلي:
- مقر البعثة: وهي تلك المباني والمساكن التي تخصصها الدولة الموفدة لاستعمال البعثة الدبلوماسية ويتم فيها مباشرة البعثة الدبلوماسية لمهامها، ويتمتع هذا المقر بحصانة دبلوماسية تمنع اتخاذ أي إجراء بحقه سواء تفتيشه أو الحجز عليه أو الاستيلاء أو التنفيذ عليه، ولا تقتصر هذه الحصانة على المباني والمساكن التابعة للبعثة بل تمتد لتشمل حديقة مقر البعثة ومواقف السيارات ووسائل النقل التابعة لها أو التي تستأجرها وكافة ممتلكات مقر البعثة من منقولات وحسابات مصرفية ووثائق ومحفوظات[3]، وأكدت على هذه الحصانة اتفاقية فيينا للعلاقات الدبلوماسية ونصّت على ضرورة صون حرمة دار البعثة وعدم جواز دخول مأموري الضبط القضائي إلا برضاء رئيس البعثة ووجوب قيام

---

[1] الحسيني، سامي حسني: **النظرية العامة للتفتيش**، مرجع سابق، ص210.

[2] الحسيني، سامي حسني: **النظرية العامة للتفتيش**، مرجع سابق، ص210+211.

[3] حبيب، معن ابراهيم جبّار: **الحصانات الخاصة لمقر البعثة الدبلوماسية والاستثناءات الواردة عليها في ضوء اتفاقية فيينا**، رسالة ماجستير، عمّان– الأردن: جامعة الشرق الأوسط ، 2012، ص33.

الدولة المستقبلة باتخاذ كافة وسائل الحماية والتدابير اللازمة للحفاظ على دار البعثة وعدم التعرض لها أو المساس بها[1].

- الحصانة الشخصية: وتعد الحصانة الشخصية التي يتمتع بها المبعوث الدبلوماسي من أهم الحصانات، فهي الأساس الجوهري الذي انبثقت عنه الامتيازات والحصانات الدبلوماسية المختلفة وتتمثل هذه الحصانة بمنع اتخاذ أي إجراء ماسّ بالمبعوث الدبلوماسي إذ لا يجوز إجراء القبض عليه أو إجراء تفتيشه أو حجزه، فأي إجراء يتم اتخاذه بحقه يعتبر اعتداء على سيادة الدولة التي يمثلها المبعوث الدبلوماسي وعلى الدولة المستقبلة للمبعوث أن تتخذ كافة الوسائل التي تحمي المبعوث وتضمن حريته وتحافظ على حياته[2]، وقد أكدت اتفاقية فيينا للعلاقات الدبلوماسية على ذلك في المادة 29: " تكون حرمة المبعوث الدبلوماسي مصونة ولا يجوز إخضاعه لأية صورة من صور القبض أو الاعتقال ويجب على الدولة المعتمد لديها معاملته بالاحترام اللائق واتخاذ جميع التدابير المناسبة لمنع أي اعتداء على شخصه أو حريته أو كرامته".

[1] مادة 22 من اتفاقية فيينا للعلاقات الدبلوماسية : "1- تكون حرمة دار البعثة مصونة ولا يجوز لمأموري الدولة المعتمد لديها دخولها إلا برضى رئيس البعثة.2-يترتب على الدولة المعتمد لديها التزام خاص باتخاذ جميع التدابير المناسبة لحماية دار البعثة من أي اقتحام أو ضرر ومنع أي إخلال بأمن البعثة أو مساس بكرامتها. 3-تعفى دار البعثة و أثاثها وأموالها الأخرى الموجودة فيها ووسائل النقل التابعة لها من إجراءات التفتيش أو الاستيلاء أو الحجز أو التنفيذ". والمادة24 من ذات الاتفاقية: " تكون حرمة محفوظات البعثة ووثائقها مصونة دائماً أياً كان مكانها".

[2] الزبن، هايل صالح: **الأساس القانوني لمنح الحصانات والامتيازات الدبلوماسية** ، رسالة ماجستير، جامعة الشرق الأوسط، عمّان-الأردن، 2011، ص 51.

وتمتد الحصانة الشخصية لتشمل أيضاً مسكن المبعوث الدبلوماسي الخاص[1] ومحل إقامته المؤقت وأمتعته الشخصية[2] وكذلك أفراد أسرته الذين يقيمون معه في المسكن ذاته بشرط ألا يكونوا من رعايا الدولة المستقبلة[3].

- حصانة المراسلات: تتمتع المراسلات بحصانة دبلوماسية مطلقة لا تقل أهمية عن الحصانة التي تتمتع بها المحفوظات والوثائق الموجودة في مقر البعثة الدبلوماسية، وتعود الأهمية في ذلك إلى تسهيل مهام المبعوث الدبلوماسي ووظائفه، لهذا فإن حصانة هذه المراسلات تمنع إجراء التفتيش عليها سواء في الدولة المستقبلة للمبعوث الدبلوماسي أو في الدولة الثالثة التي تمر المراسلات في أراضيها[4]، لذا فإن حرمة جميع المراسلات الرسمية المتعلقة بالبعثة ووظائفها تكون مصونة، وتشمل هذه المراسلات كافة الاتصالات والرسل الدبلوماسيون والرسائل المرسلة بالرموز والشيفرة وكذلك الحقيبة الدبلوماسية التي لا يجوز فتحها أو حجزها[5].

ويقع على عاتق الدولة المعتمد لديها المبعوث الدبلوماسي السماح للبعثة بحرية الاتصال لجميع الأغراض الرسمية وتصون هذه الحرية، كما وتعمل على حماية المبعوث الذي يتمتع بالحصانة أثناء قيامه بوظيفته وعلى أن يكون مزوداً بوثيقة رسمية تبين مركزه وتحدد الطرود التي تتألف منها الحقيبة الدبلوماسية[6].

---

[1] مادة 1/30 " يتمتع المنزل الخاص الذي يقطنه المبعوث الدبلوماسي بذات الحصانة والحماية التي يتمتع بهما دار البعثة".

[2] مادة 2/36 " تعفى الأمتعة الشخصية للمبعوث الدبلوماسي من التفتيش ما لم توجد أسباب تدعو إلى الافتراض بأنها تحتوي مواد لا تشملها الاعفاءات المنصوص عليها في الفقرة 1 من هذه المادة أو مواد يحظر القانون استيرادها أو تصديرها أو مواد تخضع لأنظمة الحجر الصحي في الدولة المعتمدة لديها ولا يجوز إجراء التفتيش إلا بحضور المبعوث الدبلوماسي أو ممثله أو مفوضه".

[3] مادة 1/37 من اتفاقية فيينا للعلاقات الدبلوماسية.

[4] أحمد، إيناس محمد: *الحماية الجنائية للبعثات الدبلوماسية*، **مجلة جامعة تكريت للحقوق**، العراق، مجلد1، العدد2017/2، ص187+188.

[5] مادة 27 من اتفاقية فيينا للعلاقات الدبلوماسية.

[6] مادة 27 من اتفاقية فيينا للعلاقات الدبلوماسية.

وعلى الرغم من تمتع البعثة الدبلوماسية بالحصانة التي تمنع الجهات المختصة من اتخاذ الإجراءات الجنائية بحقها، إلا أنّ ذلك لا يسمح للبعثة بمخالفة قوانين وأنظمة الدولة المستقبلة بل عليها احترام القوانين ومباشرة وظائفها بشكل قانوني وسليم، فلا يجوز لها استغلال واستخدام مقر البعثة أو المساكن الخاصّة بالبعثة لأغراض غير مشروعة وتؤثر على أمن واستقرار الدولة المستقبلة لها، وفي المقابل يقع على عاتق الدولة المستقبلة اتخاذ كافة الإجراءات والتسهيلات التي من شأنها تسهّل عمل البعثة ومباشرتها لوظائفها وكذلك العمل على حماية وصون البعثة من أي تعرض أو اعتداء عليها.

- الحصانة البرلمانية: وهي الحصانة المقررة لأعضاء البرلمان بحيث يتمتعوا بنوعين من الحصانة وهما: الحصانة المطلقة والتي تتعلق بكافة الآراء والأفكار التي يتم إبداؤها أثناء أعمالهم التشريعية والرقابية، وحصانة نسبية تتعلق بالجرائم التي يرتكبونها خلال أدوار انعقاد جلسات المجلس بحيث لا يمكن ملاحقتهم إلا بعد الحصول على إذن من المجلس التشريعي، أما فيما يتعلق بالجرائم التي يتم ارتكابها خارج أدوار انعقاد المجلس أو تم إلقاء القبض على عضو البرلمان متلبساً في الجريمة فيكفي إخطار المجلس ولا حاجة للحصول على إذن لملاحقة العضو، لذا تتمثل الحصانة البرلمانية لعضو البرلمان بعدم جواز إلقاء القبض عليه أو توقيفه أو إجراء تفتيشه جسمانياً أو لمنزله أو لمكتبه أو لمركبته أو رسائله أو التنصّت على مكالماته[1]، و أي إجراء يتم اتخاذه دون الحصول على إذن المجلس يعتبر هذا الإجراء باطلاً ولا يمكن تصحيحه.

ويكمن الهدف من الحصانة البرلمانية إلى وضع أعضاء البرلمان تحت الحماية خشيةً من أن تتخذ السلطة التنفيذية ضدهم إجراءات كيدية، لذلك تحرص مختلف الدساتير على تقرير حصانة لأعضاء البرلمان حتى تضمن لهم ممارسة أعمالهم بحرية[2]، وتأكيداً على ذلك فقد نص المشرع الفلسطيني على: " لا يجوز

[1] عبدالباقي، مصطفى: **شرح قانون الإجراءات الجزائية الفلسطيني**، بيرزيت–فلسطين: وحدة البحث العلمي والنشر كلية الحقوق والإدارة العامة، 2015، ص109+110.

[2] الحسيني، سامي حسني: **النظرية العامة للتفتيش**، مرجع سابق، ص113+114.

التعرض لعضو المجلس التشريعي بأي شكل من الأشكال ولا يجوز إجراء أي تفتيش في أمتعته أو بيته أو محل إقامته أو سيارته أو مكتبه وبصفة عامة أي عقار أو منقول خاص به طيلة مدة الحصانة"[1]، وكذلك المشرع المصري على: "لا يجوز في غير حالة التلبس بالجريمة اتخاذ أي إجراء جنائي ضد عضو مجلس النواب في مواد الجنايات والجنح إلا بإذن سابق من المجلس وفي غير دور الانعقاد يتعين أخذ إذن مكتب المجلس ويخطر المجلس عند أول انعقاد بما اتخذ من إجراء وفي كل الأحوال يتعين البت في طلب اتخاذ الإجراء الجنائي ضد العضو خلال ثلاثين يوماً على الأكثر وإلا عد الطلب مقبولاً"[2].

وتمتاز الحصانة البرلمانية المقررة لأعضاء البرلمان بعدة خصائص لعل أهمها:1- أنها محددة المدة تسري فقط خلال فترة اشغاله لمنصب عضو في البرلمان.2- تعد من النظام العام بحيث لا يجوز التنازل عنها.3- مقررة لحماية عضو البرلمان من اتخاذ أي إجراء بحقه قد يمس به كإجراء التفتيش والقبض والضبط. 4- أنها حصانة شخصية تقتصر على عضو البرلمان فقط فلا تمتد إلى أفراد عائلته.5- حصانة تتعلق بالإجراءات الجنائية بالتالي لا مانع من إقامة دعوى مدنية ضد عضو البرلمان.[3]

وترى الباحثة هنا أنه على الرغم من أن أعضاء البرلمان يتمتعون بحصانة برلمانية ضد الإجراءات الجنائية، إلا أنه لا يجري ذلك على الإطلاق أي على كافة الإجراءات إذ إن الإجراءات الجنائية تقسم إلى إجراءات ماسّة بالشخص كالتفتيش والقبض وإجراءات أخرى غير ماسّة كسماع الشهود وإجراءات المعاينة، لذلك فإنهم يتمتعون بالحصانة ضد الإجراءات الماسّة فقط أما الإجراءات غير الماسّة فيمكن للجهات المختصة بالتحقيق اتخاذها ضد أعضاء البرلمان.

---

[1] مادة 2/53 من القانون الأساسي الفلسطيني المعدّل لسنة 2003.

[2] مادة 113 من الدستور المصري لسنة 2014 والمعدّل لسنة 2019.

[3] شكر، نجيب: *الحصانة البرلمانية ضد الإجراءات الجنائية*، **مجلة المحقق الحلي للعلوم القانونية والسياسة**، ع1/السنة الخامسة، ص224.

- الحصانة القضائية: وهي الحصانة المقررة للقضاة ضد الإجراءات الجنائية، وعمل كل من المشرع الفلسطيني والمشرع المصري على التفرقة بين ما إذا كانت متلبس بها أم لا، ففي حالة تلبس القاضي بجريمة ما سواء أكانت جناية أو جنحة فإن القانون أجاز للنائب العام أن يأمر بالقبض على القاضي أو أن يقوم بحبسه احتياطياً ولكن حتى يتسنى له اتخاذ هذا الإجراء يجب عليه أن يرفع الأمر إلى مجلس القضاء الأعلى خلال 24 ساعة من تنفيذ الأمر، أما إذا كانت الجريمة غير متلبس بها فإنه لا يجوز إجراء القبض على القاضي أو حبسه إلا بعد الحصول على إذن من مجلس القضاء الأعلى.

لذلك فإن أي إجراء من إجراءات التحقيق الماسّة بالشخص كإجراء التفتيش لشخصه ولمسكنه فإنه لا يجوز اتخاذها بحق القاضي إلا بعد الحصول على إذن من مجلس القضاء الأعلى وبناءً على طلب من النائب العام، أما فيما يتعلق بالإجراءات الجنائية الأخرى والتي تكون غير ماسّة بالشخص كإجراء المعاينة يمكن اتخاذها بحق القاضي دون الحاجة إلى الحصول على إذن من مجلس القضاء الأعلى[1].

ثانياً: العناصر التي تكون محلاً لإجراء التفتيش

أ. **تفتيش الأشخاص:** ويقصد بالشخص كمحل للتفتيش بأنه كل ما يتعلق بالشخص وما يتصل به، إذ يجري التفتيش على جسمه وملابسه وأمتعته التي في حوزته، وتستمد هذه الأشياء حرمتها من كونها في حيازة الشخص حتى لو لم تكن هذه الأشياء مُلكه، ولا يشترط في هذه الأمتعة أن تكون في يد المتهم وقت تفتيشها بل يمكن تفتيشها أثناء تواجدها أمامه طالما ظاهر الحال لا يوحي بتخليه عنها، وقد تأخذ هذه الأمتعة أشكالاً متعددة لا حصر لها ومنها أن تكون حقيبة أو صندوق[2].

[1] عبدالمطلب، إيهاب: **تفتيش الأشخاص والأماكن**، الطبعة الأولى، مصر: المركز القومي للإصدارات القانونية ، 2009، ص224.

[2] اليماحي، عبدالله راشد سعيد: **اجراءات تفتيش وضبط نظم الحاسب الآلي والإنترنت**، رسالة ماجستير، أكاديمية شرطة دبي، 2014، ص89.

وقد يكون هذا الشخص المتهم المراد تفتيشه شخصاً عادياً لا يمتلك أدنى خبرة في الأجهزة الإلكترونية ولكنه يمتلك إحدى هذه الأجهزة كالهاتف المحمول مثلاً ويقوم بإساءة استخدامه ويرتكب جريمة ما، كما أنه يمكن أن يكون هذا الشخص لديه خبرة واسعة وعلى علم ودراية تامة بالأجهزة الإلكترونية والتقنيات المختلفة كأن يكون مختص أو خبير.

ويجري التفتيش لإيجاد أي دليل يتعلق بالجريمة من خلال البحث والتنقيب والفحص للشخص ولملابسه وما يحمل من أمتعة كأكياس أو حقائب وغيرها من الأشياء، وقد يكون البحث حول جهاز الحاسوب أو هاتف محمول أو فلاشة أو ذاكرة تتضمن بيانات ومعلومات متعلقة بالجريمة[1]، وفيما يتعلق بمركبة هذا الشخص فلم ينظم المشرع الجزائي أحكام تفتيش المركبات، مما خلق جدلاً فقهياً في ذلك وثار خلاف حول اعتبارها من أمتعة الشخص أم لا، لذا انقسمت في ذلك الآراء وسنقوم بتوضيحها فيما يلي:

ويقصد بتفتيش المركبة أو فحصها بأنه: " المعاينة المشروطة للمناطق التي يمكن الوصول إليها داخل المركبة وخارجها أو أي وسيلة نقل أخرى بما فيها مقصورتا السائق والركاب ومقصورة التابلوه والمقصورات الأخرى والصندوق"[2].

أ. تفتيش المركبات الخاصة للشخص: فقد انقسمت الآراء في ذلك:

1. فمنهم من اعتبر أن المركبة تتمتع بحرمة المسكن سواء أكانت هذه المركبة داخل المسكن أم خارجها[3].
2. ومنهم من فرّق فيما إذا كانت المركبة الخاصة في الطريق العام أم في ساحة المسكن أو محيطه، فإذا كانت المركبة الخاصة في الطريق العام أو في حوزة صاحبها وهو من يقودها فهنا يتم معاملتها بذات

[1] الطوالبة، علي حسن محمد: **التفتيش الجنائي على نظم الحاسوب والإنترنت**، مرجع سابق، ص78+79.

[2] مادة 126 من القوانين النموذجية للإجراءات الجنائية.

[3] الحسيني، سامي حسني: **النظرية العامة للتفتيش**، مرجع سابق، ص235.

المعاملة التي تتم على الشخص فتأخذ حكم تفتيش الأشخاص[1]، وعندما يتم إجراء التفتيش على الشخص يتم تفتيش مركبته ولكن بشرط أن يكون التفتيش بموجب إذن صادر من السلطة المختصة بالتفتيش، وقد أكد على ذلك الحكم الصادر من محكمة النقض المصرية "عدم جواز تفتيش السيارات الخاصة بالطرق العامة بغير إذن"[2]، أما إذا كانت المركبة الخاصة واقفة في محيط المسكن فإنها تأخذ حكمه ويكون لها حرمة المسكن ويتم اتباع كافة القواعد المنصوص عليها لإجراء التفتيش على المسكن[3]، وتكون المركبة مشمولة بذات الحماية القانونية بشقيها الموضوعي والإجرائي[4].

3. وفيما يتعلق بتخلي الشخص عن مركبته الخاصة وليست بحوزته وكان ظاهر الحال يشير إلى تخليه عنها بمحض إرادته واختياره، فهنا لا تأخذ حكم تفتيش المسكن ولا حكم تفتيش الأشخاص، بالتالي يمكن لمأمور الضبط القضائي إجراء التفتيش عليها، وقضت في ذلك محكمة النقض المصرية بجواز إجراء التفتيش بدون إذن صادر عن الجهة المختصة فيما إذا كانت المركبة خالية وكان ظاهر الحال أن صاحبها قد تخلى عنها[5].

ب. تفتيش المركبات العامة: وهي المركبات التي لا يمكن اعتبارها في حيازة السائق أو أنها تابعة له[6] مثل القطارات والباصات، فهذا النوع من المركبات يتم معاملته معاملة المحال العامة بحيث لا يجوز إجراء التفتيش عليها إلا في حالات التلبس بالجريمة.

---

[1] الوليد، ساهر إبراهيم شكري: **شرح قانون الإجراءات الجزائية الفلسطيني**، الطبعة الأولى، غزة–فلسطين: بدون ناشر، 2012، ص372+373.

[2] نقض/جزاء مصري رقم 6042 لسنة 81 قضائية الصادر بجلسة 2012/1/23.

[3] الوليد، ساهر إبراهيم شكري، **شرح قانون الاجراءات الجزائية الفلسطيني**، مرجع سابق، ص 373.

[4] زواوي، شنة: *أحكام تفتيش المساكن والأشخاص والمركبات في القانون بين النظرية والتطبيق*، **مجلة الاجتهاد للدراسات القانونية والاقتصادية**، مجلد7، العدد2/لسنة2018، ص154.

[5] نقض/جزاء مصري رقم 17523/ لسنة 85 قضائية والصادر بجلسة 2017/1/24:" عدم جواز تفتيش السيارات الخاصة بالطرق العامة بغير إذن وفي غير حالات التلبس إذا كانت خالية وكان ظاهر الحال قد تخلى صاحبها عنها".

[6] الحسيني، سامي حسني: **النظرية العامة للتفتيش**، مرجع سابق، ص235.

ج. تفتيش مركبات الأجرة: تعتبر هذه المركبات في حيازة سائقها وركابها وبالتالي يمكن إجراء التفتيش عليها طالما أن أحدهم يجوز تفتيشه وكان في حالة تلبس بالجريمة، ويتم اتباع حينئذٍ قواعد تفتيش الأشخاص عليها[1].

وعمل المشرع (الفلسطيني والمصري) على إقرار عدة ضمانات عند تفتيش الشخص سواء أكان هذا الشخص متهماً أم غير متهم وتتمثل هذه الضمانات على النحو الآتي:

1. تفتيش الشخص المتهم: فإما أن يكون هذا الشخص قد تم القبض عليه أو يكون في حالة تلبس، فإذا كان قد قبض عليه بموجب أمر قبض صادر بحقه لوجود دلائل كافية على اتهامه بارتكابه لجريمة جناية أو جنحة[2]، جاز لمأمور الضبط القضائي تفتيشه والبحث عمّا لديه من أدلة تتعلق بالجريمة الإلكترونية المرتكبة[3]، أما في حالة التلبس فقد نصّ المشرع (الفلسطيني والمصري)[4] على الحالات التي يكون فيها تلبس وبالتالي يتم إلقاء القبض على المتهم فيها دون الحاجة إلى أمر صادر من الجهات المختصة وتتمثل هذه الحالات فيما يلي:

أ. في حالة ارتكاب الجريمة أو عقب ارتكابها في فترة وجيزة.

ب. إذا قام المجني عليه باتباع الجاني واللحاق به أو تبعته العامة بصراخ وصخب على أثر وقوع الجريمة.

---

[1] الوليد، ساهر إبراهيم شكري : **شرح قانون الاجراءات الجزائية الفلسطيني**، مرجع سابق، ص374.

[2] مادة 2/31 من قانون الإجراءات الجزائية الفلسطيني رقم 3لسنة 2001ومادة35 من قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950.

[3] المادة1/38 من قانون الإجراءات الجزائية الفلسطيني رقم3 لسنة 2001 ومادة46 من قانون الإجراءات الجنائية المصري رقم150 لسنة 1950.

[4] مادة 26 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 ومادة 30 من قانون الاجراءات الجنائية المصري رقم 150 لسنة 1950.

ج. إذا وجد مرتكب الجريمة بعد وقوعها حاملاً لآلات أو أسلحة أو أمتعة أو أوراق أو أي شيء آخر وتم الاستدلال من خلاله على أنه هو فاعل أو شريك في الجريمة أو كان على هذا المرتكب دلالات وآثار تفيد بارتكابه للجريمة.

وفي حالة توافر إحدى هذه الحالات وجرى إلقاء القبض على المتهم فإنه يعتبر قبضاً صحيحاً، ويمكن لمأمور الضبط القضائي حينها إجراء التفتيش عليه.

ويثور السؤال هنا حول إمكانية وجود حالة تلبس في الجرائم الإلكترونية؟

بالتطبيق على حالات التلبس سالفة الذكر فيمكن تصّور حدوث جرائم إلكترونية متلبس بها وذلك من خلال:

أ. ففي الحالة الأولى إما أن يتم رؤية المتهم أثناء ارتكابه للجريمة الإلكترونية لكنها تعتبر حالة نادرة جداً، ومن الأمثلة عليها أن يكون مأمور الضبط القضائي متواجد في أحد مقاهي الإنترنت ويشاهد أحد المستخدمين لأجهزة الحاسوب يقوم بتحميل صور إباحية وطباعتها[1]، أو يمكن مشاهدة الجريمة بعد فترة وجيزة من ارتكابها وتفترض هذه الحالة أن مأمور الضبط القضائي لم يشاهد الجريمة وقت ارتكابها بل شاهد آثار الجريمة أو عاين بداية نتائج الجريمة[2]ولعلّ أصدق مثال على هذه الحالة وهو إذا ضبط المتهم أثناء تواجده داخل نظام معلوماتي لا يسمح له بالدخول إليه بقصد اختراقه وإلحاق الضرر به وبالمعلومات المخزنة عليه إما بإتلافها أو تغييرها أو الإضافة عليها أو بأي وسيلة ممكنة تلحق الضرر بهذا النظام.

---

[1] فضل، سليمان أحمد: **المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)**، القاهرة–مصر: دار النهضة العربية، 2012،ص294.

[2] ابراهيم، محمد فوزي: *دور مأمور الضبط القضائي في الحصول على الدليل الإلكتروني*، **مجلة البحوث القانونية والاقتصادية**، الشارقة، العدد66/اغسطس/ 2018، ص93.

ب. أما في الحالة الثانية من حالات التلبس فهذه الحالة تختلف في الجرائم الإلكترونية عن الجرائم التقليدية العاديّة كون أن الجرائم الإلكترونية تعتمد في ارتكابها على الأجهزة الإلكترونية بشكل أساسي، ففي الجريمة العادية يتم اللحاق واتباع الجاني سيراً على الأقدام أما في الجريمة الإلكترونية يتم تتبع حسابات الجاني وحتى تتضح الصورة أكثر نعطي هذا المثال وهو قيام شخص بإنشاء حساب إلكتروني أو موقع إلكتروني ويقوم بنشر فيديوهات مخلة بالآداب أو معلومات مغلوطة أو نشر شائعات تلحق الضرر بأشخاص معينين فبالتالي إذا كشف عن هويته أو تم بإحدى الطرق التعرّف عليه وتم نشر صوره أو مكان تواجده، فإن هذا الأمر يجعل كل شخص قد تضرر منه أو الناس كافة بتتبعه وتطالب بإلقاء القبض عليه[1] وبهذا تكون تطبقت الحالة الثانية رغم اختلاف وسيلة التتبع واللحاق بالجاني.

ج. أما الحالة الثالثة ففيها يتم مشاهدة الجاني في وقت قريب من الجريمة حاملاً أدوات أو به آثار تفيد على أنه هو مرتكب للجريمة، كأن يتم مشاهدة المتهم حاملاً اسطوانات تحتوي على فيديوهات مخلة بالآداب أو صور إباحية مطبوعة كان قد حمّلها عن الإنترنت[2]، أو مشاهدة مأمور الضبط القضائي لشخص يحمل أدوات تقنية تثير الشك والريبة فيه وكان قد استخدمها أمام أجهزة الصرّاف الآلي بطريقة مختلفة عن الطرق العادية المتبعة في سحب النقود[3].

---

[1] كمال، صابر: *التلبس في الجريمة المعلوماتية*، **مقال منشور في مجلة القانون والأعمال الدولية–جامعة الحسن الأول–، المغرب**، 2019.

[2] فضل، سليمان أحمد: **المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)**، مرجع سابق، ص296.

[3] الشعّار، خالد علي نزّال: **التحقيق الجنائي في الجرائم الإلكترونية**، رسالة دكتوراة، جامعة المنصورة–مصر، ص31.

2. تفتيش الشخص غير المتهم: ويقصد به هو ذلك الشخص الذي يتواجد في المكان الذي يجري تفتيشه وتم الاشتباه فيه بأنه يخفي شيئاً مما يجري البحث والتفتيش عنه بالتالي يجوز لمأمور الضبط القضائي أو القائم بإجراء التفتيش أن يقوم بتفتيشه[1]، ولكن المشرع المصري هنا أكد على أنه لا يكفي مجرد الاشتباه بالشخص غير المتهم حتى يتم تفتيشه وإنّما يجب أن يكون هناك إمارات قوية تدل على أنه حائز لأشياء تتعلق بالجريمة[2].

3. تفتيش الأنثى: أقرّ المشرع للأنثى سواء أكانت متهمة أم غير متهمة ضمانات عند إجراء التفتيش عليها، بحيث لا يمكن إجراء التفتيش على الأنثى إلا من قبل أنثى يتم انتدابها من قبل الجهات المختصة بالتفتيش[3]، ويقع باطلاً إجراء التفتيش إذا لم يتم من قبل أنثى[4].

ب. **تفتيش الأماكن:** وتقسم هذه الأماكن إلى: 1- الأماكن العامة: ويقصد بها " كل طريق عام وكل مكان أو ممر يباح للجمهور المرور به أو الدخول إليه في كل وقت وبغير قيد أو كان مقيداً بدفع مبلغ من النقود وكل بناء أو مكان يستعمل إذ ذاك لأي اجتماع أو حفل عمومي أو ديني أو كساحة مكشوفة "[5] ومن الأمثلة على هذه الأماكن المدارس والجامعات والمستشفيات، وفيما يتعلق بإجراء التفتيش عليها فإنها لا تحتاج إلى إذن مسبق للقيام بتفتيشها؛ ويعود السبب في ذلك إلى أن المشرع لم يقرّ لها حرمة وحماية وبالتالي يمكن للجهات المختصّة القيام بإجراء التفتيش عليها[6]، ويمكن اعتبار المواقع

---

[1] مادة 44 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 ومادة 49 من قانون الاجراءات الجنائية المصري رقم 150 لسنة 1950.

[2] مادة 206 من قانون الاجراءات الجنائية المصري رقم 150 لسنة 1950.

[3] مادة 47 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 ومادة 46 من قانون الاجراءات الجنائية المصري رقم 150 لسنة 1950.

[4] انظر المادة 52 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

[5] انظر المادة 2 من قانون العقوبات الفلسطيني رقم 16 لسنة 1960.

[6] خلف، مازن: **المحاضرة الثامنة عشر بعنوان "تنفيذ التفتيش والبيانات التي يتضمنها أمر التفتيش"** ، الجامعة المستنصرية : العراق ، 2015-2017 ، ص1.

الإلكترونية المفتوحة لكافة الناس والتي يمكن للعامة دخولها كالأماكن العامة، لذلك يمكن للجهات المختصة إجراء التفتيش عليها دون الحاجة إلى إصدار إذن لتفتيشها[1].

2. الأماكن الخاصة: وتتمثل في:

أ- الأماكن التي تكون مسكونة أو معدّة للسكن والتي تتمتع بحرمة خاصّة أقرّها المشرع لها، وهذه الأماكن تحتاج إلى إذن مسبق من قبل الجهات المختصة للقيام بتفتيشها، كما وأقرّ عدة ضمانات يجب مراعاتها عند إجراء التفتيش عليها[2]، ويجري تفتيش هذه الأماكن للبحث والتنقيب عن وسائل تكنولوجية متعلقة بالجريمة الإلكترونية كالهاتف النقّال أو الحاسوب أو أقراص تخزين المعلومات ومن ثم ضبط هذه الوسائل والتحفظ عليها.

ب- الأماكن المخصصة لممارسة وظيفة الشخص كمكاتب المحامين أو عيادات الأطباء فهذه الأماكن يجوز للسلطات المختصة إجراء التفتيش عليها وذلك بعد الحصول على إذن مسبق للتفتيش عليها، وتحتاج بعض هذه الأماكن إلى إجراءات خاصة عند تفتيشها فمثلاً عند تفتيش مكاتب المحامين يتطلب عند إجرائه حضور نقيب المحامين أو من يمثله[3] .

---

[1] يمكن الاستدلال على ذلك من خلال ما ورد في الاتفاقية العربية لمكافحة جرائم تقنية الإنترنت في المادة 40 حيث سمحت للجهات المختصة الوصول إلى معلومات مخزنة ومتوافرة للعامة وبالتالي تكون على مصدر مفتوح وبغض النظر عن مكان وجود الموقع المخزنة عليه حتى لو كانت خارج الحدود الإقليمية للدولة فيمكن لها النفاذ إلى هذا المصدر والتفتيش على المعلومات، لذلك طالما سمحت الاتفاقية لأي دولة طرف أن تقوم بذلك دون الحصول على تفويض أو إنابة من الدولة الموجود لديها المصدر المفتوح، فإنه من باب أولى يمكن للجهات المختصة في الدولة أن تقوم بإجراء التفتيش على المواقع الإلكترونية أو المصادر المفتوحة الموجودة لديها دون الحاجة إصدار إذن التفتيش في ذلك.

[2] خلف، مازن: **تنفيذ التفتيش**، مرجع سابق، ص1.

[3] انظر المادة 20 من قانون المحامين النظاميين الفلسطيني المعدل رقم 3لسنة 1999، والمادة 51 من قانون المحامين المصري المعدل رقم 17 لسنة 1983.

وهناك بعض الأماكن التي يمكن أن تأخذ خصوصية على الرغم من تواجدها في أماكن مسموح دخولها للعامة كالمتاجر مثلاً والتي يجوز لمأموري الضبط القضائي الدخول إليها دون الحاجة إلى إذن بذلك، لكنّها إذا أرادت إجراء التفتيش على الخزنة أو الأرفف والجوارير للمكتب فإنه لا يجوز إجراء التفتيش عليها إلا بإذن مسبق صادر عن الجهات المختصة[1].

ج- **تفتيش وسائل تكنولوجيا المعلومات:** ويقصد بوسائل تكنولوجيا المعلومات وفقاً للقانون الفلسطيني بأنها" أي وسيلة إلكترونية مغناطيسية بصرية كهروكيميائية أو أي وسيلة أخرى سواء أكانت مادية أم غير مادية أو مجموعة وسائل مترابطة أو غير مترابطة تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية وتشمل أي قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الوسيلة"[2]، أما في القانون المصري والتي أطلق عليها مسمى تقنية المعلومات فقد عرّفها " هي أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تستخدم لتخزين واسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل المعلومات أو البيانات ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكياً أو لا سلكياً"[3]،ومن الأمثلة على هذه الوسائل: البريد الإلكتروني، أقراص، ذاكرات لتخزين المعلومات والبيانات، أجهزة الحواسيب، الهواتف النقالة، البرامج، المواقع الإلكترونية، المستندات الإلكترونية، الشبكات الإلكترونية والسجلات الإلكترونية.

ويجري تفتيش هذه الوسائل بعد الحصول على إذن مسبق ويكون مسبباً ومحدداً إذ يسمح بالنفاذ المباشر والولوج إلى هذه الوسائل من قبل مأموري الضبط القضائي أو من يتم الاستعانة بهم من أهل الخبرة[4]، ولعلّ السبب في اشتراط أن يكون هناك إذن مسبق مسبب ومحدد لما سيجري عليه التفتيش هو حماية

---

[1] الشهاوي، قدري عبدالفتاح: **مناط التفتيش**، مرجع سابق، ص47.

[2] انظر المادة 1 من القرار بقانون الفلسطيني رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[3] انظر المادة 1 من قانون جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 .

[4] انظر المادة 52 من القرار بقانون الفلسطيني رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات والمادة 6 من قانون جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.

خصوصية الشخص المراد تفتيش وسائل التكنولوجيا الخاصة به، بحيث لا يتم تفتيشها جميعاً وخرق خصوصيته وإنّما يكون إجراء التفتيش فقط على الجزئية المتعلقة بالجريمة، وفيما يتعلق بالوسائل التكنولوجية التي تكون لأنثى فإن المشرع (الفلسطيني والمصري) لم ينصّ على قواعد تفتيش الوسائل التكنولوجية المتعلقة بأنثى، لذا **نرى هنا** أنه من المستحسن أن نعود إلى القواعد العامة الواردة في قانون الإجراءات الجزائية والتي تنص على أن تفتيش الأنثى لا يتم إلا من قبل أنثى فبتالي إذا كانت هذه الوسائل تتعلق بأنثى أن يتم إجراء التفتيش عليها من قبل أنثى لحماية خصوصيتها.

المطلب الثاني: الشروط الشكلية لإجراء التفتيش في الجرائم الإلكترونية

إن إجراء التفتيش كونه أحد إجراءات التحقيق فإنه يخضع لذات الشروط الشكلية التي يخضع لها التحقيق وهي: 1. إذن التفتيش 2. حضور إجراء التفتيش3. وقت إجراء التفتيش 4. محضر إجراء التفتيش.

الفرع الأول: إذن التفتيش

وهو ما يسمى بأمر التفتيش ويعني تفويض من قبل السلطة المختصة بإجراء التفتيش إلى أحد مأموري الضبط القضائي ويتم تخويل هذا الأخير بموجبه القيام بإجراء التفتيش الذي تختص به تلك السلطة[1].

ويشترط في إذن التفتيش مجموعة من الشروط والتي تتمثل بما يلي:

[1] هروال، نبيلة هبة: **الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات" دراسة مقارنة"**، الاسكندرية-مصر: دار الفكر الجامعي، 2007،ص243.

أولاً: تسبيب إذن التفتيش

ويعني تبيان وتوضيح الأسباب التي دعت إلى إصدار إذن التفتيش وتم الاستناد عليها من قبل المختص بإصداره[1]، وأكدت النصوص الدستورية[2] والقانونية[3] الفلسطينية والمصرية على ضرورة تسبيب إذن التفتيش لما فيه من حماية سواء أكان هذا التفتيش للأشخاص أو للأماكن بحيث يجعل السلطة تصدره وفقاً لمبررات ضرورية وبالتالي تكون بعيدة عن التعسف في إصداره[4].

ثانياً: صدور الإذن كتابةً

حتى يعتد بالإذن ويكون ذو قيمة قانونية فإنه لا بدّ من أن يتم إصداره كتابةً، ونعني بالكتابة أن كل عبارة تكون واضحة الدلالة إذ بمجرد الاطلاع عليها تفيد بأنها إذن للتفتيش[5]، بحيث يتناول كافة البيانات التي يطلبها المشرع وتقوم الجهة المختصة بالتفتيش بصياغة الإذن بأي شكلٍ كان إذ إنّ المشرع (الفلسطيني والمصري) لم ينصّ على شكلاً معيناً للكتابة بالتالي يمكن كتابتها بواسطة اليد أو باستخدام الوسائل الحديثة كطباعتها باستخدام الحاسوب أو الفاكس، وباعتبار الجرائم الإلكترونية بحاجة إلى السرعة في اتخاذ الإجراءات فإنه يمكن تبليغ مأمور الضبط بالإذن هاتفياً[6] ويقوم بإجراء التفتيش دون أن يكون الإذن بيده لكن شريطة أن تكون الجهة المختصّة قد صاغته كتابياً قبل تبليغه بذلك حتى لا يشوب الإجراء أي بطلان، وقضت في ذلك محكمة النقض المصرية " لما كان ذلك وكان من المقرر أنه لا يلزم وجود ورقة

---

[1] أحمد، حسام الدين محمد: **الإذن بالتفتيش والضبط**، الطبعة الثالثة، مصر: دار النهضة العربية، 2003،ص 286.

[2] انظر المواد 2/11 والمادة17 من القانون الأساسي الفلسطيني المعدل لسنة 2003 والمواد 54، 57و58 من الدستور المصري لعام 2014 والمعدل في سنة 2019.

[3] المواد 2/39 من قانون الاجراءات الجزائية الفلسطيني رقم 3لسنة 2001 و91 من قانون الاجراءات الجنائية المصري رقم 150 لسنة 1950.

[4] أحمد، حسام الدين محمد: **الإذن بالتفتيش والضبط**، مرجع سابق، ص 287.

[5] أحمد، حسام الدين محمد: **الإذن بالتفتيش والضبط**، مرجع سابق، ص264.

[6] حيث قضت محكمة النقض المصرية في ذلك" لا يشترط أن يكون أصل الإذن بيد الضابط الذي أجرى التفتيش ويمكن أن يصدر الإذن تلفونياً أو بالفاكس...إلخ" : نقض/ جزاء مصري رقم 13 لسنة 14 قضائية جلسة 1943/12/20.

الإذن بالقبض والتفتيش بيد مأمور الضبط القضائي وقت إجرائهما إذ لا يشترط إلا أن يكون الأمر ثابتاً بالكتابة"[1].

وتأكيداً على ضرورة الكتابة للإذن فقد نصّ المشرع الفلسطيني على مجموعة من البيانات الواجب توافرها في إذن التفتيش ومنها: 1-اسم صاحب المنزل المراد تفتيشه وشهرته وإذا كان المراد تفتيشه هو شخص فيجب تحديد اسم الشخص وذكره في الإذن 2-تحديد عنوان المنزل المراد تفتيشه بالتفصيل ولا يشوبه أي جهالة 3-تحديد الغرض من إجراء التفتيش بشكل واضح والمتمثل في ضبط الأدلة والأشياء المتعلقة بالجريمة المرتكبة والتي تفيد في كشف الحقيقة 4-اسم مأمور الضبط القضائي المصرح له بالتفتيش[2]، كما وقضت محكمة النقض المصرية في ذلك:" أن إذن النيابة لمأموري الضبط القضائي بإجراء التفتيش يجب أن يكون مكتوباً موقعاً عليه بإمضاء من أصدره لأنه من القواعد العامة أن إجراءات التحقيق والأوامر الصادرة بشأنه يجب إثباتها بالكتابة لكي تبقى حجة يعامل الموظفون- الآمرون والمؤتمرون- بمقتضاها ولتكون أساساً صالحاً لما يبنى عليها من نتائج ولما كان الإذن وهو من أعمال التحقيق لا يكفي فيه الترخيص الشفوي بل يجب أن يكون له أصل مكتوب[3].

ثالثاً: توقيع مصدر الإذن

بحيث يجب على الجهة المختصة بإصداره وهي النيابة العامة أن تقوم بالتوقيع على إذن التفتيش وعلى أن يقوم مصدره بذكر اسمه وصفته وتوقيعه، ولم يرسم القانون شكلاً خاصاً لهذا التوقيع[4].

---

[1] نقض/جزاء مصري رقم 7963 لسنة 78 قضائية جلسة 2017/1/4.

[2] انظر المادة 40 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

[3] نقض/جزاء مصري رقم 1359 لسنة 80 قضائية جلسة 2012/3/6.

[4] نقض/ جزاء مصري رقم 20309 لسنة 87 قضائية جلسة 2020/1/19.

رابعاً: تحديد تاريخ وساعة إصدار الإذن

بحيث يتوجب على مُصدر إذن التفتيش أن يحدد تاريخ وساعة إصداره، ولعلّ السبب في ذلك هو أن إجراء التفتيش يكون للبحث عن الأدلة وبالتالي يجب أن يكون إذن التفتيش بعد وقوع الجريمة، لذلك يتم معرفة متى صدر هذا الإذن فيما إذا كان بعد ارتكاب الجريمة أم قبل (بحيث إذا كان الإذن الصادر لجريمة مستقبلية لم تحدث فإن إجراء التفتيش يعتبر باطلاً)[1]، كما أن معرفة تاريخ وساعة إصدار الإذن يؤدي إلى معرفة كم مضى مدة على سريان الإذن وفيما إذا مضت مدة طويلة على صدوره أم لا وأن التنفيذ قد تم خلال الأجل المصرّح فيه وأخيراً معرفة إذا كان مصدر الإذن مختصّاً وقت صدور الإذن أم لا، لذلك يعتبر تحديد تاريخ وساعة إصدار الإذن كضمان لصحة إجراء التفتيش[2].

خامساً: تحديد وقت تنفيذ الإذن

يمكن لمأمور الضبط القضائي المنتدب لتنفيذ إذن النيابة العامة بالتفتيش تخير الظرف المناسب لإجرائه بطريقة مثمرة خلال المدة المحددة بالإذن[3]، وإذا حددت النيابة أن تنفيذ الإذن يكون خلال 48 ساعة من تاريخ صدوره فإن اليوم الذي صدر فيه الإذن لا يحسب في الميعاد طبقاً للقواعد العامة بل يجب احتساب الساعات من ابتداء اليوم التالي[4].

سادساً: تحديد أجل لسريان تنفيذ الإذن

إذ يجب تحديد المدة التي تسري خلالها إذن التفتيش بحيث لا تكون هذه المدة مفتوحة لما في ذلك من حماية للمتهم المراد تفتيشه وتفتيش منزله، وبذلك فقد نص المشرع الفلسطيني فيما يتعلق بالجرائم الإلكترونية على أن يكون الإذن محدد المدة مع جواز تجديده لأكثر من مرة طالما أن مبررات إجراء

---

[1] الشواربي، عبد الحميد: **إذن التفتيش في ضوء القضاء والفقه**، مرجع سابق، ص42.

[2] طنطاوي، إبراهيم حامد: **الدفع ببطلان إذن النيابة العامة بالتفتيش**، الطبعة الثانية، الاسكندرية–مصر: دار النهضة العربية،1997، ص54+ص55.

[3] نقض/ جزاء مصري رقم 29117 لسنة 85 قضائية جلسة 2017/12/25.

[4] نقض/ جزاء مصري رقم 1484 لسنة 11 قضائية جلسة 1941/5/19.

التفتيش ما زالت[1]، أما المشرع المصري فقد حدد مدة الإذن 30 يوماً قابل للتجديد مرة واحدة إذا كان هذا التجديد سيجني فائدة وبالتالي تظهر الحقيقة[2]، ويعتبر الإذن الصادر لتفتيش شخص أو منزل منتهي مفعوله بمجرد تنفيذ مقتضاه فمتى أجرى المأمور المنتدب التفتيش فليس له أن يعيده مرة ثانية اعتماداً على الإذن المذكور[3].

وترى الباحثة هنا أن المشرع المصري أصاب في تحديد المدة وفي تجديد مدة الإذن، وذلك لما فيه من حماية أكثر للمتهم في الجرائم الإلكترونية بحيث لا يبقى مدة طويلة تحت تهديد التفتيش.

الفرع الثاني: حضور إجراء التفتيش

لقد نص كل من المشرع الفلسطيني والمصري على ضرورة حضور أشخاص معينين عند إجراء التفتيش؛ ويعود السبب في ذلك إلى حماية الشخص الخاضع للتفتيش وذلك من خلال مراقبة صحة إجراءات التفتيش وسلامة ضبط الأدلة، الأمر الذي يحقق قاعدة علانية التحقيق بالنسبة للخصوم مما يتيح للأشخاص الحاضرين لإجراءات التفتيش الاطلاع على ما يتم ضبطه أثناء تنفيذه لذلك يعتبر حضور الأشخاص ضمانة لإجراء التفتيش وحتى لا يفقدهم الحق في مراقبة التفتيش وقانونيته[4]، ويضاف إلى ما سبق أن حضور الأشخاص لإجراءات التفتيش تحمي القائمين على التفتيش من تلفيق أي اتهامات بحقهم فيما بعد كأن يتم اتهامهم بسرقة أموال أو مجوهرات خلال إجراء التفتيش.

وفيما يتعلق بحضور المتهم فإنه يعتبر حضوره بديهياً عند إجراء التفتيش عليه كونه هو الخاضع للتفتيش، لكن الإشكالية تثور عندما يكون التفتيش لمسكنه فإنه يمكن أن لا يكون حاضراً وتعذر حضوره بالتالي

---

[1] انظر المادة 2/52 من القرار بقانون الفلسطيني رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] المادة 6 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.

[3] نقض/ جزاء مصري رقم 8015 لسنة 81 قضائية جلسة 2012/3/20.

[4] الذنيبات، محمد جمال مطلق والعناسوة، معن أحمد: *التفتيش في الجرائم الإلكترونية ماهيته وشروطه الشكلية*، **المجلة الأردنية في القانون والعلوم السياسية**، مجلد13، العدد3/2021، ص100.

يمكن له أن ينيب أحد الأشخاص ليقوم بالحضور عنه عند إجراء التفتيش، كما ويمكن إجراء التفتيش بوجود شاهدين من أقاربه أو جيرانه أو من القاطنين معه في المنزل، ويجب ذكر أسماء من حضر عند إجراء التفتيش في محضر التفتيش[1].

وهناك من ذهب إلى اعتبار حضور المتهم هو من الشروط الجوهرية لصحة إجراء التفتيش وأن عدم حضوره يرتب البطلان عليه، إلا أن القضاء قد فصل في ذلك وأكد على أن حضوره لا يرتب البطلان على الإجراء[2]، وقضت محكمة النقض الفلسطينية على: " لا يرد القول باعتبار إجراءات تفتيش منزل أهل المتهم الذي يقيم فيه أو المسؤول عن المكان المراد تفتيشه دون حضوره باطلة"[3]، أما محكمة النقض المصرية فقد قضت سابقاً ببطلان التفتيش عند عدم حضور المتهم إلا أنها عدّلت فيما بعد ذلك وأكدت على " حصول التفتيش بغير حضور المتهم لا يترتب عليه البطلان"[4].

وفيما يتعلق بإجراء التفتيش في الجرائم الإلكترونية بحضور المتهم أو إنابة أحد عنه فإن القوانين المتعلقة بالجرائم الإلكترونية لم توضح ذلك، إلا أنه **نرى** أن يتم تطبيق القواعد العامة سالفة الذكر لما فيها من حماية للمتهم وضمانة له لذلك، إذا تم ضبط الوسيلة الإلكترونية تمهيداً لإجراء التفتيش عليها فإن حضور المتهم أو من ينيب عنه أو الشهود من الساكنين معه أو الجيران أو الأقارب يعتبر أمر ضروري لكن يجب التفرقة فيما إذا سيتم تفتيشها مباشرة أو أنه سيتم نقل الوسيلة ليتم فيما بعد تفتيشها، فإذا كانت الحالة الأولى فإنه يتطلب الأمر أن يكون من كان حاضراً لإجراء التفتيش على دراية وعلم بالوسائل التكنولوجية والتقنيات لما فيه من حماية للمتهم وضمانة لحقوقه ومنع القائمين على التفتيش من التعسف في الإجراء أو

[1] مادة 43 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 ومادة51 من قانون الاجراءات الجنائية المصري رقم 150 لسنة 1950.

[2] هروال، نبيلة هبة: **الجوانب الإجرائية لجرائم الإنترنت**، مرجع سابق، ص256.

[3] نقض/جزاء فلسطيني رقم 147 لسنة 2020.

[4] نقض/ جزاء مصري رقم 4077 لسنة 57 قضائية قاعدة رقم 63 صفحة435 لسنة 1988.

قيام أحدهم باختلاق الأدلة، أما في الحالة الثانية فإن عملية الضبط للوسيلة التكنولوجية بحد ذاتها لا تتطلب توافر خبرة وعلم لدى الحاضرين لإجراء التفتيش لأنه لن يتم التفتيش مباشرة.

وترى الباحثة هنا أن توافر الدراية والخبرة والاختصاص فهي ممكنة في المتهم كونه هو من ارتكب الجريمة الإلكترونية وبالتالي فهو بالطبع لديه القدرة على التعامل مع الوسائل التكنولوجية والتقنيات المختلفة، أما الأشخاص الآخرين غير المتهم والذين يحضرون التفتيش غالباً يكونوا أشخاص عاديين ولا تكون لهم أي خبرة أو علم في الوسائل التكنولوجية لذلك يعتبر حضورهم غير مفيد.

الفرع الثالث: وقت إجراء التفتيش

نص المشرع الإجرائي الفلسطيني على تحديد وقت إجراء التفتيش ويكون هذا الوقت في النهار وفي حالات استثنائية يمكن إجراؤه ليلاً، أما عن المشرع الإجرائي المصري فلم يحدد وقتاً لإجراء التفتيش إذ لم يورد أي قيد بموعد إجراء التفتيش لذلك يمكن إجراؤه نهاراً أو ليلاً[1].

وترى الباحثة أن تحديد وقت إجراء التفتيش نهاراً وفي حالات استثنائية ليلاً لهو أمرٌ جيد كونه يحد من تعسف السلطة المختصة بإجراء التفتيش فلو كان الأمر مفتوحاً لإجراء التفتيش للمنازل ليلاً لأصبحت البيوت مهددة لإجراء التفتيش في أي وقت وفي ذلك تأثير على الساكنين فيها مما يرهبهم ويؤثر على طمأنينتهم وحرياتهم.

أ. إجراء التفتيش نهاراً: لقد حدد المشرع الفلسطيني كما ذكرنا أنه يجب أن يكون إجراء التفتيش نهاراً إلا أنه لم يحدد الساعات التي تتم بها، وبالرجوع إلى قانون العقوبات الساري في فلسطين نرى أنه قد عرّف الليل: "هو الفترة التي تقع بين غروب الشمس وشروقها"[2]، وبذلك يمكن اعتبار الفترة الممتدة ما بين شروق الشمس إلى غروبها هي فترة النهار والتي تختلف باختلاف الفصول فقد تكون قصيرة في

[1] الشهاوي، قدري عبدالفتاح: **مناط التفتيش**، مرجع سابق، ص163.

[2] انظر المادة 2 من قانون العقوبات رقم 16 لسنة 1960 والساري المفعول في فلسطين.

فصل الشتاء وقد تكون طويلة في فصل الصيف، وعلى الرغم من عدم تحديد الساعات ولاختلاف الفصول فإنه يفهم ضمنياً الساعات التي يتم فيها إجراء التفتيش نهاراً والساعات التي يتم فيها إجراؤه استثناءً ليلاً[1].

ب. إجراء التفتيش ليلاً: فاستناداً للمشرع الإجرائي الفلسطيني فإنه يتم إجراء التفتيش في حالات استثنائية وهي على سبيل الحصر وتتمثل في 1-توافر إحدى حالات التلبس في الجريمة: لقد تحدثنا سلفاً في هذه الدراسة عن الحالات التي يكون فيها تلبس بالجريمة، وبالتالي إذا ما توافرت إحدى هذه الحالات فإن المشرع أجاز للسلطة القائمة بالتفتيش إجراء التفتيش ليلاً على المنازل[2].

وعلى الرغم من أن المشرع الإجرائي المصري كان قد أورد في المادة 47 منه أنه يمكن لمأمور الضبط القضائي في حالات التلبس بالجريمة أن يقوم بإجراء التفتيش على منزل المتهم إلا أن المحكمة الدستورية العليا المصرية قضت بعدم دستورية نص المادة 47 وألغتها وذلك في سبيل حماية الحقوق والحريات[3] ولعدم مخالفة النص الدستوري[4] الذي أكد على أن المنازل لا يمكن إجراء تفتيشها إلا بناءً على أمر قضائي مسبب وبالتالي حتى لو توافرت إحدى حالات التلبس فإنه لا يمكن إجراء التفتيش عليها، أما تفتيش الأشخاص فإنه إذا ما توافرت إحدى حالات التلبس يجوز إجراء التفتيش عليهم دون أمر قضائي[5].

2. في ظروف الاستعجال: على الرغم من أن المشرع الإجرائي الفلسطيني نص على أنه يمكن في ظروف الاستعجال إجراء التفتيش على المنزل إلا أنه لم يوضح هذه الظروف ولم يبين ماهيتها، وبالرجوع إلى قانون الاجراءات الجزائية الفلسطيني في المادة 98منه نرى أنه قد أورد إحدى حالات

---

[1] عموري، أشرف أحمد مصطفى: **التفتيش في الجرائم الإلكترونية**، رسالة ماجستير ، جامعة القدس-فلسطين، 2018، ص61

[2] انظر المادة 41 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

[3] القضية رقم 5 لسنة 4 قضائية جلسة 1984/2/2.

[4] انظر المادة 58 من الدستور المصري لسنة 2014 والمعدل في سنة 2019.

[5] انظر المادة 54 من الدستور المصري لسنة2014 والمعدل في سنة 2019.

الضرورة والاستعجال والتي تتمثل بالخوف من ضياع الأدلة وعلى أن يتم تدوين هذا السبب في المحضر.

وننوه هنا أنه هناك حالة يتم فيها إجراء التفتيش ليلاً بناءً على موافقة المتهم ورضائه ودون إصدار إذن للتفتيش، وتم استخلاص هذه الحالة من خلال بعض الأحكام ومنها:" من المقرر أن حرمة المنازل وما أحاط به الشارع من رعاية تقتضي حين يكون دخولها بعد رضاء أصحابها وبغير إذن النيابة العامة أن يكون هذا الرضاء حراً صريحاً حاصلاً منهم قبل التفتيش وبعد إلمامهم بظروفه وبعدم وجود مسوغ يخول من يطلبه سلطة إجرائه وتقدير صحة هذا الرضاء هو من شؤون المحكمة تقدره حسبما يتكشف لها من ظروف الدعوى[1]، ويتم إجراء التفتيش في هذه الحالة استناداً إلى موافقة صريحة وواضحة من قبل المتهم المراد تفتيش منزله أي صاحب الشأن وليس أحدٍ غيره وأن تكون هذه الموافقة مكتوبة وحقيقية وخالية من أي زيفٍ أو خداع وأن الموافقة قد تمت دون أي إجبار أو إكراه من قبل مأموري الضبط القضائي[2]، وبالرجوع إلى القوانين الإجرائية والقوانين المتعلقة بالجرائم الإلكترونية نرى أنها لم تنص على إمكانية إجراء التفتيش بناءً على رضاء المتهم أو صاحب المنزل.

وترى الباحثة هنا أن الرضا والقبول من قبل صاحب الشأن لإجراء التفتيش على منزله هو أمر غير جيد، فطالما أن الدستور قد كفل لك الحق بعدم جواز انتهاك حرمة المنزل إلا بأمر مسبب وأن القوانين لم تنص على حالة الرضا، فلماذا يتم التنازل عن هذا الحق، ونرى أيضاً أن صدور الرضا من قبل صاحب الشأن قد يكون معيب وأنه قد قبل نتيجة الضغط والقوة لإجراء التفتيش، لذلك لا بد من أن لا يوافق على إجراء تفتيش منزله إلا بموجب إذن صادر من الجهات المختصة حتى يضمن حقوقه.

---

[1] نقض/ جزاء مصري رقم 1226 لسنة 45 قضائية جلسة 1975/11/23.

[2] عطية، طارق إبراهيم الدسوقي: **الأمن المعلوماتي النظام القانوني للحماية المعلوماتية**، الاسكندرية–مصر: دار الجامعة الجديدة للنشر، 2009، ص439+ 440.

وفيما يتعلق بالجرائم الإلكترونية فإن القوانين المتعلقة فيها لم تحدد الوقت الذي يتم فيه إجراء التفتيش لهذا يتم تطبيق القواعد العامة سالفة الذكر.

الفرع الرابع: محضر إجراء التفتيش

إن إجراءات التحقيق بشكل عام يتوجب على السلطة المختصة بإجرائها أن تقوم بتنظيم محاضر رسمية ويتم فيها تدوين كافة الإجراءات التي يتم اتخاذها، لذلك يجب عند القيام بإجراء التفتيش أن يتم تنظيم محضر يدوّن فيه كافة الاجراءات التي تم اتخاذها[1].

ونص كل من المشرع الفلسطيني والمصري على أنه يجب اصطحاب كاتباً في جميع إجراءات التحقيق ليقوم بتدوين المحضر وبالتالي فإنه عند إجراء التفتيش يجب اصطحاب كاتباً لتدوين كل ما يتعلق بالإجراء في محضر وعلى أن يقوم القائم بالتفتيش وهذا الكاتب بالتوقيع على المحضر[2]، وعلى الرغم من اشتراط المشرع لاصطحاب الكاتب إلا أن محكمة النقض المصرية كان لها رأي في ذلك أن إجراءات التحقيق التي تستلزم اصطحاب كاتباً ليقوم بتحرير المحاضر كسماع شهادة الشهود واستجواب المتهم وإجراء المعاينة وذلك لأن هذه الإجراءات تستلزم انصراف المحقق بفكره إلى مجريات التحقيق أما إجراءات التحقيق كالأوامر الصادرة بالحبس والقبض والتفتيش فهي بطبيعتها لا تستلزم تحرير محاضر تصرف فكر المحقق عن مهمته الأصلية ولا توجب بالتالي أن يصاحبه فيها كاتب يوقع معه عليها[3]. ويكمن الهدف من تدوين محضر التفتيش هو لتوثيق ما يبديه المتهم من ملاحظات عند إجراء التفتيش على الأشياء المضبوطة، وقضت محكمة النقض المصرية أنه وفي حالة الإغفال عن تحرير المحضر فإنه لا يبطل الإجراء[4].

---

[1] مادة 50 من قانون الاجراءات الجزائية الفلسطيني رقم3 لسنة 2001 و55 و56 من قانون الاجراءات الجنائية المصري رقم 150 لسنة 1950.

[2] مادة 58 من قانون الاجراءات الجزائية الفلسطيني رقم3 لسنة 2001 ومادة 73 من قانون الاجراءات الجنائية المصري رقم150 لسنة 1950.

[3] نقض/جزاء مصري رقم 612 لسنة 31 قضائية جلسة 1961/10/23.

[4] نقض/ جزاء مصري رقم 441 لسنة 27 قضائية جلسة 1957/6/10 مكتب فني(سنة 8 قاعدة 173 صفحة 633).

ويتم تدوين المحضر باللغة الرسمية وهي اللغة العربية وفيما يتعلق بالجرائم الإلكترونية فهناك مصطلحات أجنبية بالتالي يجب مراعاتها وتدوينها في المحضر، ويمكن الاستعانة بمترجم في حالة إذا كان المراد تفتيش منزله ممن يجهل اللغة العربية وأبدى ملاحظاته ومن ثم تدوين هذه الملاحظات في المحضر[1].

ويتوجب عند تدوين المحضر كتابة تاريخ ووقت إجراء التفتيش ويفيد إثبات ذلك في المحضر في بدء قطع التقادم بالنسبة للدعوى الجنائية كون أن إجراء التفتيش هو إجراء من إجراءات التحقيق[2]، ويجري التوقيع على المحضر من قبل القائم به ومن المتهم الذي تم تفتيشه أو تفتيش منزله ومن الحاضرين الشاهدين ومن الكاتب الذي دوّن المحضر، وفي حالة امتناع أي أحد عن التوقيع على المحضر فإنه يتوجب تدوين ذلك في المحضر[3].

وفي حالة تدوين المحضر عند التفتيش في الجرائم الإلكترونية[4] يجب كتابة كافة ما يجري من كيفية القيام به وما تم ضبطه والملاحظات التي يبديها المتهم أو الشهود الحاضرين وفيما إذا جرى أي منع أو إعاقة لإجراء التفتيش كأن يمتنع المتهم عن فتح جهازه الذي عليه كلمة سر فيجب تدوين ذلك وكذلك الحالة التي كان عليها الوسائل التكنولوجية عندما تم ضبطها وكيف تم الولوج إليها وتفتيشها.

المطلب الثالث: خصوصية التفتيش في الجرائم الإلكترونية العابرة للحدود

لقد تحدثنا حول الشروط الموضوعية والشكلية الواجب توافرها لإجراء التفتيش بالشكل الصحيح في الجرائم الإلكترونية إذا ما ارتكبت هذه الجريمة داخل الدولة، إلا أنه كما نعلم أن من خصائص الجريمة الإلكترونية أنها جريمة عابرة للحدود أي بمعنى أنه يمكن ارتكاب الجريمة الإلكترونية داخل حدود الدولة لكن آثارها ونتائجها تتحقق في دولة أو عدة دول أخرى، لذلك خلق هذا الأمر إشكاليات عديدة أمام الجهات المختصة

---

[1] المادة 60 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

[2] الشهاوي، قدري عبدالفتاح: **مناط التفتيش**، مرجع سابق، ص 161.

[3] المادة 55 من قانون الاجراءات الجنائية المصري رقم 150 لسنة 1950.

[4] المادة 54 من القرار بقانون الفلسطيني بشأن الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات" وعلى من قام بالتفتيش... أن ينظم محضراً بذلك وتقديمه للنيابة العامة".

بالتحقيق في مثل هذه الجرائم، إذ إن الأمر يتطلب إجراء التفتيش والبحث والتقصّي عن الأدلة التي تكون مخزنة على وسائل تكنولوجية موجودة خارج النطاق الإقليمي للدولة وقيامها عندئذٍ بإجراء التفتيش على هذه الوسائل فيه اعتداء ومساس بسيادة الدولة الموجود لديها الوسائل التكنولوجية والأدلة، لذلك كان لا بدّ من معالجة هذه الإشكاليات دون أن يتم المساس بسيادة الدول الأخرى، وتمثلت هذه المعالجة من خلال تحقيق التعاون بين الدول والمساعدة في القيام بالإجراءات من أجل تحقيق العدالة وإلقاء القبض على المتهم وملاحقته ومحاكمته أينما كان، ومن صور المساعدة والتعاون القضائي الدولي ما يسمى بالإنابة القضائية ونتعرف في هذا المطلب على هذه الإنابة وكيف تم تنظيمها في التشريعات والاتفاقيات حتى تتمكن الدول من تبادل المساعدة القضائية في إجراءات التحقيق وخاصة إجراء التفتيش في الجرائم الإلكترونية.

الفرع الأول: وجود الإنابة القضائية

ويقصد بها بشكل عام أنها "هي إجراء بموجبه يعهد فيه إلى السلطات القضائية المطلوب منها اتخاذ إجراء القيام بالتحقيق لمصلحة السلطة القضائية المختصّة في الدول الطالبة مع مراعاة احترام حقوق وحريات الإنسان المعترف بها عالمياً ومقابل ذلك تتعهد الدولة طالبة المساعدة بالمعاملة بالمثل واحترام النتائج القانونية التي توصلت إليها الدولة المطلوب منها المساعدة القانونية[1]، كما وعرفتها اتفاقية الرياض للتعاون القضائي على أنها:" هي قيام أحد الأطراف المتعاقدة في الاتفاقية بالطلب من أي طرف متعاقد آخر أن يقوم في إقليمه نيابة عنه بأي إجراء قضائي متعلق بدعوى قائمة وبصفة خاصة سماع شهادة الشهود وتلقي تقارير الخبراء ومناقشتهم وإجراء المعاينة وطلب تحليف اليمين"[2].

ويكمن الهدف من اللجوء إلى الإنابة القضائية إلى تحقيق التعاون بين الدول من أجل حماية حقوق الأفراد وإلى تحقيق العدالة وضمان ملاحقة المجرمين والمتهمين أينما كانوا ومحاكمتهم على أفعالهم، كما أن الإنابة القضائية تحمي الدولة من المساس بسيادتها من قبل دولة أخرى من خلال قيام هذه الأخيرة بإنابة

[1] الخضري، سمر خضر صالح: **أحكام تسليم المجرمين في فلسطين**، رسالة ماجستير، جامعة الأزهر: غزة–فلسطين، 2010،ص27.

[2] المادة 14 من اتفاقية الرياض للتعاون القضائي.

سلطات الدولة الموجود لديها المتهم أو الأدلة للقيام بإجراءات التحقيق وجمع الأدلة وضبطها وملاحقة المجرم والقبض عليه ومن الأمثلة على الإجراءات التي يمكن أن تكون فيها إنابة قضائية إجراءات التقاضي وإجراءات التحقيق، وقد أكدت الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية فيما سبق على أنه لا يمكن لدولة أن تقوم بممارسة الولاية القضائية في إقليم دولة أخرى وكذلك لا يمكنها أداء الوظائف التي يناط بأدائها حصراً لسلطات إقليم الدولة الأخرى[1].

الفرع الثاني: تنظيم الإنابة القضائية في التشريعات والاتفاقيات

أولاً: تنظيم الإنابة القضائية في التشريعات الداخلية

نظراً لأهمية الإنابة القضائية باعتبارها إحدى صور التعاون القضائي الدولي لتحقيق العدالة وحماية الحقوق، لذا سعت معظم الدول إلى تنظيمها في تشريعاتها ووضع الضوابط الواجب التقيد بها عند الاستعانة بها، وعلى الرغم من أهميتها إلا أنه وبالرجوع إلى التشريعات الداخلية ففي فلسطين لا يوجد ما ينظمها في التشريع الإجرائي الفلسطيني ولم يتم التطرق إليها، إلا أن القرار بقانون المتعلق بالجرائم الإلكترونية تحدث عن الإنابة القضائية بحيث يمكن لفلسطين تبادل المساعدة القانونية مع الدول الأخرى في مجال إجراءات التحقيق والإجراءات الجنائية المرتبطة بالجرائم المنصوص عليها في هذا القرار بقانون وكذلك في مجال عملية تسليم المجرمين، وعلى أن يتم الاستناد في تبادل المساعدة إلى ما هو مقرر في قانون الإجراءات الجزائية النافذ والاتفاقيات الثنائية ومتعددة الأطراف أو وفقاً لمبدأ المعاملة بالمثل وبما لا يتعارض مع أحكام هذا القرار بقانون[2]، وكذلك في مصر فقد خلى أيضاً التشريع الإجرائي المصري من أي

[1] المادة 4 من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية.

[2] المادة 1/63من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات الفلسطيني رقم 10 لسنة 2018.

تنظيم للإنابة القضائية الدولية، واكتفى بالأحكام المنظمة لها والواردة في الاتفاقيات الدولية التي انضمت إليها مصر[1].

ثانياً: تنظيم الإنابة القضائية في الاتفاقيات الثنائية والجماعية

حتى يتم تنفيذ الإنابة على وجه السرعة وضبط الادلة وجمعها والوصول إلى المتهم بارتكابها فإنه لا بدّ من اختصار الشكليات والإجراءات عند اللجوء لهذه الإنابة ويكون ذلك من خلال إبرام الاتفاقيات التي يتم الاستناد عليها لربط السلطات المختصة في الدولتين لتتمكن من التواصل مباشرة وعلى وجه السرعة فيما بينها[2]، وهذه الاتفاقيات إما أن تكون اتفاقيات ثنائية بين دولتين أو اتفاقيات جماعية دولية.

أ. الاتفاقيات الثنائية: وهي تلك الاتفاقيات التي يتم إبرامها بين دولتين والتي تتضمن التزامات متبادلة لكلا الطرفين المتعاقدين، وأبرمت فلسطين قديماً بشأن التعاون القضائي الدولي مجموعة من الاتفاقيات الثنائية وهي الاتفاق المؤقت بين الحكومة المصرية وحكومة فلسطين بشأن تسليم المجرمين وذلك في1922/12/21[3]،اتفاق فلسطين مع حكومة شرق الأردن بشأن تسليم المجرمين بتاريخ1934/7/26 والذي استند على القوانين الصادرة في كلى الدولتين وهما قانون تسليم المجرمين الفارين الأردني لسنة1927وقانون تسليم المجرمين الفلسطيني لسنة 1926[4]، والاتفاق الثنائي بين سوريا وفلسطين[5].

---

[1] فضل، سليمان أحمد: **المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية(الانترنت)**، مرجع سابق، ص426.

[2] فضل، سليمان أحمد: **المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية(الانترنت)**،مرجع سابق، ص427.

[3] موقع بوابة مصر للقانون والقضاء:
https://www.laweg.net//Default.aspx?action=ViewActivePages&ItemID=36537&Type=6

[4] http://muqtafi2.birzeit.edu/yamen2/ar/legislations/act_card/JTJGZGIlMkZtdXF0YWZpJTJGYWN0JTJGeG1sJTJGMTkzNCUyRmFnbW50X0hpZ2hDb21taXNzaW9uZXJfMTkzNC0wNy0yNl9hciUyRjg2NT=BfMTkzNC54bWw

[5] الزاملي، ابراهيم سالم: **فلسطين في التقارير البريطانية 1919-1947**، دار ابن رشد، ص112.

وتعتبر هذه الاتفاقيات قديمة وتم إصدارها بشأن تسليم المجرمين باعتبارها كأحد صور التعاون القضائي بين الدول، أما بخصوص الإنابة القضائية فإننا نجد أن فلسطين لم تبرم أي اتفاق ينظم هذا الأمر على الرغم من الحاجة الملحة والضرورية لعقد مثل هذه الاتفاقيات، ولعل السبب في رأيي يعود في عدم إبرامها لهذه الاتفاقيات إلى الحالة السياسية الخاصة التي تتمتع بها فلسطين كونها تقبع تحت الاحتلال الإسرائيلي والذي شكّل عقبة أمامها وعمل على تقسيمها.

أما مصر فقد أبرمت العديد من الاتفاقيات الثنائية مع الدول الأخرى والتي تعمل على تنظيم التعاون القضائي وتبادل المساعدة القضائية فيما بينها، ومن هذه الاتفاقيات اتفاقية التعاون القضائي بين الأردن ومصر رقم 3 لسنة 2001، اتفاقية التعاون القانوني والقضائي في المواد المدنية والتجارية والأحوال الشخصية والمواد الجزائية بين الجمهورية التونسية وجمهورية مصر العربية في 1976/5/12 واتفاقية التعاون القانوني والقضائي بين مصر والكويت، وقد ضمت هذه الاتفاقيات وغيرها نصوصاً تتعلق بالأحكام التي تنظم عملية الإنابة القضائية من حيث الكيفية التي تتم بها والحالات التي يمكن رفض القيام بتنفيذها وكذلك الحالات التي يتعذر فيها تنفيذها.

وترى الباحثة **أن** عملية الإنابة القضائية لإجراء التفتيش في الجرائم الإلكترونية تعد منظمة في مصر وفقاً للاتفاقيات الثنائية مما يسهل عملية إجراؤها وتنفيذها بشكل سريع، أما في المقابل فإن فلسطين تفتقر لمثل هذه الاتفاقيات مما يشكل عقبة في تبادل المساعدة والإنابة إلى جانب عدم سيطرتها على الحدود.

ب. الاتفاقيات الجماعية: وهي الاتفاقيات التي يتم إبرامها بين مجموعة من الدول أي تشترك فيها أطراف عديدة أي أكثر من دولتين وتتعلق هذه الاتفاقيات بقواعد عامة في القانون الدولي وتعالج مسائل ذات مصلحة عامة للدول جميعاً[1] ويتم بموجبها فرض التزامات معينة ويجب على كل دولة تنضم إلى هذه الاتفاقية أن تلتزم بها، ومن أبرز هذه الاتفاقيات:

1. اتفاقية الرياض العربية للتعاون القضائي[2]: وتناولت هذه الاتفاقية عدة نصوص نظمت فيها الإنابة القضائية، حيث نصّت المادة 14 على أن "يحق لكل طرف متعاقد في هذه الاتفاقية أن يطلب من أي طرف متعاقد آخر أن يقوم هذا الأخير نيابةً عنه بأي إجراء قضائي".

ونرى هنا أن هذه الاتفاقية عملت على تنظيم عملية الإنابة القضائية ومكّنت الدول من التعاون القضائي فيما بينها وإنابة بعضهما البعض في اتخاذ أي إجراء بما فيها إجراءات التفتيش وضبط وجمع الأدلة[3]، وعلى الرغم من ذلك يؤخذ على هذه الاتفاقية أنها جعلت طلبات الإنابة تتم عن طريق وزارة العدل وهذا يجعل الأمر أكثر بطئاً وتعقيداً ويأخذ وقت وجهد كبير مما يؤدي إلى فقدان الأدلة في الجرائم الإلكترونية[4]، أما في القضايا المدنية والأحوال الشخصية فجعلت هذه الاتفاقية الإنابة القضائية تتم مباشرة بين الجهات المختصّة دون أن يكون هناك وسيط من أي جهة[5] مما يجعل الأمر أكثر فعالية وسرعة في اتخاذ الإجراءات، لذلك كان لا بدّ من أن تكون الإنابات القضائية المتعلقة بالجرائم والمسائل الجنائية أن تتم بذات الطريقة وأن تكون مباشرة بين السلطات المختصّة في الدولتين.

---

[1] باشي، علا شكيب: **التحفظ على المعاهدات الدولية متعددة الأطراف**، رسالة ماجستير، جامعة الشرق الأوسط للدراسات العليا: عمّان– الأردن، 2008، ص15.

[2] عندما تم توقيع هذه الاتفاقية صادقت عليها فلسطين بتاريخ 1983/11/28 إلا أن مصر لم توقع عليها في ذلك الوقت، لكن بعد ذلك أصدر الرئيس عبدالفتّاح السيسي قراراً جمهورياً رقم 278 لسنة 2014 تم بموجبه الموافقة على انضمام مصر لهذه الاتفاقية.

[3] المادة 14 من اتفاقية الرياض العربية للتعاون القضائي.

[4] المادة 15/ب من اتفاقية الرياض العربية للتعاون القضائي.

[5] المادة 15/أ من اتفاقية الرياض العربية للتعاون القضائي.

2. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[1]: والتي صدرت بموجب قرار الجمعية العامة للأمم المتحدة رقم 25 في الدورة الخامسة والخمسون المؤرخ بتاريخ 2000/11/15، ونصّت المادة 1 منها على الهدف من هذه الاتفاقية والذي يتمثل في تعزيز التعاون في منع الجريمة المنظمة عبر الوطنية ومكافحتها بمزيد من الفعالية، ويتم بموجب هذه الاتفاقية تقديم المساعدة القانونية المتبادلة بين الدول الأطراف وذلك فيما يتعلق بالتحقيقات والملاحقات والإجراءات القضائية المتعلقة بالجرائم[2] ومن هذه الإجراءات: أ-الحصول على أدلة ب-تنفيذ عمليات التفتيش والضبط[3].

وبيّنت هذه الاتفاقية البيانات الضرورية الواجب توافرها عند تقديم طلب الإنابة القانونية ومن بينها موضوع وطبيعة التحقيق أو الملاحقة أو الإجراء الجنائي والغرض من جمع الأدلة أو المعلومات[4]، وأكدت الاتفاقية على أن تنفيذ طلب الإنابة القضائية يتم بموجب القانون الداخلي للدولة المتلقية لطلب الإنابة وبشرط أن لا يتعارض الطلب مع قانونها الداخلي[5]، كما ويمكن للدولة رفض تقديم المساعدة بموجب طلب الإنابة إذا رأت أنه قد يؤدي تنفيذه إلى المساس بسيادتها أو أمنها أو نظامها[6].

وفيما يتعلق بالجرائم الإلكترونية فإننا **نرى** أنه يمكن تطبيق هذه الاتفاقية على هذه الجرائم لكن شريطة أن تكون هذه الجرائم منظمة تقوم بها جماعات إجرامية منظمة (جماعات ذات هيكل تنظيمي غير مشكلة عشوائياً مؤلفة من3 أشخاص أو أكثر[7]) مستخدمة في ذلك الوسائل التكنولوجية المختلفة كأن تقوم بجرائم خطيرة يعاقب عليها بالسجن لمدة لا تقل عن 4 سنوات أو بعقوبة أشد[8] مثل جرائم غسل الأموال التي تتم

---

[1] انضمت فلسطين إلى هذه الاتفاقية بتاريخ 2015/1/2 وصادقت عليها بتاريخ 2015/2/1، أما مصر فقامت بالتوقيع عليها في 2000/12/13 وصادقت عليها في 2004/3/5.

[2] مادة 1/18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

[3] مادة 3/18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

[4] مادة 15/18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

[5] مادة17/18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

[6] مادة 21/18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

[7] مادة 2/أ+ ج من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

[8] مادة 2/ب من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

عبر شبكة الإنترنت أو جرائم فساد، وبالتالي نستنتج أنه إذا كانت هذه الجريمة غير منظمة ويتم ارتكابها عشوائياً إما من شخص أو شخصين فإن مثل هذه الجرائم المرتكبة من قبلهم فإنها لا تندرج تحت هذه الاتفاقية ولا يمكن تطبيق الاتفاقية عليها.

3. الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية[1]: تم إبرام هذه الاتفاقية في 2010/12/21 ودخلت حيز النفاذ في 2013/10/5، وهدفت هذه الاتفاقية إلى تعزيز التعاون العربي في مجال منع ومكافحة الجريمة المنظمة عبر الحدود الوطنية[2] في المجالين القضائي والأمني وتجريم الأفعال المكونة لهذه الجريمة واتخاذ تدابير وإجراءات منعها ومكافحتها وملاحقة ومعاقبة مرتكبيها وشركائهم وذلك وفقاً لأحكام الشريعة الاسلامية أو القوانين الوطنية مع مراعاة النظام العام لكل دولة وتسليمهم إلى الدول الطالبة[3].

وتناولت هذه الاتفاقية في الفصل الثالث منها حول التعاون القضائي والقانوني بين الدول العربية الأعضاء، كما وتحدثت عن المساعدة القانونية المتبادلة وإمكانية الإنابة القضائية فيما بينها عند وقوع جريمة مشمولة في الاتفاقية، فيمكن لإحدى الدول أن تطلب من دولة أخرى أن تنيب عنها في القيام بالملاحقة وإجراءات الاستدلال والتحقيق والإجراءات القضائية بما فيها ضبط الأدلة وإجراءات التفتيش والحصول على الأدلة[4]، كما وتطرقت الاتفاقية أيضاً إلى كيفية تقديم طلب الإنابة والشروط الواجب توافرها[5] والحالات التي يمكن فيها رفض الإنابة[6] وكذلك كيفية عملية إجراء الضبط والمصادرة للأشياء المتحصلة عن الجرائم وإجراءات تسليمها بين الدول[7].

---

[1] تم انضمام فلسطين إليها بتاريخ 2010/12/21 وصادقت عليها في 2013/5/21 ، أما مصر فانضمت إليها بتاريخ 2010/12/21.

[2] المادة 1 من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية.

[3] ديباجة الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية.

[4] المادة 1/26 من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية.

[5] المادة 4/26 من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية.

[6] المادة 27 من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية.

[7] المادة 32 من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية.

وترى الباحثة هنا أن هذه الاتفاقية ما هي إلا صورة طبق الأصل عن اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية وأن الاختلاف يكمن في أن هذه الأخيرة تطبق بشكل دولي وتشمل دول أجنبية وعربية بينما الاتفاقية العربية هي مقتصرة على الدول العربية فقط، وتتشابه الاتفاقيتين في مجال تطبيقها على الجرائم الإلكترونية إذ إنه يشترط أن تكون الجريمة الإلكترونية عابرة الحدود المرتكبة من قبيل الجرائم المنظمة والتي يتم ارتكابها من قبل مجموعات منظمة ومحددة كالجرائم التي يتم فيها استعمال غير مشروع لتقنية أنظمة المعلومات من تعطيل أو تحريف أو اختراق كما أنه يمكن أن تكون جرائم تقليدية لكن تم ارتكابها بإحدى وسائل تقنية أنظمة المعلومات، بالتالي إذا كانت الجريمة غير منظمة ومرتكبة من شخص أيضاً غير تابع لأي جماعة منظمة وحتى لو نتجت آثارها في دولة أخرى فإن لا يمكن تطبيق هذه الاتفاقية على مثل هذه الحالة.

وهناك اتفاقيات جماعية تم عقدها بشأن الجرائم الإلكترونية ومن هذه الاتفاقيات:

أ. الاتفاقية الأوروبية بشأن الجريمة المعلوماتية: وتم عقد هذه الاتفاقية بتاريخ 2001/11/23 وتعتبر أهم اتفاقية تم إبرامها على مستوى دولي وتُعنى بالجرائم الإلكترونية، وعملت هذه الاتفاقية على تنظيم أحكام هذه الجرائم سواء من الناحية الموضوعية أو من الناحية الإجرائية، كما وسعت إلى تعزيز التعاون بين الدول الأعضاء من خلال الدعوة إلى ضرورة اتباع سياسة جنائية مشتركة لحماية المجتمع الدولي من الجريمة الإلكترونية وإلى مكافحة الجريمة الإلكترونية بشكل فعّال من خلال التعاون القضائي الدولي في المسائل الجنائية[1].

وتضمنت هذه الاتفاقية المبادئ العامة التي تحكم المساعدة المتبادلة بين الدول الأطراف وذلك في المادة 25 منها، بحيث يتوجب على كل من دول الأطراف أن تقدم المساعدة على أوسع نطاق وذلك في مجال إجراء التحقيق وفي كافة الإجراءات المتعلقة بالجرائم الإلكترونية الواردة في الاتفاقية وكذلك في إجراءات

[1] ديباجة الاتفاقية الأوروبية بشأن الجريمة المعلوماتية بودابيست.

جمع الأدلة المتعلقة بالجرائم الإلكترونية[1] ويقع على عاتق كل دولة طرف القيام بكافة التدابير التشريعية لتنفيذ جميع الالتزامات الواردة في المواد 27-35 من هذه الاتفاقية[2].

وفيما يتعلق بالظروف العاجلة والتي تتطلب سرعة في اتخاذ الإجراءات فإنه يجوز لكل دولة طرف أن تطلب المساعدة بواسطة وسائل الاتصال المختلفة كالفاكس أو البريد الإلكتروني مع ضرورة مراعاة المحافظة على البيانات وعلى أن تقبل الدولة المطلوب منها تقديم المساعدة وتستجيب لهذا الطلب بواسطة أي وسيلة من وسائل الاتصال العاجلة[3].

وتخضع المساعدة المتبادلة وتنفيذ الطلب إلى قانون الدولة الطرف المطلوب منها المساعدة أو وفقاً للمعاهدات المنضمة إليها وتتعلق بالمساعدة المتبادلة، وتقوم هذه الدولة بتقديم المساعدة بغض النظر عمّا إذا كانت قوانينها تدرج الجريمة داخل التصنيف ذاته أو في تصنيف آخر طالما أن الفعل يعتبر جريمة بموجب قانونها[4]، وتناولت الاتفاقية أحكاماً خاصّة تتعلق بالإجراءات المؤقتة والعاجلة عند القيام بالمساعدة المتبادلة ومن هذه الأحكام أنها أجازت لأي دولة طرف أن تقوم بتقديم طلب لدولة أخرى وتأمرها لاتخاذ إجراءات مستعجلة للحفاظ على بيانات مخزنة على أنظمة معلوماتية متواجدة لديها وعلى أراضيها، ويعود الهدف من هذا الإجراء المستعجل للحفاظ على البيانات والمعلومات المخزنة حتى يتسنى للدولة تقديم طلب للمساعدة من أجل إجراء التفتيش على البيانات والقدرة على النفاذ إليها أو مصادرتها[5]، ويشترط بالطلب المستعجل للحفظ أن يتم تحديد فيه الجهة الطالبة للحفظ ونوع الجريمة والبيانات والمعلومات المخزنة على الأنظمة وعلاقتها بهذه الجريمة والأسباب التي دعت إلى القيام بحفظ البيانات ونوع الإجراء الذي سيتم طلب تنفيذه من خلال طلب المساعدة المتبادلة كإجراء النفاذ إلى البيانات والتفتيش عليها وضبطها[6]، ويقع

---

[1] المادة 1/25 من الاتفاقية الأوروبية بشأن الجريمة المعلوماتية بودابيست.

[2] المادة 2/25 من الاتفاقية الأوروبية بشأن الجريمة المعلوماتية بودابيست.

[3] المادة 3/25 من الاتفاقية الأوروبية بشأن الجريمة المعلوماتية بودابيست.

[4] المادة 4/25 من الاتفاقية الأوروبية بشأن الجريمة المعلوماتية بودابيست.

[5] المادة 1/29 من الاتفاقية الأوروبية بشأن الجريمة المعلوماتية بودابيست.

[6] المادة 2/29 من الاتفاقية الأوروبية بشأن الجريمة المعلوماتية بودابيست.

على عاتق الدولة المطلوب منها إجراء الحفظ أن تقوم مباشرة باتخاذ كافة الإجراءات للتعجيل في حفظ البيانات المحددة وفقاً لقانونها الداخلي[1]، وعلى أن يستمر هذا الحفظ لمدة لا تقل عن 60 يوماً حتى تتمكن الدولة طالبة الحفظ خلال هذه الفترة من تقديم طلب المساعدة لإجراء التفتيش والضبط للأدلة[2]، ويمكن للدولة رفض طلب الحفظ للبيانات إذا ما كانت الجريمة تشكّل جريمة سياسية أو مرتبطة بجريمة سياسية أو إذا كان تنفيذ هذا الطلب سيؤدي إلى إلحاق الضرر بسيادتها أو نظامها العام أو مصالحها[3].

لذا يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث والتنقيب والتفتيش عن بيانات ومعلومات مخزّنة على نظام معلوماتي موجود لدى الدولة الأخرى[4]، وعلى أن تقوم هذه الأخيرة بالاستجابة لطلب المساعدة بأسرع وقت ممكن خاصّة إذا كان هنالك خشية من ضياع أو تعديل أو إتلاف للبيانات أو إذا كانت القوانين والاتفاقيات تنصّ على التعجيل في التعاون القضائي بين الدول الأطراف[5].

وترى الباحثة هنا أن الاتفاقية الأوروبية للجرائم المعلوماتية قد تناولت موضوع الإنابة القضائية أو المساعدة القضائية المتبادلة بشكل جيّد لا سيما فيما يتعلق باتخاذ إجراءات سريعة للمحافظة على البيانات والمعلومات المخزنة على الأنظمة المعلوماتية وكذلك تسهيل إجراء التفتيش عليها وضبطها، فهذا الأمر يتناسب تماماً مع طبيعة الجرائم الإلكترونية والتي بحاجة إلى اتخاذ إجراءات سريعة دون الدخول في تعقيدات وشكليات مما يؤدي إلى الحفاظ على الأدلة وحمايتها من الفقدان، كما وأصابت الاتفاقية عندما نصّت على الإجراءات التي يمكن اتخاذها في حالة عدم وجود اتفاقية وكانت الدولة بحاجة إلى المساعدة القضائية فيمكن في الحالات الطارئة أن يتم التواصل بين السلطات القضائية في الدولتين بصورة مباشرة لطلب المساعدة المتبادلة أو من خلال المنظمة الدولية للشرطة الجنائية الإنتربول.

---

[1] المادة 3/29 من الاتفاقية الأوروبية بشأن الجريمة المعلوماتية بودابيست.

[2] المادة 7/29 من الاتفاقية الأوروبية بشأن الجريمة المعلوماتية بودابيست.

[3] المادة 5/29 من الاتفاقية الأوروبية بشأن الجريمة المعلوماتية بودابيست.

[4] المادة 1/31 من الاتفاقية الأوروبية بشأن الجريمة المعلوماتية بودابيست.

[5] المادة 2/31+3 من الاتفاقية الأوروبية بشأن الجريمة المعلوماتية بودابيست.

ب. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: تم إبرامها بتاريخ 2010/12/21 وسعت الدول العربية من خلالها إلى تعزيز التعاون العربي الدولي لمكافحة جرائم تقنية المعلومات (الجرائم الإلكترونية) والتي يمكن أن تهدد أمنها وسلامة مجتمعها ومصالحها، وكذلك إلى إيجاد سياسية جنائية مشتركة تهدف إلى حماية المجتمع العربي ككل من الجرائم الإلكترونية مع ضرورة مراعاة النظام العام لكل دولة[1].

وأكدت هذه الاتفاقية على تبادل المساعدة القانونية والقضائية بين الدول الأطراف وذلك في إجراء التحقيقات أو في القيام بالإجراءات المتعلقة بجرائم المعلومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية[2]، ويقدم طلب المساعدة المتبادلة بشكل خطّي على أنه يمكن أن يكون بشكل مستعجل عن طريق الاتصالات بواسطة الفاكس أو البريد الإلكتروني إذا ما توافرت إحدى الحالات الطارئة والضرورية شريطة أن توفر وسائل الاتصالات هذه الأمن والمحافظة على البيانات وذلك باستخدام التشفير ويشترط على الدولة المطلوب منها المساعدة أن تستجيب لهذا الطلب بصورة عاجلة دون تأخير[3].

ويتم تطبيق طلب المساعدة المتبادلة وفقاً لقانون الدولة المطلوب منها المساعدة أو وفقاً للمعاهدات الثنائية إذا ما كان هناك معاهدات للمساعدة المتبادلة فيما بينها ولا يمكن للدولة المطلوب المساعدة منها رفض الطلب لأن الجريمة تعتبر جريمة مالية[4]، ويشترط في المساعدة المتبادلة أن يكون هناك ازدواجية في التجريم أي أن الفعل مجرّم لدى الدولتين بغض النظر إذا كانت هذه الجريمة تحمل ذات التصنيف أم لا فالمهم هو أن الفعل يعتبر جريمة لدى الدولة المطلوب منها المساعدة[5].

---

[1] ديباجة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2] المادة 1/32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3] المادة 3/32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[4] المادة 4/32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[5] المادة 5/32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

ويمكن لأي دولة طرف في هذه الاتفاقية أن تطلب من دولة طرف أخرى البحث والوصول والتفتيش والضبط لمعلومات تقنية مخزّنة على نظام معلوماتي موجودة لدى الطرف المطلوب منها المساعدة[1] ويتم الاستجابة من هذه الأخيرة بصورة عاجلة خاصة إذا ما كانت عرضة للفقدان أو التعديل[2]، وفي حالة إذا كانت المعلومات متوافرة للعامة على مصدر مفتوح فإنه يمكن لأي دولة طرف ودون الحصول على تفويض من الدولة الموجود لديها المعلومات أن تصل لهذه المعلومات تبحث فيها وتجري التفتيش عليها[3].

وأكدت الاتفاقية على ضرورة التعاون والمساعدة الثنائية المتبادلة بين دولتين طرف للجمع الفوري والمستعجل لمعلومات تتبع المستخدمين المصاحبة لاتصالات معينة في أقاليمها والتي تثبت باستخدام وسائل تقنية المعلومات[4]، كما وتقوم الدولتين بتوفير المساعدة الثنائية لبعضهما فيما يتعلق بالجمع الفوري لمعلومات المحتوى لاتصالات معيّنة تبث بواسطة تقنية المعلومات وذلك ضمن الحد المسموح بحسب المعاهدات المطبقة والقوانين[5].

ولضمان توفير المساعدة الفورية لغايات التحقيق أو الاجراءات المتعلقة بجرائم تقنية المعلومات فقد نصّت الاتفاقية على أنه على كل دولة طرف وفقاً للمبادئ الأساسية لنظامها القانوني أن توفر جهاز متخصص ومتفرغ على مدار الساعة يعمل على تسهيل تقديم طلب المساعدة المتبادلة أو تنفيذها بشكل سلس ويقدم المشورة الفنية التي قد تحتاجها الدولة ويحمي المعلومات ويحافظ على سريتها ويقوم بجمع الأدلة وتحديد مكان المشبوهين[6] ويكون التواصل مباشر بين هذه الأجهزة في كل من الدولتين[7].

---

[1] المادة 1/39 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2] المادة 2/39+3 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3] المادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[4] المادة 1/41 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[5] المادة 42 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[6] المادة 1/43 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[7] المادة 2/43 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

ويتم تطبيق هذه الاتفاقية على كافة جرائم تقنية المعلومات (الجرائم الإلكترونية) للتحقيق فيها وملاحقة مرتكبيها وسواء تم ارتكابها من شخص أو مجموعة أشخاص منظمة طالما أن الجريمة هي عابرة للحدود، فإنه يتم بموجب هذه الاتفاقية ملاحقة الشخص وإجراء التحقيق والتفتيش على الأدلة أ–إذا ارتكبت في أكثر من دولة عربية ب–ارتكبت في دولة وتم الاعداد والتخطيط لها في دولة أو دول أخرى ج–إذا تم ارتكابها من قبل جماعة إجرامية منظمة تمارس جرائمها في أكثر من دولة د–إذا ارتكبت في دولة وكان لها آثاراً شديدة في دولة أو دول أخرى[1]، وقامت كل من فلسطين[2] ومصر[3] بالتوقيع على هذه الاتفاقية وإصدار القوانين المتعلقة بالجرائم الإلكترونية مراعيةً في ذلك أن تنسجم أحكام هذه القوانين مع هذه الاتفاقية والتأكيد على ضرورة التعاون وتبادل المساعدة القضائية الدولية لمكافحة الجريمة الإلكترونية.

ونستنتج مما سبق أن الجرائم الإلكترونية عابرة الحدود عند إجراء التفتيش عليها فإنها بحاجة إلى إجراءات أكثر مما لو كانت جريمة إلكترونية محلية، بحيث يتم اللجوء للإنابة القضائية الدولية من خلال الاستعانة بالطرق الدبلوماسية وإرسال طلب من الجهات القضائية متضمناً الملف الخاص بالدعوى الجنائية ومرفقاته من مستندات ووثائق ومحاضر التحقيق إذا ما كان قد تم البدء فيها من قبل السلطة القضائية المختصة في الدولة[4]، ويصدر الطلب من قبل النيابة العامة وعبر وزارة العدل والذي يشترط فيه أن يكون مؤرخاً وموقعاً عليه ومختوماً من قبل الجهة طالبة المساعدة القضائية هو وسائر الأوراق، كما ويشترط في الطلب أن يكون متضمناً صراحةً طلب إجراء الإنابة وكل ما يتعلق بالقضية والأمور المراد القيام بها من معاينة أو استجواب أو إجراء تفتيش أو سماع الشهود وغير ذلك من الإجراءات[5].

---

[1] المادة 3 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2] قامت فلسطين بالتوقيع على الاتفاقية بتاريخ 2010/12/21 وصادقت عليها بتاريخ 2013/5/21.

[3] قامت مصر بالتوقيع عليها بموجب قرار رئيس الجمهورية رقم 276 لسنة 2014 ومع التحفظ بشرط التصديق.

[4] فضل، سليمان أحمد: **المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية**، مرجع سابق، ص425+426.

[5] الخضري، سمر خضر صالح: **أحكام تسليم المجرمين في فلسطين" دراسة تحليلية"**، مرجع سابق، ص28.

ويعتبر المسؤول عن تقديم طلبات الإنابة والمساعدة القضائية في فلسطين هي وحدة في النيابة العامة أطلق عليها مسمى نيابة التعاون الدولي حيث تختص هذه الوحدة بإعداد طلبات الإنابة أو المساعدة القضائية لسماع أقوال الشهود وضبط للأشياء وتفتيش الأشخاص والأماكن ومن ثم تصديق هذه الطلبات لإرسالها إلى الجهات القضائية في الدولة المطلوب منها تنفيذ طلب الإنابة أو المساعدة القضائية[1]، أما في مصر فالوحدة المسؤولة عن هذه الطلبات تدعى إدارة التعاون القضائي الدولي وهي تابعة للنيابة العامة وتختص في الإنابات القضائية من خلال إرسال الطلب إلى شؤون الأجانب والتصديقات بوزارة الخارجية التي بدورها تقوم بإرسال الطلب ومرفقاته إلى وزارة الخارجية للدولة المراد منها تنفيذ الإنابة[2].

[1] موقع النيابة العامة الفلسطينية:
http://www.pgp.ps/ar/SP/Pages/InternationalCrimes-CooperationProsecution.aspx

[2] موقع بوابة وزارة العدل المصرية: http://departmentic.jp.gov.eg/competence_m

الفصل الثاني

كيفية إجراء التفتيش في الجرائم الإلكترونية

لقد بيّنا في الفصل السابق من هذا البحث حول إجراء التفتيش في الجرائم الإلكترونية والقواعد الموضوعية والشكلية التي تحكمه عند إجرائه، إذ تتشارك الجرائم الإلكترونية في هذه القواعد مع الجرائم التقليدية العادية لكنها تختلف عنها بأنها بحاجة إلى قواعد وإجراءات خاصّة عند القيام بهذا الإجراء على الوسائل التكنولوجية المختلفة وذلك لتتمكن الجهات المختصة من الوصول إلى الأدلة الإلكترونية وضبطها، فهذه الأدلة ليست كالأدلة العادية التي تنتج عن الجرائم العادية وإنما هي أدلة تحتاج إلى طرق خاصة وتقنيات معينة وأشخاص يتمتعون بخبرة تقنية للتعامل معها والتفتيش والبحث والتنقيب عنها ليتم إحرازها وحفظها حتى لا يتم فقدانها وضياعها، إذ إن ضياع هذه الأدلة يؤدي إلى عدم القدرة على إثبات الجريمة ونسبتها إلى المتهم.

ونظراً للخصوصية التي تتمتع بها الأدلة الإلكترونية فإن ذلك أدى إلى وجود صعوبات عديدة تقف أمام الجهات المختصة بالتفتيش والتي تعيق عملها أحياناً، وهذه الصعوبات قد تتعلق بالجريمة المرتكبة وبالأدلة الناتجة عنها أو بالجهات المختصة بإجراء التفتيش، ونتحدث في هذا الفصل حول آلية إجراء التفتيش في الجرائم الإلكترونية والقواعد التي يتم اتباعها وكيفية ضبط الأدلة والتعامل معها ومن ثم نستعرض أهم الصعوبات التي تعيق إجراء التفتيش، وعليه سنقسم هذا الفصل إلى:

المبحث الأول: الآلية المتبعة عند إجراء التفتيش في الجرائم الإلكترونية

المبحث الثاني: ضبط الأدلة المتحصلة من إجراء التفتيش في الجرائم الإلكترونية

المبحث الأول: الآلية المتبعة عند إجراء التفتيش في الجرائم الإلكترونية

كما أسلفنا أن إجراء التفتيش بشكل عام يكون للبحث والتنقيب عن الأدلة والأشياء وذلك في سبيل الكشف عن الجريمة وإظهاراً للحقيقة ومن ثم ضبط الأدلة ليتسنى نسب التهمة إلى المتهم.

ويمتاز التفتيش في الجرائم الإلكترونية بأنه يتم استخدام فيه تقنيات وأساليب فنية خاصة للتنقيب والبحث عن الأدلة والتي قد تكون أدلة مادية وأدلة معنوية وذلك على عكس الجرائم العادية التي يتم فيها إجراء التفتيش التقليدي العادي والذي يكون في الغالب للبحث عن أدلة مادية.

وتتنوع الأدلة الإلكترونية التي يتم التعامل معها كتلك الأدلة التي تتعلق بشبكات الإنترنت والحواسيب، وقد تكون هذه الأدلة مخزنة على وسائل تكنولوجية تتواجد داخل حدود إقليم الدولة والتي يمكن الوصول إليها بشكل سريع، وأدلة إلكترونية أخرى تكون مخزنة على وسائل تكنولوجية تتواجد خارج حدود الدولة والتي تتطلب جهد ووقت كبير للوصول إليها والتنقيب عنها، وعليه نقسم هذا المبحث إلى مطلبين وهما:

المطلب الأول: السلطات المختصّة بإجراء التفتيش في الجرائم الإلكترونية

المطلب الثاني: القواعد المتبعة في إجراء التفتيش في الجرائم الإلكترونية

المطلب الأول: السلطات المختصّة بإجراء التفتيش في الجرائم الإلكترونية

طالما أن إجراء التفتيش هو أحد إجراءات التحقيق الابتدائي فالأصل فيه أن يتم إجراؤه من قبل سلطات التحقيق المختصّة إلا أنه هناك بعض الحالات الاستثنائية التي أجاز فيها المشرع أن يتم إجراء التفتيش من قبل جهات أخرى لذلك هناك نوعين من السلطات التي تقوم بإجراء التفتيش وهما السلطة الأصلية المخولة بإجرائه والسلطة الاستثنائية التي يتم تفويضها لإجرائه.

الفرع الأول: السلطة الأصلية المختصة بإجراء التفتيش

وتتمثل هذه السلطة في فلسطين بالجهة المختصّة بالتحقيق وهي النيابة العامة وذلك سنداً للمادة 1/55 من قانون الإجراءات الجزائية الفلسطيني: "تختصّ النيابة العامة دون غيرها بالتحقيق في الجرائم والتصرّف فيها"، أما في مصر فقد نصّ قانون الإجراءات الجنائية المصري في المادة 64على أن الجهة المختصّة بالتحقيق تتمثل في النيابة العامة بصورة أصلية وفي قاضي التحقيق في حالات خاصّة، بالتالي يمكن لكافة أعضاء النيابة العامة القيام بإجراء التحقيق فيما عدا معاون النيابة العامة الذي يتمتع بذات الصلاحيات التي يتمتع بها مأمور الضبط القضائي في هذا الصدد[1].

ويشترط في السلطة الأصلية أن تكون مختصة بالتحقيق في الجريمة ويكون هذا الاختصاص إما اختصاص نوعي أو اختصاص مكاني[2]، ويتمثل الاختصاص النوعي بالقيام بإجراء التحقيق في نوع معيّن من الجرائم، وعلى الرغم من أن النيابة العامة ينعقد لها الاختصاص بإجراء التحقيق في كافة الجرائم إلا أنّ في هذه النيابة تكون الاختصاصات مقسّمة أي بمعنى أن يكون لكل نيابة مختصّة بنوع معيّن من الجرائم، فالنيابة المتخصصة بالجرائم الإلكترونية تختص بإجراء التحقيق في الجرائم الإلكترونية التي يتم ارتكابها بواسطة وسائل تكنولوجيا المعلومات، وإذا قامت نيابة أخرى غير النيابة المختصة بالجرائم الإلكترونية وعملت على إجراء التحقيق بجريمة إلكترونية فهذا ليس باطلاً؛ وذلك لأن النيابة المختصة بالجرائم الإلكترونية لا تنشأ بموجب نص قانوني وإنما بموجب قرار تنظيمي وبالتالي فإنه لا يمكن منع النيابات الأخرى من القيام بإجراء التحقيق في الجرائم الإلكترونية[3].

---

[1] الشهاوي، قدري عبدالفتاح: **مناط التفتيش**، مرجع سابق، ص148.

[2] هروال، نبيلة هبة: **الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات" دراسة مقارنة"**، مرجع سابق، ص241.

[3] راسخ، إبراهيم: **التحقيق الجنائي العلمي**، الطبعة الأولى، دبي–الإمارات: أكاديمية شرطة دبي" كلية القانون وعلوم الشرطة"، 1991،ص389.

أما فيما يتعلق بالاختصاص المكاني فهو يتمثل باختصاص السلطة المختصة بإجراء التحقيق في دائرة معينة ولا يجوز لها القيام بالتحقيق في دائرة أخرى ليس من اختصاصها وينعقد الاختصاص المكاني إما بمكان وقوع الجريمة أو بالمكان الذي يقيم فيه المتهم أو في المكان الذي يقبض عليه[1].

لذلك تعد النيابة العامة هي السلطة الأصلية المختصة بإجراء التفتيش في الجرائم الإلكترونية، وتتولى في ذلك نيابة متخصصة وهي نيابة مكافحة الجرائم الإلكترونية كون أن التفتيش في هذه الجرائم بحاجة إلى خبرة والقدرة على البحث عن الأدلة الإلكترونية في الوسائل التكنولوجية المختلفة، وتقوم هذه النيابة بإجراءات التفتيش وتتعاون مع وحدات مكافحة الجرائم الإلكترونية التابعة لأجهزة الشرطة والأجهزة الأمنية ذات الاختصاص، كما وتعمل على التواصل مع الجهات الرسمية والمؤسسات والشركات المتخصصة بالجرائم الإلكترونية والاتصالات والحصول على الدليل الإلكتروني ومن ثم نسب التهمة إلى المتهم وتعمل هذه النيابة بسرعة عالية وسرية ممكنة حتى لا يتم فقدان الأدلة[2].

الفرع الثاني: السلطة الاستثنائية المختصة بإجراء التفتيش

هناك حالات عديدة تؤدي إلى قيام السلطة الأصلية المختصة بإنابة سلطات أخرى لتقوم بإجراءات التحقيق والتي من بينها إجراء التفتيش، ومن هذه الحالات كثرة المهام التي تقع على عاتق السلطات المختصة وكذلك وقوع الجريمة في دائرة ليست من اختصاصها، لذلك تلجأ إلى إنابة السلطات الأخرى لمباشرة بعض الإجراءات، وهذه السلطات إما أن تكون السلطة المختصّة بالتحقيق إذا كانت الجريمة المرتكبة في دائرة أخرى ليست ضمن اختصاصها المكاني، أو سلطة استثنائية متمثلة بمأموري الضبط القضائي ويكون ذلك عندما لا تستطيع السلطة المختصّة بالتحقيق مباشرة إجراء معيّن فيتم إنابة مأمور الضبط القضائي[3]، لذا

---

[1] مادة 163 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001و 217 من قانون الاجراءات الجنائية المصري رقم 150 لسنة 1950.

[2] الموقع الرسمي للنيابة العامة في فلسطين:
https://www.pgp.ps/ar/SP/Pages/TheAnti-CyberCrimesProsecution.aspx

[3] عبدالباقي، مصطفى: **شرح قانون الإجراءات الجزائية الفلسطيني**، مرجع سابق، ص190.

فإن الضرورة العملية والإجرائية هي التي تبرر اللجوء إلى إنابة مأموري الضبط القضائي لمباشرة الإجراءات لما في ذلك من ضمان حسن سير العمل وانجاز المهام في أسرع وقت ممكن[1].

ويقصد بالإنابة أو الندب بالتفتيش: أنه نوع من أنواع تفويض السلطة الأصلية لمأموري الضبط القضائي للقيام بإجراء التفتيش، وبالتالي قيام مأموري الضبط القضائي بإجراء التفتيش يعتبر استثناءً على الأصل وأجاز لهم القانون بذلك لاعتبارات عملية[2].

وحدد المشرع الفلسطيني في نص المادة 21 من قانون الإجراءات الجزائية والمشرع المصري في المادة 23 من قانون الإجراءات الجنائية الفئات الممنوحة صفة مأموري الضبط القضائي وتقسيمهم إلى نوعين فمنهم من يكون من ذوي الاختصاص العام كضباط صف الشرطة وضباط إدارة المباحث العامة، ومنهم من يكون ذوي الاختصاص الخاص كالموظفين الذين يتم اكسابهم هذه الصفة بموجب القانون وذلك بالنسبة للجرائم التي تقع ضمن دائرة اختصاصهم وتتعلق بأعمال وظائفهم ويتم تخويلهم بذلك من خلال قرار صادر من وزير العدل وبالاتفاق مع الوزير المختص.

ويشترط في مأمور الضبط القضائي الذي يتم انتدابه لمباشرة الإجراء أن: أ-يكون مختصاً نوعياً بإجراء التفتيش على نوع معين من الجرائم، فمأمور الضبط القضائي ذوي الاختصاص الخاص لا يمكن له إجراء التفتيش في جريمة لا تدخل ضمن نطاق عمله إلا أنه يمكن لذوي الاختصاص العام إجراء التفتيش بشأن جريمة تدخل ضمن اختصاص من ذوي الاختصاص الخاص ب-يكون مختصاً مكانياً بحيث تكون

---

[1] الهيتي، بلال محمود مرهج: **الجرم المشهود وأثره في توسيع سلطات الضابطة العدلية دراسة مقارنة بين القانونين الأردني والعراقي**، رسالة ماجستير، جامعة الشرق الأوسط للدراسات العليا، الأردن، 2010-2011، ص 112.

[2] ثروت، جلال وعبدالمنعم ، سليمان: **أصول المحاكمات الجزائية" الدعوى الجنائية"**، الطبعة الأولى، بيروت-لبنان: المؤسسة الجامعية للدراسات والنشر والتوزيع، 1996، ص439.

الجريمة التي يجري التفتيش بشأنها قد حدثت ضمن دائرة عمله أو المتهم يقيم في هذه الدائرة أو تم إلقاء القبض على المتهم في هذه الدائرة[1].

ويتمتع مأمورو الضبط القضائي بذات الصلاحيات التي يتمتع بها السلطة المختصة عند إجراء التفتيش ويترتب عليه كافة الآثار القانونية كما لو كانت السلطة المختصة بإجرائه هي من قامت به وقد أكد على ذلك كل من القانون الفلسطيني والمصري[2]، ويتم تحديد سلطاتهم بإرادة جهة التحقيق من خلال:-

أ. النطاق الموضوعي إذ تتمثل سلطات مأمور الضبط القضائي في قيامه بعمل أو أكثر من الأعمال التحقيقية الواردة والمحددة في قرار الندب وعلى مأمور الضبط الالتزام بموضوع الندب ولا يجوز له تجاوزه، فلو كان مثلاً موضوع قرار الندب هو القيام فقط بإجراء تفتيش الشخص فإنه لا يجوز تفتيش شيء آخر فيجب عليه القيام فقط بإجراء تفتيش الشخص.

ب. النطاق الزمني ويعني التزام مأمور الضبط بالمدة الزمنية المقررة في قرار الندب وإذا قام بإجراء التفتيش بعد انتهاء المدة المحددة في القرار فإنه يكون هذا الإجراء باطلاً، وإذا لم يتوافر أي مدة في القرار فإن ذلك لا يعني أن يتراخى مأمور الضبط في تنفيذ موضوع الندب وإنّما عليه إنجازه في أقرب فرصة وأسرع وقت ممكن.

ج. في النطاق الإجرائي: فهناك مجموعة من القيود الإجرائية التي تحيط بمأمور الضبط القضائي عند قيامه بتنفيذ موضوع قرار الندب، ومن هذه القيود أن قرار الندب يصدر لعضو مأمور ضبط معين فلا يمكن لعضو آخر القيام به ووجوب تدوين ما يتعلق بالإجراء في محضر التفتيش[3].

---

[1] طنطاوي، إبراهيم حامد: **الدفع ببطلان إذن النيابة العامة بالتفتيش**، مرجع سابق، ص30.

[2] مادة 55 من قانون الإجراءات الجزائية الفلسطيني رقم 3لسنة2001ومادة 70 من قانون الاجراءات الجنائية المصري رقم 150 لسنة 1950.

[3] ثروت، جلال وعبدالمنعم، سليمان: **أصول المحاكمات الجزائية**، مرجع سابق، ص440 وما بعدها.

وكون أن الجرائم الإلكترونية هي من الجرائم الصعبة التي تكون بحاجة إلى تعامل خاص معها ومع الأدلة التي تنتج عنها، لذلك تم إنشاء بموجب القرار بقانون الفلسطيني وحدة متخصصة في جهاز الشرطة وقوى الأمن من مأموري الضبط القضائي والتي تسمى بوحدة الجرائم الإلكترونية[1]، وفي مصر فقد تم تأسيس مباحث الإنترنت وهي إدارة مكافحة جرائم الحاسبات وشبكة المعلومات التابعة لقطاع نظم الاتصالات وتكنولوجيا المعلومات بوزارة الداخلية.

وعملت التشريعات المتعلقة بالجرائم الإلكترونية أيضاً على منح موظفي وزارة الاتصالات وتكنولوجيا المعلومات صفة مأموري الضبط القضائي، فالمشرع الفلسطيني كان قد نصّ على ذلك في المادة 54 من القرار بقانون المتعلق بالجرائم الإلكترونية إلا أنه وبعد التعديل الذي جرى على القرار بقانون تم إلغاء هذه المادة[2]، أما المشرع المصري[3] فقد نصّ على أنه يمكن لوزير شؤون الاتصالات وتكنولوجيا المعلومات أن يستصدر قرار من قبل وزير العدل بمنح صفة الضبط القضائي للعاملين أو غيرهم ممن تحددهم جهات الأمن القومي(وزارة الدفاع، وزارة الداخلية، المخابرات وهيئة الرقابة الإدارية) وعلى أن يقوموا ممن منحوا هذه الصفة بإجراء التفتيش في الجرائم الإلكترونية الواردة في هذا القانون[4].

وترى الباحثة هنا أن المشرع الفلسطيني قد أصاب في إلغاء المادة كون أنه يوجد وحدة متخصصة من مأموري الضبط القضائي وهي وحدة الجرائم الإلكترونية والتي تكون مدرّبة ومجهزة وبالتالي هي أجدر للتعامل مع مختلف الجرائم الإلكترونية، لذلك القيام بمنح صفة الضبط القضائي لفئات عديدة ومختلفة كموظفين أو عاملين في وزارات أخرى أمر غير جيّد وذلك لما فيه من مساس بحقوق وحريات الأفراد،

[1] انظر المادة 3 من القرار بقانون الفلسطيني رقم 10 لسنة 2018بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] انظر المادة 26 من القرار بقانون رقم 38 لسنة 2021 لتعديل القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[3] المادة 5 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.

[4] المري، بهاء: **شرح قانون مكافحة جرائم تقنية المعلومات وحجية الدليل الرقمي في الإثبات**، مصر: العربية للنشر والتوزيع، 2019، ص50

ويمكن الاستفادة من موظفي وزارة الاتصالات وتكنولوجيا المعلومات وغيرهم من خلال الاستعانة بهم في تقديم المساعدة والمشورة الفنية والخبرات فقط لمن يقوم بإجراء التفتيش

المطلب الثاني: القواعد المتبعة في إجراء التفتيش في الجرائم الإلكترونية

إن إجراء التفتيش في الجرائم الإلكترونية يتم على مختلف الوسائل التكنولوجية ومن الوسائل التي يتم استخدامها بشكل كبير وواسع هي الحواسيب والهواتف الذكية والشبكات الإلكترونية والبريد الإلكتروني ونتحدث في هذا المطلب حول بعض هذه الوسائل، لكن قبل الحديث عن كيفية إجراء التفتيش عليها فإنه لا بدّ من معرفة مدى قابلية المكونات المادية والمعنوية للوسائل التكنولوجية لإجراء التفتيش عليها، ومن ثم التطرق إلى أهم الخطوات التي تمكّن القائمين بإجرائه من إنجاح هذا الإجراء وتحقيق أهدافه.

الفرع الأول: مدى قابلية المكونات المادية والمعنوية للوسائل التكنولوجية لإجراء التفتيش عليها

أولاً: إجراء التفتيش على المكونات المادية لوسائل تكنولوجيا المعلومات

ويقصد بهذه المكونات المادية بأنها كافة الأجهزة الملموسة والتي تستخدم في إدخال ومعالجة وإخراج البيانات والمعلومات[1].

وفي الحقيقة أن إجراء التفتيش على المكونات المادية لوسائل تكنولوجيا المعلومات لا يثير أي خلاف حول جواز تفتيشها طالما أنه تم ذلك وفقاً للقانون[2]، ويسري حكم التفتيش على هذه المكونات وفقاً للمكان الموجودة فيه ولطبيعة هذا المكان فإذا كانت الوسيلة موجودة مع الشخص فيطبق عليها حكم إجراءات التفتيش على الأشخاص وإذا كانت في مسكن المتهم أو أحد ملحقاته فيسري عليه حكم تفتيش المسكن[3]،

[1] قرون، نورهان وبوضياف، جهاد والعيفة، رحيمة: *تكنولوجيا المعلومات والاتصال كركيزة أساسية لعملية التدريب الإلكتروني*، **مجلة التعليم عن بعد**، جامعة بني سويف اتحاد الجامعات العربية، مجلد8، عدد15/ديسمبر 2020 ص46.

[2] حسنية، أحمد أسامة: *الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية*، **مرجع سابق**، ص29.

[3] الفيل، علي: *إجراءات التحقيق الابتدائي في الجريمة المعلوماتية" دراسة مقارنة"*، **مجلة الحقوق**، مجلد8، بلا عدد، ص459.

وذلك لإجراء التفتيش عليها هو للبحث عن شيء ما يتصل بجريمة إلكترونية قد وقعت وأن هذا الإجراء من شأنه أن يفيد في كشف الحقيقة.

وتتكون هذه المكونات من:

1. وحدات الإدخال التي تعتبر حلقة وصل بين المستخدم والجهاز الإلكتروني ويتم استخدامها في إدخال البيانات والبرامج إلى وحدة التشغيل الرئيسية[1].
2. وحدة المعالجة المركزية التي تشكل الجزء الأساسي والدماغ المسيطر على جميع العمليات التي يقوم بها الحاسوب بحيث يتم فيها معالجة كافة البيانات الداخلة لتوليد المخرجات المطلوبة وهي تتكون من وحدة الحساب والمنطق ووحدة التحكم ووحدة الذاكرة الرئيسية[2].
3. وحدة الإخراج والتي تعمل على استخراج نتائج الاتصال بين المستخدم والجهاز الإلكتروني والمتولدة عن عمليات المعالجة من وحدة المعالجة المركزية إلى الجهات المستفيدة[3].
4. وحدة الذاكرة الثانوية: ويتم استخدامها عندما يكون هناك كميات كبيرة من المعلومات المراد تخزينها على الحاسوب ولا يمكن تخزينها جميعها في وحدة التخزين الرئيسية بالتالي يتم الاستعانة بهذه الوحدة وتقسم هذه الوحدة إلى وحدات تخزين مباشرة ووحدات تخزين تتابعية[4].

---

[1] الملط، ، أحمد خليفة : **الجرائم المعلوماتية " دراسة مقارنة"** ، مرجع سابق، ص32.

[2] خلف، جاسم خريبط: *التفتيش في الجرائم المعلوماتية*، **مركز دراسات البصرة والخليج العربي**، مجلد41، العدد2013/4، ص257.

[3] قرون، نورهان وبوضياف، جهاد والعيفة، رحيمة: **تكنولوجيا المعلومات والاتصال كركيزة أساسية لعملية التدريب الإلكتروني**، مرجع سابق، ص46+ص47.

[4] سلامة، محمد عبدالله أبو بكر: **جرائم الكمبيوتر والإنترنت**، الاسكندرية–مصر: المكتب العربي الحديث، 2007، ص 45.

ثانياً: إجراء التفتيش على المكونات المعنوية (المنطقية) لوسائل تكنولوجيا المعلومات

ويقصد بهذه المكونات أنها "تعليمات مكتوبة بلغة ما موجهة إلى جهاز تقني معقد يسمى بالنظام المعلوماتي بغرض الوصول إلى نتيجة معينة"[1] أو هي "مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات"[2]، وتقسم هذه المكونات إلى أ- الكيانات المنطقية الأساسية والتي تتمثل في نظام التشغيل والبرامج المساعدة ونظم إدارة قواعد البيانات وبرامج ترجمة اللغات[3] ب-الكيانات التطبيقية وهي نوعين وهما برامج التطبيقات سابقة التجهيز وبرامج التطبيقات طبقاً لاحتياجات العميل[4]. والقيام بإجراء التفتيش على مثل هذه المكونات أثار خلافاً فقهياً بشأن جواز تفتيشها من عدمه مما أدى إلى انقسام الآراء إلى اتجاهين وهما:

الاتجاه الأول: ويرى أصحاب هذا الاتجاه أنه يجوز إجراء التفتيش على هذه المكونات ويعود السبب في ذلك إلى أن على الرغم من أن المعلومات(والتي تعتبر مجرد ذبذبات ونبضات إلكترونية أو إشارات أو موجات كهرومغناطيسية) لا تعد ذات طبيعة مادية إلا أنه يمكن تخزينها على وسائل مادية كالأقراص وبالتالي أصبحت موجودة على شيء محسوس في العالم الخارجي لذلك يمكن إجراء التفتيش عليها[5].

---

[1] الملط، أحمد خليفة : **الجرائم المعلوماتية "دراسة مقارنة"**، مرجع سابق، ص45.

[2] الطوالبة، علي حسن محمد: **التفتيش الجنائي على نظم الحاسوب والانترنت**، مرجع سابق ، ص32.

[3] سلامة، محمد عبدالله أبو بكر: **جرائم الكمبيوتر والإنترنت**، مرجع سابق، ص54+ص55.

[4] سلامة، محمد عبدالله أبو بكر: **جرائم الكمبيوتر والإنترنت**، مرجع سابق، ص57.

[5] حسنية، أحمد: *الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية*، مرجع سابق، ص30.

الاتجاه الثاني: يذهب أصحاب هذا الاتجاه إلى عدم جواز إجراء التفتيش على المكونات المعنوية وذلك بسبب كونها عبارة عن أشياء أو بيانات غير مرئية وغير ملموسة وبالتالي هي بطبيعتها لا تصلح أن يتم إجراء التفتيش عليها لأنها أشياء غير مادية[1]إذ إن إجراء التفتيش يهدف بالأساس إلى التفتيش على الأدلة المادية وضبطها لذا يروا أنه لا يمكن ضبط هذه الأشياء باعتبارها غير ملموسة[2] .

وتؤيد الباحثة هنا الاتجاه الأول كون أن الغاية من التفتيش هي لإظهار الحقيقة بالتالي سواء كانت هذه المكونات مادية او معنوية فإنه يجوز إجراء التفتيش عليها حتى يتم تحقيق الغاية والكشف عن الحقيقة، كما أن القوانين المتعلقة في الجرائم الإلكترونية قد أكدت على جواز إجراء التفتيش على وسائل تكنولوجيا المعلومات سواء كانت هذه الوسائل مادية أم معنوية.

الفرع الثاني: الخطوات الواجب اتباعها لإنجاح إجراء التفتيش

حتى يتم إنجاح إجراء التفتيش وتحقيق الأهداف المرجوة منه فإنه لا بد من اتّباع مجموعة من الخطوات والمتمثلة فيما يلي:

أولاً: أن يكون قد صدر بدايةً إذناً بالتفتيش من قبل الجهات المختصة بإصداره.

ثانياً: أن يتم تحديد محل إجراء التفتيش ألا وهو وسائل تكنولوجيا المعلومات التي سيجري التفتيش عليها حتى يكون الإجراء صحيحاً ولا يعتريه البطلان، ويمكن أن تكون هذه الوسائل بحوزة الأشخاص فحينئذٍ يجب تعيين الشخص أو الأشخاص المراد تفتيشهم وتحديد الاسم واللقب واسم شهرته وسنّه ووظيفته ومحل

[1] محمودي، سماح: *مشكلات التفتيش الجنائي عن المعلومات في الكمبيوتر والإنترنت*، **مجلة الحقوق والعلوم السياسية**، العدد8/2017 الجزء الأول، ص331.

[2] زيدات، حابس يوسف: *مدى استيعاب النصوص التقليدية للسرقة الإلكترونية " دراسة مقارنة"*، **مجلة مركز حكم القانون ومكافحة الفساد**، العدد2/2019.

إقامة عمله وتحديد أوصافه، ويكمن الهدف من تحديد هذه الأمور إلى نفي احتمالية الخطأ في تفتيش شخص آخر[1].

وإذا كانت الوسائل التكنولوجية موجودة في أحد الأماكن فيجب تحديد هذا المكان وتحديد أوصافه والتعرف على مداخل ومخارج المكان والطرق التي تؤدي إلى الوصول للوسائل بأسرع وقت ممكن، ويتم تحديد ذلك من خلال إجراء معاينة سرية لهذا المكان، وتتمثل الغاية من الدقة في هذا التعيين ومعرفة كافة التفاصيل المتعلقة بالمكان هو للمحافظة على عنصر المفاجأة عند القيام بإجراء التفتيش وكذلك حتى لا يستطيع المتهم التخلص من الأدلة أو تهريب الوسائل التكنولوجية أو أي فعل من شأنه أن يؤدي إلى ضياع الأدلة[2].

ثالثاً: وجود فريق فني للتفتيش في الجرائم الإلكترونية والذي يتكون من مجموعة من الأشخاص ويكون لكل منهم دور معيّن يقوم به، ويقسم هذا الفريق إلى:

1. المشرف على التحقيق ويشترط فيه أن يكون متمتعاً بخبرة في هذا المجال ويتولى الإشراف على بقية أعضاء الفريق وعلى كافة إجراءات التفتيش[3].
2. فريق لأخذ الإفادات: وهم يتولون مهام أخذ الإفادات ويراعى عددهم بحسب عدد المتهمين والشهود وبحسب حجم الجريمة المرتكبة[4].
3. فريق الرسم والتصوير: وقد يكون أعضاء هذا الفريق مكوّن من شخصين أو أكثر يقومون برسم خرائط الكروكية ويتم تحديد مواقع الأجهزة والملفات والمستندات الإلكترونية والأشخاص (الذين بحوزتهم الوسائل التكنولوجية)، كما يقوموا بإلتقاط الصور الفوتوغرافية وتصوير فيديوهات مع مراعاة عند

---

[1] راسخ، إبراهيم: **التحقيق الجنائي العلمي**، مرجع سابق، ص392+ص393.

[2] راسخ، إبراهيم: **التحقيق الجنائي العلمي**، مرجع سابق، ص393+ص394.

[3] موسى، مصطفى محمد: **التحقيق الجنائي في الجرائم الإلكترونية**، الطبعة الأولى، مصر: مطابع الشرطة،2009، ص243+ص244.

[4] الفيل، علي: *إجراءات التحقيق الابتدائي في الجريمة المعلوماتية" دراسة مقارنة"*، **مرجع سابق**، ص 468.

تصوير الفيديوهات أن يتم تنبيه من يتواجد في مسرح الجريمة بأنه سيتم البدء في التصوير حتى لا يتم تسجيل أصوات المشتركين من الفرق في إجراء التفتيش[1].

4. فريق التفتيش العلمي: وهذا الفريق قد يكون شخصاً واحداً أو أكثر حسبما تتطلب الحالة ويعمل هذا الفريق على إجراء البحث والتنقيب وفقاً للنظم الفنية التي يتم اتباعها في تفتيش مسرح الجريمة والأماكن التي يتواجد بها الأدلة من غرف أو مخازن، ولا يشترط في أعضاء هذا الفريق التمتع بخبرة في الأجهزة الإلكترونية ولكن من المستحسن أن يتم تنبيههم على نوعية الأشياء التي ينبغي البحث عنها وكيفية التعامل معها[2].
5. خبراء مسرح الجريمة العادية: كخبير البصمات.
6. فريق التأمين والقبض: يتولى هذا الفريق مهمة السيطرة على مداخل ومخارج مسرح الجريمة وكذلك القبض على المشتبه بهم[3].
7. فريق ضبط وتحريز الأدلة: وهم خبراء تقنيين يتمتعون بدراية وخبرة عالية في مجال التعامل مع الوسائل التكنولوجية، ويقوموا بضبط الأدلة المعلوماتية وحفظها بالشكل الصحيح حتى لا يتم فقدانها وقد يكونوا شخصين أو أكثر[4].

رابعاً: وضع خطة لتنفيذ التفتيش فعند وضع خطة لتنفيذ إجراء التفتيش فإنه لا بد من أن يتم بدايةً من جمع معلومات حول عدد الأجهزة ونوعها وأنظمتها، وذلك لكي يتم تحديد الإمكانيات والوسائل اللازمة للتعامل معها فنياً وكيفية ضبطها وتأمين المعلومات الموجودة عليها وحفظها[5].

---

[1] الديربي، عبدالعال و إسماعيل ، محمد صادق : **الجرائم الإلكترونية " دراسة قانونية قضائية مقارنة "**، مرجع سابق، ص310.

[2] الديربي، عبدالعال و إسماعيل ، محمد صادق : **الجرائم الإلكترونية " دراسة قانونية قضائية مقارنة "**، مرجع سابق، ص311.

[3] موسى، مصطفى محمد: **التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص244.

[4] الفيل، علي: *إجراءات التحقيق الابتدائي في الجريمة المعلوماتية" دراسة مقارنة"*، **مرجع سابق**، ص 469.

[5] البشري، محمد الأمين: *التحقيق في جرائم الحاسب الآلي والانترنت*، **المجلة العربية للدراسات الأمنية والتدريب**، مج15، ع30، ص356.

وبعد القيام بجمع المعلومات اللازمة وإعداد الفريق الذي سيباشر إجراء التفتيش فإنه يتم وضع خطة وتكون هذه الخطة من مسؤولية رئيس فريق التفتيش والذي بدوره يرسم هذه الخطة ويحددها بناءً على حجم المهمة والجريمة ونوع الدليل الذي يتم البحث والتفتيش عنه، واستناداً لذلك يقوم بتحديد كيفية القيام بهذا الإجراء وتوزيع المهام والمسؤوليات على أعضاء الفريق[1].

ويشترط في هذه الخطة أن تكون واضحة ومفهومة لكافة أعضاء الفريق، بحيث تشتمل على رسومات وخرائط والتي تحدد كيفية الوصول إلى التيار الكهربائي والتأمين عليه تجنباً لأي قطع له وآلية الدخول المفاجئ للمكان والسيطرة على كافة المداخل والمخارج لمنع دخول أو خروج شخص من شأنه أن يؤثر على سير إجراء التفتيش، وكذلك تحديد أماكن تواجد الأجهزة المستهدفة لإجراء التفتيش عليها والكيفية التي يتم اتباعها للوصول إلى الأدلة وضبطها والمحافظة عليها[2].

وترى الباحثة هنا أنه لإنجاح خطة تنفيذ التفتيش أن تكون هذه الخطة شاملة ودقيقة، وأن يتم وضع أشخاص مناسبين لتنفيذها وإفهامهم بأدوارهم ومهامهم بدقة وأن يكون عنصرا المفاجأة والمباغتة حاضران في تنفيذها، وأن تقتصر الخطة على عناصر الفريق فوجود السرية أمر مهم وضروري لسلامة الأدلة من أي ضياع أو إتلاف.

الفرع الثالث: أهم الوسائل الإلكترونية التي يجري عليها إجراء التفتيش

هناك العديد من الوسائل الإلكترونية التي يجري عليها إجراء التفتيش ونتحدث هنا عن أهم هذه الوسائل وهم الحاسوب والشبكات والبريد الإلكتروني.

---

[1] حسين، سامي جلال فقي: **التفتيش في الجرائم المعلوماتية "دراسة تحليلية"**، مرجع سابق، ص201.

[2] البشري، محمد الأمين: *التحقيق في جرائم الحاسب الآلي والانترنت*، **مرجع سابق**، ص356+ص357.

أولاً: إجراء التفتيش على جهاز الحاسوب ويقصد به أنه جهاز آلي إلكتروني ويتكون من العناصر أو المكونات المادية والمعنوية، إذ تتمثل المكونات المادية بكافة الأجهزة الإلكترونية التي يتم استخدامها أما المكونات المعنوية فتتمثل بجميع البرامج التي يتم تحمليها وتخزينها على هذه الأجهزة، ويعمل الحاسوب على تشغيل هذه البرامج ويستقبل المعلومات والبيانات ليقوم بمعالجتها حسبما يطلب منه وذلك للوصول إلى نتائج معينة ليتم الاستفادة منها فيما بعد[1].

وتختلف الطرق والأساليب المتبعة في إجراء التفتيش بحسب الظروف والملابسات فلا يتم التقيّد بطريقة معينة، بحيث يمكن للقائمين على البحث والتفتيش تحديد فيما إذا سيتم التفتيش على الأجهزة في موقعها أو أن يقوموا بنقلها إلى المختبر الجنائي المختصّ بالجرائم المعلوماتية إذ يعتمدوا في ذلك على مجموعة من العوامل:

1. حجم الأدلة ونطاقها.
2. المشاكل التي تنشأ عن البحث في الأجهزة أو عند نقلها من مكان لآخر.
3. تحديد دور جهاز الحاسوب في الجريمة وهل سيتم ضبطه كامل أم على جزء منه أم على المعلومات التي يحتويها بداخله[2]، إذ تتنوع أدوار أجهزة الحاسوب في الجريمة الإلكترونية فقد يكون الجهاز: أ- أداة للجريمة إذ يتم استخدام النظام المعلوماتي للحاسوب في ارتكاب الجريمة ومثال على ذلك جريمة تزييف العملة فيقوم الجاني باستخدام الحاسوب والماسح الضوئي والطابعة لمسح العملة ثم طباعة النقود[3]. ب- دليل على الجريمة فضبط الجهاز باعتباره دليل يساهم في إلقاء القبض على المتهم بارتكاب الجريمة[4] ومن الأمثلة على ذلك جرائم التهديد والابتزاز بحيث يكون جهاز حاسوب

---

[1] الهيتي، محمد حماد مرهج: **جرائم الحاسوب" ماهيتها موضوعها أهم صورها والصعوبات التي تواجهها"**، الطبعة الأولى، عمّان- الأردن: دار المناهج للنشر والتوزيع، 2006،ص30.

[2] Federal Guidelines for searching and seizing computers/July 1994/USA Department of Justice Criminal Division – office of Professional Development and Training. p.7

[3] ابراهيم، خالد ممدوح: **إجراءات التفتيش في الجرائم المعلوماتية**، مصر: دار الفكر الجامعي، 2022،ص65.

[4] Federal Guidelines for searching and seizing computers. p:25

الجاني مخزّن عليه ما يثبت جريمة التهديد والابتزاز كوجود صور أو ملفات تتعلق بالمجني عليه. ج- أداة للجريمة ومستودع لتخزين الأدلة بحيث يتم استخدام جهاز الحاسوب لوظيفتين في آن واحد فمثلاً كأن يقوم الجاني باستخدام جهازه في مهاجمة أنظمة حواسيب أخرى ثم تخزين ما سرقه من ملفات على جهازه[1].

4. مراعاة فيما إذا كان جهاز الحاسوب مرتبط بأجهزة أخرى أم لا، فكما نعلم أن نظام الكمبيوتر هو عبارة عن مزيج من المكونات المتصلة لذا يجب أن يتم النظر إلى كل مكوّن بشكل مستقل، فضبط جهاز الكمبيوتر لا يمكن أن يكون بالضرورة سبباً لضبط جميع الأجهزة المتصلة به تلقائياً فليس من المنطق ضبط كافة الأجهزة المرتبطة والمتصلة به بواسطة شبكة الانترنت والمنتشرة في أماكن عديدة، لذلك يتوجب تحديد فيما إذا كان هذا المكوّن أو الجهاز المتصل هو عبارة عن أداة للجريمة أو دليل حتى يتم تقرير إذا سيتم ضبطه أم لا[2].

ويجري التفتيش للحاسوب عادةً في إحدى مكانين والتي تتمثل بما يلي:

1. إجراء التفتيش على جهاز الحاسوب بموقعه أي في المكان الذي ضبط فيه الجهاز وفي هذه الحالة:

أ. إما أن يقوم القائمون على التفتيش بطباعة كافة الملفات التي تم ضبطها على نسخ ورقية وهذه الطريقة معيبة كونها تؤدي إلى فقدان كمية كبيرة من المعلومات المهمّة والبيانات الضرورية كاسم الملف السرّي أو تاريخه لذلك تعتبر طريقة غير مجدية للحصول على الأدلة والمعلومات كاملة دون نقصان[3].

---

[1] ابراهيم، خالد ممدوح: **إجراءات التفتيش في الجرائم المعلوماتية**، مرجع سابق، ص66.

[2] Federal Guidelines for searching and seizing computers. p:25+26

[3] حسين، سامي جلال فقي: **التفتيش في الجرائم المعلوماتية**، مرجع سابق، ص205.

ب. أو أن يقوم القائمون على التفتيش بعمل نسخة رقمية طبق الأصل من القرص الصلب وتخزينها على وسائط تخزين ليتم فيما بعد إجراء التفتيش على هذه النسخة ويطلق عليها نسخة الصورة Tis بحيث يتم فيها نسخ كافة البيانات والمعلومات والملفات المخزنة في هذا القرص الصلب[1]، وكما نعلم أن جهاز الحاسوب لا يكون مخصص لهدف أو غرض معين لذلك يمكن أن يحتوي على معلومات وسجلات ووثائق متنوعة والتي في غالبها لا تمت بأي صلة بالجريمة وتكون ملفات شخصية أو ملفات تتعلق بعمل الشخص[2] وبالتالي تعتبر هذه الطريقة غير مناسبة كونها تتوسع في إجراء البحث والتفتيش وتتعدّى على الحقوق الشخصية للمتهم ولا تقدم أي فائدة للتحقيق في الجريمة.

ج. أو أن يعمل القائمون على التفتيش بالاستيلاء على وسائط التخزين الإلكترونية أو أن يتم نسخ المعلومات المخزنة إلكترونياً عليها في وسائط تخزين مادية[3] ليتم البحث والتفتيش عليها فيما بعد كون أن البحث في وسائط التخزين في الموقع قد تؤدي إلى المخاطرة بإتلاف الأدلة لذلك نسخها ومن ثم التفتيش عليها يكون أفضل، وعلى أية حال يجب الحذر عند نقل البيانات على وسائط التخزين للمعلومات كالأقراص بحيث يتم نقلها بطريقة تتناسب مع طبيعتها ويتم تخزينها بشكل جيد وبحرص شديد فالعوامل الطبيعية كالحرارة والرطوبة وظروف التخزين السيئة تؤثر عليها وتؤدي إلى إتلافها وفقدانها[4]، ويتم اللجوء إلى مثل هذه الحالات إذا كان إجراء البحث قد يستغرق وقتاً طويلاً.

---

[1] Searching and Seizing Computers and Obtaining Electronic Evidence In Criminal Investigations، office of legal education executive office for United States Attorneys، USA، 1979،p.78

[2] Searching and Seizing Computers،p.87

[3] Searching and Seizing Computers،p.96

[4] محمود، عبدالله ذيب ودرّاج، أسامة اسماعيل: **الوجيز في الجرائم الإلكترونية**، مرجع سابق، ص207.

2. إجراء التفتيش على جهاز الحاسوب في المختبر الجنائي وذلك بعد القيام بضبط الجهاز بأكمله وإزالة ملحقاته، ويتم اللجوء إلى مثل هذه الحالة عادةً لأن فحص جهاز الحاسوب والبحث والتفتيش فيه قد يحتاج إلى وقتاً طويلاً قد يكون ساعات أو أيام أو مواجهة القائمين على التفتيش لصعوبات تقنية لإجراء البحث على الجهاز، لذا من غير المجدي إجراء التفتيش على الجهاز في موقعه[1].

وعلى أية حال إذا تم نقل جهاز الحاسوب سواء كان يشكل دليل على الجريمة أو هو أداة لارتكاب الجريمة فإنه يجب نقله بشكل صحيح ويتم ذلك بواسطة أشخاص يتمتعون بخبرة عالية ليتمكنوا من ضبطه والمحافظة عليه بصورة صحيحة وحمايته من التلف[2]، كما ويتوجب على الأشخاص الموكل إليهم بالتفتيش أن يتخذوا كافة الاحتياطات اللازمة عند تفكيك وتوصيل أجهزة الحاسوب وذلك لحماية وسلامة البيانات الموجودة بداخل الجهاز وإمكانية الوصول إليها قبل فصل أي كيبلات ومن المستحسن عند إجراء التفكيك أن يتم تصوير الموقع بالفيديو لحالة الشاشة وجميع التوصيلات والأسلاك والحالة التي توجد عليها[3].

ترى الباحثة هنا أنه أفضل أسلوبين يمكن اتباعهما هما طريقة نسخ المعلومات والبيانات على وسائط التخزين لكن مع أخذ كامل الحيطة والحذر حتى لا تتعرض البيانات والمعلومات للتلف وبالتالي فقدانها وتكون هذه الطريقة جيدة إذا كان جهاز الحاسوب الخاص بالشخص هو مجرد مستودع لتخزين الملفات أي الأدلة المتعلقة بالجريمة فحينئذٍ الاستيلاء على هذه الملفات المتعلقة بالجريمة ونسخها على وسائط التخزين لهو أمر كافٍ ويعود بالفائدة على التحقيق أكثر من أن يتم ضبط الجهاز بالكامل، أما الطريقة الثانية فهي تتمثل بضبط الجهاز بالكامل إذا كان إجراء البحث والتفتيش قد يستغرق وقتاً طويلاً أو كان الجهاز محمي بكلمة مرور أو أن الملفات الموجودة بداخله هي محمية ومقفلة بكلمات مرور أو أن القائم بالتفتيش واجه صعوبات فنية وتقنية وبحاجة إلى دقة في التعامل معها حتى لا يتم فقدان البيانات لذلك إن نقل الجهاز بأكمله إلى المختبر الجنائي لتفتيشه هو الخيار الصح.

---

[1] Searching and Seizing Computers،p.77

[2] Federal Guidelines for searching and seizing computers،p.31

[3] Federal Guidelines for searching and seizing computers،p32

ثانياً: إجراء التفتيش على الشبكات فالشبكة الإلكترونية أو المعلوماتية عرّفها القرار بقانون بشأن الجرائم الإلكترونية الفلسطيني في المادة 1 منه بأنها هي ارتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها بما في ذلك الشبكات الخاصة أو العامة أو الشبكة العالمية "الإنترنت"، أما قانون مكافحة جرائم المعلومات المصري في المادة 1 منه فقد عرّفها على أنها مجموعة من الأجهزة أو نظم المعلومات مرتبطة معاً ويمكنها تبادل المعلومات والاتصالات فيما بينها ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية والتطبيقات المستخدمة عليها.

ويقصد بالشبكات بشكل عام على أنها:" هي مجموعة من الأجهزة المتصلة ببعضها البعض من خلال وسائط اتصال ماديّة سلكية أو لا سلكية تسمح لأجهزة الحاسوب بالاتصال المباشر بين مستخدمي نفس الشبكة والأفراد ومشاركة المعلومات"[1]، وتعتبر هذه الشبكات ذات أهمية كبيرة كونها تعمل على ربط الأجهزة ببعضها البعض في أي مكان تتواجد فيه هذه الأجهزة مما يسّهل عملية نقل البيانات والمعلومات والملفات بصورة سريعة.

ويمكن تقسيم الشبكات إلى عدة أنواع والتي تتمثل فيما يلي:

أ. الشبكة المحلية (Local Area Network) ويقصد بها هي تلك الشبكة التي تعمل على ربط الحواسيب مع بعضها البعض في منطقة محصورة ضمن مؤسسة أو مصرف أو وزارة بحيث تكون المسافة التي تفصلهما عن بعض هي قصيرة وذلك لتحقيق عملية مشاركة الملفات والسرعة في تبادل البيانات والمعلومات[2].

---

[1] مقال بعنوان " **تعريف الشبكات وأنواعها**"، موقع الموسوعة العربية الشاملة، نشر بتاريخ25 أكتوبر 2019، أنظر: https://www.mosoah.com/computer-and-electronics/networking/%D8%AA%D8%B9%D8%B1%D9%8A%D9%81-%D8%A7%D9%84%D8%B4%D8%A8%D9%83%D8%A7%D8%AA-%D9%88%D8%A7%D9%86%D9%88%D8%A7%D8%B9%D9%87%D8%A7/

[2] الأنصاري، وحيد حسين: *طرق تعلم الانترنت باستخدام Visual Basic* ، **مجلة كلية التراث الجامعة**، ع7 ص155.

ب. الشبكة الإقليمية (Metropolian Area Network) وهي الشبكة التي تتكون من شبكتين محليتين أو أكثر ويتم عادةً استخدام مثل هذه الشبكات من قبل المؤسسات متعددة التواجد جغرافياً أي لها أفرع في ذات البقعة الجغرافية وذلك لربطها مع بعضها البعض إما بشبكة الانترنت أو بواسطة شبكة تلفزيونية سلكية وتعمل هذه الشبكة على نقل وإرسال الصوت والبيانات بين هذه المؤسسات بسهولة[1].

ج. الشبكة الواسعة (Wide Area Network) وتعمل هذه الشبكات على ربط الحواسيب مع بعضها البعض عن طريق خطوط الهاتف أو الأقمار الصناعية أو كوابل الألياف الضوئية، وتكون هذه الحواسيب منتشرة وموزعة على عدة مناطق فإما أن تكون بين المدن في الدولة الواحدة أو بين الدول أو حتى القارات[2]، وتمتاز هذه الشبكة بقدرتها على ربط مجموعة كبيرة من الأجهزة الأمر الذي يسمح بنقل وتبادل للبيانات والمعلومات بكميات ضخمة.

وتعد الشبكة العنكبوتية العالمية(الانترنت) أهم نوع من هذه الشبكات والتي تعتبر منظومة واسعة جداً من شبكات المعلومات الحاسوبية إذ تعمل على ربط مجموعة كبيرة من أجهزة الحاسوب بطريقة مركزية وتكون هذه الأجهزة موزعة على مختلف دول العالم ويمكن لمستخدمي هذه الشبكة المشاركة في تبادل المعلومات في أي وقت[3].

وفيما يتعلق بمدى إمكانية إجراء التفتيش على الشبكات فإنه يجب التفرقة فيما إذا كانت الحواسيب متصلة ببعضها البعض في شبكات محلية داخل إقليم الدولة أو شبكات واسعة في عدة دول ففي الحالة الأولى يسهل على الجهات المختصة إجراء التفتيش على هذه الشبكات أما في الحالة الثانية فإن الجهات

---

[1] بعلي، حمزة و قدوم، لزهر: **دور الشبكات المعلوماتية في الحد من أخطار المخدرات من خلال مواقع التواصل الاجتماعي**، الملتقى الوطني الأول حول تعاطي المخدرات في المجتمع الجزائري الأسباب الآثار طرق الوقاية والعلاج، جامعة قالمة، الجزائر، 2018/10/15.

[2] المومني، نهلا عبدالقادر ، **الجرائم المعلوماتية**، عمّان–الاردن : دار الثقافة للنشر والتوزيع ، 2008، ، ص35.

[3] محمودي، سماح: *مشكلات التفتيش الجنائي عن المعلومات في الكمبيوتر والانترنت*، مرجع سابق ، ص 334.

المختصة تواجه مشكلة في إمكانية امتداد إجراء التفتيش على الشبكات المتواجدة خارج إقليمها مما يستدعي الأمر إلى اللجوء للتعاون الدولي والتنسيق مع الدولة الأخرى من أجل إجراء التفتيش عليها[1].

وتثور إشكالية هنا فيما إذا كان حاسوب المتهم يتصل بحاسوب آخر أو خادم سواء من خلال شبكة محلية أو شبكة واسعة وكانت تتواجد بيانات مهمة على الحاسوب الآخر أو الخادم ، فهنا نكون أمام احتمالين: أولاً أن يكون الحاسوب أو الخادم المتصل بحاسوب المتهم موجود داخل إقليم الدولة ففي هذه الحالة يمكن أن يمتد إجراء التفتيش على المعلومات والبيانات المخزنة عليه وذلك استناداً للمادة 19 من الاتفاقية الأوروبية بودابيست 2001، وبالرجوع إلى القانون نجد أن المشرع الفلسطيني أيضاً سمح بإجراء التفتيش وامتداده على الحاسوب المتصل بحاسوب المتهم وذلك في المادة 52 من القرار بقانون المتعلق بالجرائم الإلكترونية (... تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة) بالتالي طالما أن حاسوب الشخص الآخر المتصل بحاسوب المتهم مخزن عليه معلومات متعلقة بالجريمة فإنه يمكن إجراء التفتيش عليه، وكذلك المشرع المصري الذي سمح بامتداد التفتيش على الحاسوب الآخر ونستشف ذلك من خلال نص المادة 6 من قانون مكافحة جرائم تقنية المعلومات (ضبط أو سحب ... أو تتبعها في أي مكان أو نظام ...) فكلمة تتبعها تعني ملاحقة ومتابعة كل ما يتعلق بالجريمة بالتالي يمكن تفتيش الحاسوب الآخر طالما هو متصل بحاسوب المتهم ويمكن أن يتواجد فيه معلومات وبيانات تفيد في كشف الحقيقة.

ثانياً: وجود الحاسوب أو الخادم المتصل بحاسوب المتهم خارج حدود إقليم الدولة ففي هذه الحالة الأصل أنه يعتبر أي تفتيش على أي جهاز يتواجد على أراضي دولة أخرى هو اعتداء على سيادة هذه الدولة الموجود لديها الجهاز أو الخادم إلا أن نص المادة 32 من الاتفاقية الأوروبية بودابيست 2001 سمح بإجراء التفتيش على الجهاز أو الخادم الموجود في إقليم دولة أخرى وذلك في حالتين وهما أ-إذا كانت

[1] لطفي، خالد حسن أحمد: **آليات التحقيق الجنائي في جرائم تقنية المعلومات "التحديات والحلول"**، الاسكندرية-مصر: دار الفكر الجامعي،2019، ص70 وما بعدها.

البيانات المطلوب البحث عنها مخزنة على مصدر مفتوح أي على موقع متاح للجميع ب- إذا كانت البيانات مخزنة على نظام كمبيوتر خاص بشخص ما فإنه يجب الحصول على الموافقة القانونية والطوعية لهذا الشخص بالتالي يتم التفتيش بعد قبول ورضاء صاحب الجهاز، ويتم أخذ هذه الموافقة من خلال اللجوء إلى التعاون الدولي والمساعدة المتبادلة بين الدول الأطراف، وقد أكد كل من المشرع الفلسطيني والمصري على تيسير التعاون مع الدول الأخرى وتبادل المعلومات والمساعدة في التحقيق في مثل هذه الحالات[1].

ويجري التفتيش على الشبكات بعدة طرق منها:

1. تتبع مسار الإنترنت: بحيث يجري التفتيش من خلال تتبع الحركة العكسية لمسار الإنترنت لمعرفة المصدر الأصلي لاتصال الشبكة ويتم ذلك من خلال تقنيات وبرامج خاصة مثل برنامج تتبع المسار Traceroute ويتم من خلاله إعادة تركيب المسار الذي سلكته الحزم في انتقالها من المصدر إلى الوجهة[2]، واختلفت الآراء الفقهية حول إمكانية إجراء هذه الطريقة من عدمها فهناك من اتجه نحو عدم إمكانية تحديد مسار الإنترنت وتتبعه بسبب عدم القدرة على تحديد مسار المعلومات في الإنترنت كونها تنقسم إلى حزم عديدة وتمر عبر مسارات مختلفة والتي من الصعب من الناحية الفنية أن يتم تحديد هذه المسارات وتتبعها جميعها[3]، وهناك من رأى بإمكانية تتبع مسار الإنترنت وبالتالي يمكن تحديد مصدر الجريمة، وتؤيد الباحثة هنا الاتجاه الثاني نظراً لتوفير برامج تقوم بهذه المهمة وكذلك أصبحت العديد من أنظمة التشغيل توفر أدوات للتتبع بالتالي أصبح تتبع مسار الإنترنت في الوقت الحالي ليس بالأمر الصعب ويمكن القيام به والكشف عن مصدر ارتكاب الجريمة.

---

[1] المادة 62 من القرار بقانون الفلسطيني رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، المادة 4 من قانون رقم 175 لسنة 2018 المصري بشأن مكافحة جرائم تقنية المعلومات.

[2] كيروز، جيمس و روس، كيث : **شبكات الحاسب والانترنت أسس ومبادئ الشبكات والانترنت**، السعودية: دار العبيكان للنشر ، 2012 ، ص 64 و65 ترجمة: الألفي، السيد محمد و عبد العال ، رضوان السعيد.

[3] حسين، سامي جلال فقي: **التفتيش في الجرائم المعلوماتية**، مرجع سابق، ص246.

2. تفتيش بروتوكول الإنترنت: ويقصد به هو بروتوكول عنونة البيانات والمواقع في شبكة الإنترنت ويتم التعرف بموجبه على جهاز الحاسوب الموصول بشبكة الإنترنت من خلال عناوين عددية إذ إن لكل جهاز حاسوب عنوان خاص به[1]، بالتالي عند التفتيش على الجريمة الإلكترونية فإنه يتم البحث والتفتيش عن الحاسوب المرتكب به الجريمة عن طريق البحث عن الIP الخاص بهذا الجهاز.

ثالثاً: إجراء التفتيش على البريد الإلكتروني: ويعرّف البريد الإلكتروني على أنه وسيلة تعمل على تسهيل الاتصال وإرسال واستقبال الرسائل والوثائق المختلفة بين الأشخاص مما جعله من أهم التطبيقات الإلكترونية التي توفرها شبكة الإنترنت[2].

كما وعرفه المشرع المصري على أنه: هو وسيلة لتبادل رسائل إلكترونية على عنوان محدد بين أكثر من شخص طبيعي أو اعتباري عبر شبكة معلوماتية أو غيرها من وسائل الربط الإلكترونية من خلال أجهزة الحاسب الآلي وما في حكمها[3].

ويجري التفتيش على البريد الإلكتروني من أجل تحديد الأجهزة المرسلة والمستقبلة لرسائل البريد الإلكتروني، وكذلك لتحديد كافة تفاصيل الرسالة فحواها وساعة وتاريخ ارسالها، وحتى لو تم حذفها سواء من قبل المرسل أو المستقبل فإنه يمكن استرجاعها[4].

وأما بالنسبة لطبيعة هذه الرسائل فهناك من اعتبرها أنها كجزء من الاتصالات بحيث لا يمكن الاطلاع عليها إلا بعد الحصول على إذن لمراقبتها، وهناك من اعتبرها كبيانات يتم تخزينها على الحاسوب وبالتالي

---

[1] عبد المطلب، ممدوح عبد الحميد: **بحث بعنوان استخدام بروتوكول IP/TCP في بحث وتحقيق الجرائم على الكمبيوتر**، 2008 انظر http://3dpolice.blogspot.com/2008/01/tcpip.html

[2] نجيب، هند: *ضبط الأدلة في الجرائم الإلكترونية بين الإجراءات التقليدية والإجراءات الحديثة*، **المجلة الجنائية القومية**، المركز القومي للبحوث الاجتماعية والجنائية، مجلد61 ع3/2018، ص108.

[3] المادة 1 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.

[4] شمس الدين، أشرف توفيق: **مدى دستورية تفتيش الهاتف المحمول كأثر للقبض دراسة مقارنة**، مقال منشور على موقع منشورات قانونية، 2021 للمزيد انظر: https://manshurat.org/node/71097

يجري التفتيش عليها والتعامل معها كالبيانات الأخرى[1]، وبالرجوع إلى القانون نجد أن المشرع سواء الفلسطيني أو المصري لم يفرق بين الرسائل العادية والرسائل الإلكترونية[2] واعتبر الرسائل من قبيل الاتصالات والتي تكون بحاجة إلى إذن قضائي للاطلاع عليها أو مراقبتها.

لذا عند إجراء التفتيش على رسائل البريد الإلكتروني الخاصة بالمتهم فإنه لا بدّ من الحصول على إذن قضائي لإجراء التفتيش عليها، فلا يمكن للجهات المختصة عند اجراء التفتيش على الحاسوب مثلاً أن تقوم بفتح البريد الإلكتروني والاطلاع على الرسائل دون وجود إذن بذلك، وعلى أية حال يجري التفتيش على البريد الإلكتروني بعد فتحه إما بعد الحصول على كلمة المرور أو السر من المتهم وبناءً على رضائه أو الاستعانة بخبير في حالة رفض المتهم إذ لا يمكن للجهات المختصة إجبار المتهم على إعطاء كلمة السر، وعليها اتباع الطرق الفنية من أجل معالجة هذا الأمر.

المبحث الثاني: ضبط الأدلة المتحصلة عن إجراء التفتيش في الجرائم الإلكترونية

تعتبر عملية ضبط الأدلة هي الأثر المترتب عن إجراء التفتيش، إذ إن الغاية من التفتيش كما ذكرنا سابقاً هي ضبط الأشياء المتعلقة بالجريمة والتي تفيد في كشف الحقيقة، ونتحدث في هذا المبحث حول ضبط الأدلة والإجراءات التي يتم اتخاذها من خلال تقسيم المبحث إلى:

المطلب الأول: ضبط الأدلة الإلكترونية وكيفية التصرف بها

المطلب الثاني: الأدلة الإلكترونية وقيمتها في الإثبات الجنائي

المطلب الثالث: الصعوبات التي يتم مواجهتها عند إجراء التفتيش وضبط الأدلة الإلكترونية

---

[1] بن يونس، عمر: **الاتفاقية الأوروبية حول الجريمة الافتراضية (المذكرة التفسيرية)**، الطبعة الأولى المعربة، 2005، ص153.

[2] مادة 51 من قانون الاجراءات الجزائية الفلسطيني رقم3 لسنة 2001ومادة 95 من قانون الاجراءات الجنائية المصري رقم150 لسنة 1950.

المطلب الأول: ضبط الأدلة الإلكترونية وكيفية التصرف بها

نظراً لطبيعة الدليل الإلكتروني غير الملموس والذي يكون عبارة عن بيانات ومعلومات مخزنة على شكل إلكتروني[1]والتي تكون صوراً رقمية أو نصّاً مكتوباً أو تسجيلاً صوتياً أو شكلاً أو رسماً، بالتالي يحتاج هذا الدليل إلى اتخاذ إجراءات تتناسب معه عند ضبطه[2]وذلك لضمان سلامتها كونه من السهل التلاعب بها وتعرضها للتغير، لذا كيف يتم ضبط هذه الأدلة الإلكترونية ومن ثم التصرف بها؟

الفرع الأول: إجراءات ضبط الأدلة الإلكترونية

أولاً: تنفيذ الضبط ويقصد **بالضبط** بمفهومه التقليدي: هو" الوسيلة القانونية التي تضع بواسطتها السلطات المختصة يدها على جميع الأشياء التي تم تحصيلها وجمعها أثناء التفتيش والتي إما أن تكون قد وقعت عليها الجريمة أو نتجت عنها أو تم استعمالها لاقترافها كالأسلحة أو الأجهزة الإلكترونية أو الأوراق...إلخ[3].

أما عن تعريف الضبط بحسب الجرائم الإلكترونية فإنه هو وضع اليد من قبل السلطات المختصة على المكونات المادية والمعنوية للأنظمة المعلوماتية وعلى كل شيء يفيد في كشف الحقيقة عن الجرائم الإلكترونية[4].

---

[1] دليل الأدلة الإلكترونية – دليل أساسي لموظفي الشرطة والمدعين العامين والقضاة–، صادر عن مجلس أوروبا، فرنسا، 2014، ص11.

[2] أحمد، طارق عفيفي صادق: **الجرائم الإلكترونية جرائم الهاتف المحمول**، مرجع سابق ، ص228.

[3] الخن، طارق: **الجرائم المعلوماتية** ، سوريا: منشورات الجامعة الافتراضية السورية، 2018، ص137.

[4] شاهين، محمد كمال: **الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي**، الاسكندرية–مصر: دار الجامعة الجديدة، 2018، ص319.

ونستنتج من هذا التعريف أن الأدلة التي يتم ضبطها عند التفتيش هي نوعين والتي تتمثل بأدلة مادية وأخرى معنوية.

1. ضبط الأدلة المادية الإلكترونية

إن عملية ضبط مثل هذا النوع من الأدلة لا يثير أية إشكالات فهي ليست محل خلاف فقهي، إذ إن كافة الأجزاء المادية الملموسة والتي تتصل بالحاسوب تكون صالحة لإجراء الضبط عليها ومن الأمثلة عليها الأوراق وأجهزة الكمبيوتر وملحقاته من وحدات إدخال وإخراج ووحدات المعالجة المركزية، بالتالي فإن الضبط يسري على كافة الأشياء المنقولة والتي يمكن تحريزها وحفظها ونقلها من مكان إلى آخر[1]، أما إذا كانت الأشياء المادية المراد ضبطها بطبيعتها يصعب نقلها كأن يكون الجهاز كبير أو كانت الأجهزة والشبكات المتصلة معها موجودة في عقار ففي هذه الحالة يتم التحفظ على هذه الأجهزة ووضع أختام عليها وكذلك تعيين حراساً عليها وذلك حتى لا يتم العبث بهذه الأدلة إلى حين الانتهاء من التحقيق[2]، وذلك سنداً للمادة 4/53 من القرار بقانون المتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات الفلسطيني والتي نصّت على ضرورة استعمال كافة الوسائل المناسبة لمنع الوصول والنفاذ إلى البيانات وذلك في حالة استحالة إجراء الضبط والتحفظ بصورة فعلية، وبالرجوع للمشرع المصري نجد أنه خلى القانون المتعلق بالجرائم الإلكترونية من النص على مثل هذه الحالة ، إلا أن نص المادة 53 من قانون الاجراءات الجنائية المصري قد تحدثت عن هذه الحالة بحيث يمكن لمأموري الضبط القضائي أن يضعوا الأختام على الأماكن التي يكون بها آثار أو أشياء أو أدلة تفيد في كشف الحقيقة ويمكن أن يضعوا على هذه الأماكن حراساً لحمايتها من أي عبث أو تخريب.

[1] عموري، أشرف أحمد مصطفى: **التفتيش في الجرائم الإلكترونية**، مرجع سابق، ص93.

[2] الطوالبة، علي حسن: **التفتيش الجنائي على نظم الحاسوب والإنترنت**، مرجع سابق، ص143.

وترى الباحثة هنا أنه على الرغم من أنه لا يوجد إشكالية في ضبط الأدلة المادية كونها عبارة عن أشياء ملموسة يسهل التعامل معها، إلا أنه لا بدّ من اتباع الحيطة والحذر في التعامل معها خاصة عند فك الأسلاك وإزالة بعض الأدوات والقطع التي يمكن أن تتضرر في حالة تم ضبطها بصورة غير صحيحة.

2. ضبط الأدلة المعنوية الإلكترونية

آثار الضبط على مثل هذه الأدلة خلافاً فقهياً وذلك بشأن جواز ضبطها من عدمه، فانقسمت الآراء في ذلك إلى:

الرأي الأول: إن بيانات الحاسوب لا تصلح أن يتم ضبطها كونها ليست مادية محسوسة وبالتالي لا يمكن تصور إجراء الضبط عليها إلا إذا تم نقلها على كيان مادي ملموس أو دعامة مادية[1].

الرأي الثاني: لا مانع من أن يتم ضبط البيانات الإلكترونية كونها يتم حفظها على وسائط ووسائل إلكترونية مادية لذا فإن العنصر المادي موجود ويمكن التعامل معه[2].

تؤيد الباحثة هنا الرأي الثاني كون أن الأدلة المعنوية لا يمكن إجراء ضبطها بشكل منفصل عن الأجهزة المتواجدة فيها إذ لا بدّ من أن يتم بدايةً التحفظ على هذه الأجهزة ومن ثم إجراء نقل ونسخ هذه الأدلة على وسائط مادية تخزّن عليها، فليس من المنطق أن يضبط دليل إلكتروني غير ملموس دون تخزينه على وسائل تخزين مادية.

[1] هروال، نبيلة هبه: **الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات**، مرجع سابق، ص265.

[2] لطفي، خالد حسن أحمد: **آليات التحقيق الجنائي في جرائم تقنية المعلومات**، مرجع سابق،ص74.

3. ضبط المراسلات الإلكترونية

وتعرف المراسلات بأنها هي "كافة الرسائل المكتوبة سواء المرسلة بطريق البريد الإلكتروني أو عن طريق البرقيات أو الرسائل الشفوية التي تتم عن طريق المحادثات التليفونية"[1].

وتختلف المراسلات التقليدية عن المراسلات الإلكترونية بأن الأولى تكون عبارة عن مستندات ورقية بالتالي تكون طبيعتها مادية ملموسة، بينما المراسلات الإلكترونية فتكون مخزنة إما على الحواسيب أو الهواتف النقالة بالتالي تكون ذات طبيعة غير ملموسة كونها مخزنة بشكل نبضات إلكترونية، لذلك فإنه لا بد من وجود أساليب وطرق خاصة يتم اتباعها عند ضبط المراسلات الإلكترونية تختلف عن ضبط المراسلات التقليدية كون المراسلات الإلكترونية يتم تحريفها وتغيير محتواها بسهولة.

وحرصت الدساتير والقوانين على حماية المراسلات التي يتم تبادلها وإحاطتها بضمانات ومن بينها ما نص عليه الدستور المصري في المادة 57 منه :" للمراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية وغيرها من وسائل الاتصال حرمة وسريتها مكفولة ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محدودة"، ووضع المشرع مجموعة من الضمانات عند القيام بضبط المراسلات[2] وهي: أ-أن يكون هناك فائدة من إجراء الضبط وهي إظهار الحقيقة ب-أن تكون الجريمة من قبيل الجنايات أو الجنح[3] ج-أن يكون أمر الضبط مسبباً ويكون هذا الأمر لمدة معينة قابلة للتجديد مرة واحدة وهذه المدة هي 15 يوماً حسب القانون الفلسطيني و30 يوماً حسب القانون المصري.

---

[1] جابر، محمود محمد محمود: **الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة-جرائم نظم الاتصالات والمعلومات-**، مصر: المكتب الجامعي الحديث، 2018، ص206.

[2] انظر نصوص المواد 51 من قانون الاجراءات الجزائية الفلسطيني و1/34 من القرار بقانون بشأن الجرائم الالكترونية الفلسطيني و 95 من قانون الاجراءات الجنائية المصري و 6 من قانون مكافحة جرائم تقنية المعلومات المصري.

[3] وتكون العقوبة المقررة لهذه الجرائم بالحبس لا تقل عن سنة حسب القانون الفلسطيني و لا تقل عن 3 أشهر حسب القانون المصري.

ثانياً: محضر ضبط الأدلة

يعتبر إجراء الضبط هو الصورة المادية التي تترتب على إجراء التفتيش، أما محضر الضبط فهو يعتبر الصورة المكتوبة لإجراء الضبط[1]؛ لذلك أوجب القانون على الجهات المختصة أن تقوم بضبط جميع الأشياء المتعلقة بالجريمة وتحريزها وحفظها ومن ثم تثبيت ذلك في محضر بحيث يدوّن فيه كافة الأشياء التي تم العثور عليها ومواصفاتها والأماكن التي وجدت فيها[2].

لذلك يتوجب عند القيام بضبط الأدلة أن تقوم الجهات المختصة بتحرير محضر ضبط يدوّن فيه كافة التفاصيل المتعلقة بالأدلة[3]، بحيث يتم عمل قائمة يوضع فيها كافة المضبوطات التي تم التحفظ عليها ومواصفاتها والحالة التي وجدت فيها ليسهل تمييزها عن بعضها البعض ويكون ذلك بحضور المتهم أو من وجد لديه المضبوط المتحفظ عليه[4].

ونص المشرع المصري على أنه بعد تدوين محضر الضبط يتم عرض جميع المضبوطات على المتهم ليبدي ملاحظاته عليها ومن ثم يقوم بالتوقيع على محضر الضبط وإذا امتنع عن التوقيع فإنه يتم تدوين ذلك في المحضر، وبالرجوع إلى المشرع الفلسطيني نرى أنه لم يتطرق إلى ذلك صراحةً لكن يمكن استنباط ذلك من خلال نص المادة 94 من قانون الاجراءات الجزائية والتي تحدثت عن الاستجواب للمتهم وعن كيفية مواجهته بالأسئلة والشبهات عن التهمة والأدلة وسماع ملاحظاته وإجاباته على ذلك.

---

[1] ثروت، جلال: **نظم الاجراءات الجنائية**، مصر: دار الجامعة الجديدة، 2003، ص450.

[2] انظر المواد 2/50+4 من قانون الاجراءات الجزائية الفلسطيني و 51 من قانون الاجراءات الجنائية المصري.

[3] انظر المواد 3/52 من القرار بقانون بشأن الجرائم الالكترونية الفلسطيني و7 من قانون مكافحة جرائم تقنية المعلومات المصري.

[4] انظر المادة 6/53 من القرار بقانون بشأن الجرائم الإلكترونية الفلسطيني.

ويكون لهذا المحضر قوة ثبوتية إذا ما تحققت مجموعة من الشروط والمتمثلة في أن يكون المحضر صحيحاً بالشكل، وأن يكون من قام بتحريره قد عاين الواقعة بنفسه أو كان قد أبلغ عنها وقام بتحريره وتدوين ما فيه ضمن حدود اختصاصاته وأثناء قيامه بمهام وظيفته[1].

وترى الباحثة هنا أن تدوين المحضر أمر في غاية الأهمية خاصّة عند ضبط الأدلة الإلكترونية كونها تتشابه في كثير من الأحيان وبالتالي يسهل عملية استبدالها أو التعديل عليها لذلك يعتبر المحضر أحد الضمانات لحماية الأدلة الإلكترونية.

الفرع الثاني: حفظ الأدلة الإلكترونية المضبوطة والتصرف بها

عمل المشرع الفلسطيني على وضع طرق لحماية الأدلة المضبوطة وأوجب على القائمين بإجراء الضبط أن يحفظوا الأدلة بحسب الحالة التي وجدت عليها ومن ثم يضعوا المضبوطات في حرز مغلق، ويكتب عليه كافة بيانات الأدلة كما ويتم كتابة تاريخ التحفظ وساعته وعدد المحاضر والقضية وتحال بعد ذلك المضبوطات إلى الجهات المختصة التي بدورها تقوم على إيداع هذه الأدلة في أماكن مخصصة للحفاظ عليها[2].

وأكد أيضاً على ذلك المشرع المصري والذي أوضح بأن كافة الأشياء والأوراق التي يجري ضبطها توضع في حرز مغلق ويربط عليها كلما أمكن ذلك، ويختم عليها ويكتب على شريط داخل الختم تاريخ المحضر المحرر بضبط تلك الأشياء ويشار إلى الموضوع الذي حصل الضبط من أجله[3].

---

[1] المادة 213 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

[2] المواد 1/72 و 2/50 من قانون الاجراءات الجزائية الفلسطيني والمادة 6/53 من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[3] مادة 56 من قانون الاجراءات الجنائية المصري.

وكون أن الأدلة الإلكترونية هي بطبيعتها حساسة فإنه يتوجب على القائمين بضبطها أن يتعاملوا معها بلين وحذر، وأن يكونوا ذو خبرة واختصاص للتعامل معها فيضعوها في أماكن مخصصة لحفظها وتكون هذه الأماكن ليست عرضة لدرجات الحرارة العالية أو الرطوبة أو الأتربة، كما ويجب عليهم أن يعملوا على تأمينها فنياً فمثلاً يتم ضبط الدعائم الأساسية للبيانات وعدم الاقتصار على ضبط نسخها وكذلك التعامل مع الأقراص والأشرطة الممغنطة بعناية شديدة فلا يتم ثنيها أو الضغط عليها أو الكتابة عليها[1].

وأما عن التصرّف في الأدلة المضبوطة ففي الأدلة بشكل عام حدد المشرع الفلسطيني والمصري كيفية التصرف بها بحيث:

1. يكون رد الأشياء المضبوطة إلى من كانت في حيازته وقت ضبطها وإذا كانت من الأشياء التي وقعت عليها الجريمة أو متحصلة منها فإنه يتم ردها إلى من فقد حيازتها بالجريمة[2].
2. إذا كانت من قبيل الأشياء سريعة التلف مع مرور الزمن فإنه يجوز للنيابة العامة أو للمحكمة أن تأمر ببيعها بالمزاد العلني[3].
3. يمكن رد المضبوطات إذا لم تكن لازمة لسير الدعوى أو لم تكن محلاً للمصادرة الوجوبية[4].
4. أما بخصوص الأدلة الإلكترونية فقد أوجب المشرع الفلسطيني على ضرورة مصادرة كافة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم الإلكترونية المنصوص عليها في القرار بقانون ودون الإخلال بحقوق الغير حسن النية وذلك سنداً للمادة 2/70 من القرار بقانون المتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

---

[1] الطحاوي، أحمد يوسف: **الأدلة الإلكترونية ودورها في الإثبات الجنائي دراسة مقارنة**، مصر: دار النهضة العربية، 2015، ص186.

[2] مادة 2/73 من قانون الاجراءات الجزائية الفلسطيني رقم3 لسنة 2001 و 102 من قانون الاجراءات الجنائية المصري رقم 150 لسنة1950.

[3] مادة 2/72 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 و 109 من قانون الاجراءات الجنائية المصري رقم 150 لسنة1950.

[4] مادة 1/73 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 و 101 من قانون الاجراءات الجنائية المصري رقم 150 لسنة 1950.

أما المشرع المصري نص في المادة 1/6 من قانون مكافحة جرائم تقنية المعلومات على أنه يتم التحفظ وجمع كافة البيانات والمعلومات أو أنظمة المعلومات وتتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه على أن لا يؤثر هذا التحفظ والضبط على استمرارية النظم، وبالتالي لم يشر المشرع المصري صراحةً على المصادرة وكيفية التصرف بالأدلة الإلكترونية.

وترى الباحثة أنه كان على المشرع الفلسطيني أن لا يجزم بأن يتم مصادرة كافة الوسائل التكنولوجية كون أن استخدام أو حيازة الوسائل التكنولوجية لا تعد جريمة بحد ذاتها، بالتالي إذا لم تكن هذه الوسيلة لازمة لإظهار الحقيقة فإنه لا مانع من أن يتم ردها، لذلك كان أجدر به أن يمنح خيارات كما فعل في قانون الاجراءات الجزائية إما بردها إذا لم تكن لازمة لسير الدعوى أو مصادرتها إذا كانت تشكل جريمة أو أن استخدامها يشكل جرائم خطيرة[1].

المطلب الثاني: الأدلة الإلكترونية وقيمتها في الإثبات الجنائي

لقد بينّا أن الجرائم الإلكترونية تقوم على أساس استخدام وسائل تكنولوجيا المعلومات، وبالتالي فإن الأدلة الناتجة عنها في الغالب هي أدلة إلكترونية تقسم إلى نوعين أدلة إلكترونية مادية كجهاز الحاسوب وأجهزة الخليوية وأدلة إلكترونية معنوية متمثلة بالبيانات المخزنة على الأجهزة والوسائل التكنولوجية[2]، ويرتبط الدليل الإلكتروني بمسرح الجريمة الإلكترونية ارتباطاً وثيقاً بحيث يمكن من خلاله اسناد الجريمة إلى مرتكبها[3]، ويعرّف الدليل الإلكتروني على أنه هو الدليل المتحصل من النظم البرمجية المعلوماتية الحاسوبية وأجهزة الاتصال المختلفة بواسطة برامج وتطبيقات وفقاً لإجراءات قانونية وفنية بعد تحليلها

[1] المادة 73 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

[2] نصيف، صفاء حسن: *التحديات الإجرائية المتصلّة بالجرائم المعلوماتية*، **مجلة العلوم القانونية والسياسية**، مجلد 5، العدد2/2016، ص258.

[3] محمود، عبدالله ذيب ودرّاج، أسامة اسماعيل: **الوجيز في الجرائم الإلكترونية**، مرجع سابق، ص199.

علمياً وتفسيرها في شكل رسوم مكتوبة أو صوراً وتقديمها للقضاء لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها[1].

إن الدليل الإلكتروني شأنه شأن الأدلة الجنائية والذي بحاجة إلى توافر مجموعة من الشروط فيه حتى يتم قبوله والاعتداد به لذلك نتحدث في هذا المطلب حول الشروط الواجب توافرها في الدليل الإلكتروني ومن ثم حجية الدليل الإلكتروني في الإثبات الجنائي.

الفرع الأول: شروط قبول الدليل الإلكتروني

ويشترط في الدليل الإلكتروني حتى يتم قبوله عدة شروط تتمثل فيما يلي:

1. الحصول على الدليل الإلكتروني بطريقة مشروعة: إذ يشترط في الدليل الإلكتروني أن يتم الحصول عليه بطريقة مشروعة بحيث لا تكون هذه الطريقة مخالفة لأحكام الدستور والقانون، ويقصد بمشروعية الدليل الإلكتروني: ضرورة اتفاق إجراء التفتيش مع القاعدة القانونية والأنظمة، كما أن مشروعية الدليل لا تقتصر فقط على الاتفاق مع القاعدة القانونية وإنما يجب مراعاة إعلانات حقوق الإنسان والمواثيق الدولية وقواعد النظام العام والمبادئ التي استقرت عليها محكمة النقض[2].

وعمل الدستور على حماية حقوق الفرد وحرياته إذ نصّ القانون الأساسي الفلسطيني المعدّل لسنة 2003 في المواد 2/11 والمادة 17 والدستور المصري لعام 2014 والمعدّل في عام 2019 في المواد 54 و57 و58 أن حقوق الأشخاص وحرياتهم مكفولة بحيث لا يجوز التعدي على مسكنهم أو المساس بالأشياء التي تتعلق بهم، إلا إذا دعت الضرورة لذلك كأن يكون هذا الشخص مشتبه به في ارتكابه لجريمة ومن أجل

---

[1] موسى، منى عبد العالي و هادي، مصطفى كريم: *وسائل اثبات جريمة الإزعاج بواسطة الرسائل السلكية واللاسلكية*، **مجلة جامعة بابل للعلوم الإنسانية**، مجلد26، ع2018/9، العراق، ص484.

[2] شهاب، أحمد عبدالحكيم عبدالرحمن: *شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي المصري*، **مجلة الاجتهاد للدراسات القانونية والاقتصادية**، مجلد7، عدد2018/2، ص175.

التثبّت من أنه هو مرتكبها فلا بدّ من البحث والتنقيب عن الأدلة التي تدينه، لذلك يجوز القيام بتفتيشه وتفتيش ما يتعلق به للوصول للحقيقة.

كما أن القوانين الإجرائية أكدت على ضرورة أن يكون الحصول على الدليل بطرق مشروعة فقد نصّ كل من المشرع الفلسطيني والمصري على أن المحكمة لا يجوز لها أن تبني حكمها على أي دليل لم يطرح أمامها في الجلسة أو تم التوصّل إليه بطريق غير مشروع كما أن كل قول يثبت أنه صدر من المتهم أو الشاهد وهو تحت وطأة الإكراه أو التهديد فإنه لا يعوّل عليه ولا تأخذ به[1].

وبناءً على ما سبق فإنه يتوجب على القاضي قبول الأدلة وتقديرها وبناء حكمه على الأدلة التي تم الحصول عليها بطريقة مشروعة فصحيح أن القاضي يتمتع بحرية في الإثبات إلا أن ذلك لا يعني الحصول على الأدلة والبحث عنها بأساليب غير مشروعة كالدليل الذي يتم الحصول عليه بالإكراه أو التهديد، أو أن يقوم بالاستناد إلى أدلة ناتجة عن إجراءات باطلة[2]، كإجبار المتهم على فك شيفرة نظام من النظم المعلوماتية أو الوصول إلى ملفات مخزنة تتعلق به، إذ إن الطرق غير المشروعة تؤدي إلى بطلان الدليل الإلكتروني فما بني على باطل فهو باطل[3].

2. يقينية الدليل الإلكتروني: بحيث يجب أن يكون اقتناع القاضي اقتناعاً يقينياً أي بمعنى أن يكون قائماً على الجزم وليس مجرد احتمال فالأصل البراءة حتى تثبت إدانة المتهم بالتالي يجب أن ينتهي حكم القاضي من خلال الأدلة إلى الجزم بوقوع الجريمة ونسبتها إلى المتهم فإذا كان لديها شك في ذلك وقامت بإدانته فالقرار في هذه الحالة معيب ويجب رفضه فالشك يفسر لمصلحة المتهم وليس ضده[4].

---

[1] مادة 273 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 و 302 من قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950.

[2] العبادي، محمد عبدالكريم: **القناعة الوجدانية للقاضي الجزائي ورقابة القضاء عليها**، الطبعة الأولى ، عمان–الاردن: دار الفكر، 2010، ص160 وما بعدها.

[3] محمود، عبدالله ذيب ودرّاج، أسامة اسماعيل: **الوجيز في الجرائم الإلكترونية**، مرجع سابق، ص236+237.

[4] نمور، محمد سعيد: **شرح لقانون أصول الإجراءات الجزائية**، الطبعة الأولى، عمان–الأردن: دار الثقافة ، 2005، ص209.

لذلك يشترط في الأدلة الإلكترونية المستخرجة من الوسائل التكنولوجية كالحاسوب والشبكة أن تكون غير قابلة للشك حتى يتم الحكم بالإدانة على المتهم ويمكن التوصل إلى حد الجزم واليقين ودحض قرينة البراءة وفرض عكسها من خلال الأدلة الإلكترونية التي يتم عرضها على القاضي بالتالي يستطيع القاضي تحديد قوة الأدلة الإلكترونية الاستدلالية ونسبة الجريمة الإلكترونية لشخص معين دون غيره[1].

3. مناقشة الأدلة الإلكترونية: إذ إن القاضي لا يجوز له أن يؤسس حكمه إلا على الأدلة التي طرحت أثناء المحاكمة فلا يمكن له أن يأخذ بأدلة اثبات أو نفي لم تكن معروضة عليه خلال المحاكمة ولم يتم مناقشتها من قبل أطراف الدعوى بالتالي إن الأدلة الإلكترونية بكافة أنواعها لا بد من أن يتم مناقشتها وتمكين المتهم من الاطلاع عليها ليتسّنى له الدفاع عن نفسه فحصها من قبل القاضي وإبداء رأيه فيها[2].

ويستند مبدأ مناقشة الأدلة الإلكترونية على قواعد أساسية تتمثل بما يلي:

أ. مبدأ شفوية إجراءات المحاكمة: وهو وجوب أداء إجراءات المحاكمة شفوياً خلال الجلسة بحيث تكون بصوت مسموع لكل الحاضرين، ويقع على عاتق المحكمة عند تكوين اقتناعها أن تستمع بنفسها لكل مصادر الأدلة من شهود وخبراء ومأموري ضبط وغيرهم فلا يجوز لها أن تكتفي بالاطلاع على محاضر الاستدلالات والتحقيقات، لذا فإن كل دليل يعتمد عليه القاضي في حكمه يجب أن يكون قد طرح شفوياً وتمت المناقشة الشفوية حوله[3]، ولقد تم إقرار هذا المبدأ استناداً إلى المادة 207 من قانون الاجراءات الجزائية الفلسطيني والمادة 289 من قانون الاجراءات الجنائية المصري، والعلة في إقرار مبدأ شفوية الإجراءات هو1-أنه يتصل بعدة مبادئ أخرى فمثلاً في مبدأ المواجهة بين الخصوم تمكّن

---

[1] العدواني، فهد دخين: **مشروعية الدليل الإلكتروني الصادر عن التفتيش الجنائي دراسة مقارنة**، دراسات في التعليم الجامعي، العدد 2017/36،ص261.

[2] العتيبي، زياد بن محمد عادي: *دراسة استطلاعية حول حجية الأدلة الرقمية في اثبات الجرائم المعلوماتية*، **المجلة الإلكترونية الشاملة متعددة التخصصات**، العدد2020/29.

[3] السعيد، كامل: **شرح قانون أصول المحاكمات الجزائية**، الطبعة الثالثة، عمان-الاردن: دار الثقافة للنشر والتوزيع،2010 ، ص 576

شفوية الإجراءات في هذا المبدأ أن يقوم كل خصم بمواجهة الآخر بما لديه من أدلة من خلال عرضها شفوياً ومناقشتها2-ويتصل مبدأ الشفوية بمبدأ العلانية إذ أنه تعرض الأدلة في الجلسة بصوت مرتفع مما يسمح لكافة الحاضرين العلم بها3-كما أنه يتصل بمبدأ الاقتناع القضائي إذ إن القاضي يكوّن قناعته من حصيلة المناقشات التي تجري في الجلسة4-ويتيح هذا المبدأ للمحكمة رقابة على أعمال التحقيق الابتدائي إذ إن الأدلة التي تتولد عنه يتم عرضها في الجلسة ويتم المناقشة فيها[1].

ب. مبدأ علنية المحاكمة: أي " أن تنعقد جلسة المحكمة التي تنظر في الدعوى في مكان يجوز لأي فرد أن يدخله ويشهد المحاكمة بغير قيد إلا ما يقتضيه حفظ النظام"[2] ويهدف هذا المبدأ إلى تحقيق المصلحة العامة للمجتمع ككل مما يشعروا بالطمأنينة، إذ أن المحاكمة تكون بشكل علني ويمكن لأي شخص أن يحضرها بحيث تتم الإجراءات وفقاً لأحكام القانون مما يؤدي إلى تحقيق العدالة، وكما أنه يهدف إلى حماية القاضي من المؤثرات الخارجية التي تؤثر على حكمه، ويضاف إلى ذلك تحقق سياسة الردع العام[3] وعلى الرغم من أن المشرع أقر بأن تجري جلسات المحاكمة بشكل علني إلا أنه ورد استثناء على مبدأ علانية الجلسات[4] بحيث تتم جلسة المحاكمة بصورة سرية وذلك لتحقيق المصلحة العامة، ففي بعض القضايا إذا تمت بصورة علنية فإنها تلحق ضرر بمصلحة المتهم، أو حتى بمصلحة المجني عليها كما هو الحال في جرائم الشرف، وتتمثل الحالات المستثناة من مبدأ العلانية في:1-مراعاة النظام العام وذلك في الدعاوى التي تتعلق بأسرار الدولة ومصلحتها 2-المحافظة على الآداب: ويكون ذلك في الجرائم التي تمس الشرف والعرض3-محاكمة الأحداث، وبالتالي تعتبر سرية المحاكمة هي وجوبية ويترتب على مخالفة ذلك لزوم نقض الحكم، وتعتبر السرية في حالتي مراعاة النظام العام والمحافظة على الآداب هي مسألة جوازية فللمحكمة سلطة تقديرية

---

[1] السعيد، كامل: **شرح قانون أصول المحاكمات الجزائية**، مرجع سابق، ص 577.

[2] العبادي، محمد عبد الكريم: **القناعة الوجدانية للقاضي الجزائي ورقابة القضاء عليها**، مرجع سابق، ص 73.

[3] نمور، محمد سعيد: **شرح لقانون أصول الإجراءات الجزائية**، مرجع سابق، ص459.

[4] مادة 237 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001، و 268 من قانون الاجراءات الجنائية المصري رقم 150 لسنة 1950.

ويشترط عند قيام المحكمة بعقد جلسة المحاكمة بصورة سرية أن تبين وتوضح الأسباب التي دعتها لاتخاذ ذلك، وذلك حتى يعلم الكافة السبب الذي دفعها في العدول عن مبدأ علانية الجلسات[1].

الفرع الثاني: حجية الدليل الإلكتروني في الإثبات الجنائي

إن أنظمة الإثبات اختلفت في تقديرها لحجية الدليل الإلكتروني وتتمثل هذه الأنظمة فيما يلي:

أولاً: نظام الإثبات الحر والذي يطلق عليه مسمى الاقتناع الذاتي بحيث يكون للقاضي الجزائي الحرية الكاملة في البحث عن الحقيقة بكافة الوسائل الممكنة والمشروعة وعلى الرغم من أنه يتمتع بحرية إلا أنها حرية مقيّدة وليست مطلقة أي بمعنى يجب أن تحاط بضمانات عديدة ويراعى فيها شروط وضوابط معينة، لذلك إن حجية الأدلة الإلكترونية في النظام الحر لا تثير أية صعوبات سواء لمدى حرية تقديم الأدلة لإثبات الجريمة الإلكترونية أو لمدى حرية القاضي الجنائي في تقدير هذه الأدلة ذات الطبيعة الخاصة باعتبارها أدلة إثبات بالمواد الجنائية إذ إن الأساس هو حرية القاضي في تقدير الأدلة بالتالي تخضع الأدلة الإلكترونية لحرية القاضي في الاقتناع الذاتي بحيث يمكن أن يطرح هذه الأدلة طالما أن الدليل يتوافق منطقياً مع ظروف الواقعة وملابساتها[2]، ويتضح لنا أن المشرع أخذ بنظام الإثبات الحر من خلال المواد 206 و 1/273من قانون الإجراءات الجزائية الفلسطيني والمواد 291 و 302 من قانون الإجراءات الجنائية المصري، والمادة 57 من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، والمادة 11 من قانون مكافحة جرائم تقنية المعلومات المصري.

ثانياً: نظام الإثبات المقيد وهو نظام الأدلة القانونية والذي يقضي بأن القاضي يستخدم وسائل الإثبات المحددة في القانون بحيث لا يملك الاقتناع إلا بهذه الأدلة المقررة قانوناً فالقانون يحدد نوع الدليل وقيمته وإجراءات تقديمه للقضاء[3]، بحيث يكون دور القاضي هنا مقتصراً على تقدير فيما إذا توافرت الشروط

---

[1] نمور، محمد سعيد: : **شرح لقانون أصول الإجراءات الجزائية**، مرجع سابق، ص461.

[2] الطوالبة، علي حسن محمد: **التفتيش الجنائي على نظم الحاسوب والانترنت**، مرجع سابق، ص 201.

[3] أبو داسر، عبدالله بن سعيد: **إثبات الدعوى الجنائية**، رسالة دكتوراة، جامعة الإمام محمد بن سعود الإسلامية، 1443هـ، ص13.

المحددة من قبل المشرع مسبقاً ومن ثم الحكم بالقيمة القانونية لهذا الدليل في الإثبات، وفي هذا النظام لا يمكن الأخذ وقبول الأدلة الإلكترونية في الإثبات الجنائي إلا إذا كان منصوصاً عليها في القانون، وبما أن الأدلة الإلكترونية تتسم بالتطور والتقدم فإن ما قد يقرره المشرع من شروط في الدليل الإلكتروني قد لا تكون مقبولة مستقبلاً وبالتالي يكون القانون بحاجة إلى تعديل من وقت لآخر ليواكب ما وصلت إليه التقنية الرقمية[1].

4. نظام الإثبات المختلط وهو نظام يجمع بين نظام الإثبات الحر ونظام الإثبات المقيّد وأخذت بهذا النظام تلك التشريعات التي تأخذ بمجمل مبادئها نظام الإثبات الحر وعلى سبيل الاستثناء وفي جرائم محددة تأخذ بنظام الإثبات المقيّد[2].

المطلب الثالث: الصعوبات التي يتم مواجهتها عند إجراء التفتيش في الجرائم الإلكترونية

تتسم الأدلة الناتجة عن الجرائم الإلكترونية بأنها تحمل طابع خاص كونها في الغالب هي بيانات ومعلومات أي أنها أشياء غير ملموسة مما يصعب التعامل معها، الأمر الذي خلق صعوبات ومعوقات منها ما يتعلق بالجريمة الإلكترونية ذاتها ومنها ما يتعلق بالجهات المختصة بالتفتيش عن هذه الأدلة، لذا نتحدث في هذا المطلب حول الصعوبات التي يتم مواجهتها عند إجراء التفتيش والضبط.

الفرع الأول: الصعوبات التي تتعلق بالجرائم الإلكترونية

إن الجرائم الإلكترونية هي عديدة ومتنوعة لذا يصعب اكتشافها بحيث يتم ارتكابها في بيئة إلكترونية مما يجعل الأدلة الناتجة عنها أدلة غير ملموسة يسهل على الجاني التخلص منها ومن آثارها[3]، أو أن يقوم

---

[1] نصيف، صفاء حسن: **التحديات الإجرائية المتصلة بالجرائم المعلوماتية**، مرجع سابق، ص262.

[2] حسن، آمال عبدالرحمن يوسف: **الأدلة العلمية الحديثة ودورها في الإثبات الجنائي**، رسالة ماجستير جامعة الشرق الأوسط، عمان- الأردن، 2011-2012، ص21.

[3] الفقي، عمرو: **الجرائم المعلوماتية" جرائم الحاسب الآلي والانترنت في مصر والدول العربية**، مصر: المكتب الجامعي الحديث، 2006، ص89.

بحمايتها من خلال وضع وسائل تعيق وتمنع الوصول إليها، لذا تتمثل الصعوبات التي تتعلق بالجرائم الإلكترونية بما يلي:

أولاً: صعوبة إثبات الجرائم الإلكترونية: إذ إن الجرائم الإلكترونية يتم ارتكابها عن طريق نقل البيانات والمعلومات على شكل نبضات إلكترونية غير مرئية تنساب في أجزاء الحاسب الآلي وشبكة الاتصالات العالمية أو عبر الأسلاك مما يصعب ضبطها[1]، وبالتالي تكون الأدلة فيها أدلة معنوية غير ملموسة مما يؤدي إلى غياب الدليل المادي المرئي لذلك يصعب إقامة واكتشاف الدليل، فعلى سبيل المثال الجرائم التي يتم ارتكابها والتي تعتمد في موضوعها على التشفير والكود السري والنبضات والأرقام والتخزين الإلكتروني فإنه من الصعوبة أن تخلف أي آثار مرئية وراءها لذلك لا يمكن الكشف عنها لعدم القدرة على اثباتها أو الاستدلال من خلالها على الجاني[2].

ثانياً: سهولة تدمير وإخفاء الدليل: تعتبر الجرائم الإلكترونية من الجرائم التي تمتاز بسهولة وسرعة تنفيذها وهذا يسهّل على الجاني التخلص من الدليل وإتلافه ومحو آثاره مما يصعب الكشف عن الجريمة لعدم وجود دليل عليها[3]،إذ إن الجاني يقوم بتدمير البيانات والمعلومات المخزنة داخل جهاز الحاسوب في خلال ثوانٍ معدودة[4]، أو أن يستعين ببرامج تكون مهمتها محو المعلومات تلقائياً إذا ما تم اختراق النظام من شخص غير مسموح له بالدخول إليه[5]بالتالي إذا ما قامت الجهات المختصة بالتفتيش بالدخول إلى هذا النظام فإنها لا تجد أي أدلة لقيام البرنامج بمحو جميع الأدلة.

---

[1] الهيتي، محمد حماد مرهج: **جرائم الحاسوب" ماهيتها موضوعها أهم صورها والصعوبات التي تواجهها"**، مرجع سابق ، ص214.

[2] لطفي، خالد حسن أحمد: **القانون الواجب التطبيق على الجريمة المعلوماتية**، الاسكندرية–مصر : دار الفكر الجامعي، 2020، ص117.

[3] هورنجور، تشالز: **الجرائم الالكترونية والمعلوماتية –بطاقات الائتمان– الكمبيوتر والانترنت**، مصر: مؤسسة شباب الجامعة، 2018، ص303+304.

[4] الرومي، محمد أمين: **جرائم الكمبيوتر والانترنت**، الاسكندرية–مصر: دار المطبوعات الجامعية، 2003، ص142.

[5] الهيتي، محمد حماد مرهج: **جرائم الحاسوب" ماهيتها موضوعها أهم صورها والصعوبات التي تواجهها"**، مرجع سابق، ص213.

ثالثاً: إعاقة ومنع الوصول إلى الدليل: غالباً ما يكون المجرم الإلكتروني مجرم محترف أو متخصص بحيث يتمتع بقدرة فائقة في المهارات التقنية ويستغل مداركه ومهاراته في اختراق الشبكات وفك الشيفرات وارتكاب الجرائم المختلفة[1] فيضع خطة لارتكاب جريمته ويستعين في ذلك بتدابير ووسائل حماية يصعب اختراقها مما يعيق الوصول إلى الدليل ومن هذه الوسائل التشفير وكلمات المرور ووضع رموز للمعلومات لا يمكن لأحد غيره فهمها.

رابعاً: عدم تخلف آثار مادية عن الجرائم الإلكترونية: فالجرائم الإلكترونية تختلف عن الجرائم التقليدية بحيث تفتقر في كثير من الأحيان إلى وجود الدليل المادي، فالعالم الذي يتم ارتكاب فيه الجرائم الإلكترونية هو عالم افتراضي ويتم فيه التعامل مع بيانات ومعلومات والتي تكون عبارة عن نبضات إلكترونية مما يسهل تغييرها ومحوها في ضغطة زر، لذا يمكن القول أن الدليل المادي ينعدم في مثل هذه الجرائم لأنه يتم التعامل مع بيانات غير مرئية وتكون مسجلة إلكترونياً ويوضع عليها الترميز بالتالي لا تترك أثراً عند التعديل أو التلاعب فيها[2].

خامساً: ضخامة حجم البيانات المعلوماتية المراد فحصها: فالمعلومات والبيانات المعالجة إلكترونياً والمراد ضبطها وفحصها تكون بكميات ضخمة خاصّة تلك الموجودة في الشبكة[3]، مما يشكل صعوبة كبيرة في كيفية ضبطها والتعامل معها خاصة عندما تكون هناك ملفات يوجد فيها أدلة الجريمة وملفات ليس لها أي علاقة أو أن يكون أسماء الملفات غير مطابق لما تحتويه مما يستدعي البحث في كافة الملفات لإمكانية وجود بعض أدلة الجريمة في إحدى هذه الملفات.

---

[1] حجازي، محمد: **جرائم الحاسبات والانترنت الجرائم المعلوماتية**، 2005، ص21+22.

[2] الحجار، عدنان ابراهيم و بشير، فايز خضر: *الأدلة الرقمية واثبات الجرائم السيبرانية ما بين التأصيل والتأويل*، **مجلة جامعة الاستقلال للأبحاث**، مجلد6، العدد1/2021، ص146.

[3] الجنبيهي، منير محمد: **صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات**، الطبعة الأولى ،الاسكندرية–مصر: دار الفكر الجامعي، 2019،ص116.

ويترتب على هذه الصعوبة العديد من المشاكل والأضرار كالأضرار الاقتصادية إذا ما تم ضبط وحجز كافة البيانات الإلكترونية وكانت حجمها يفوق القدرة البشرية لمراجعتها وكذلك مشكلة ضياع الأدلة إذا ما تم التغاضي عن بعض البيانات والاعتماد على أمل الحصول على اعتراف من الجاني[1].

الفرع الثاني: الصعوبات التي تتعلق بالجهات المختصة بإجراء التفتيش

إن إجراء التفتيش في الجرائم الإلكترونية يتطلب بذل وقت وجهد كبير من قبل الجهات المختصة للوصول إلى الأدلة، إذ ليس من السهل القيام بهذا الإجراء كونه يتم في بيئة إلكترونية والتي تحتاج إلى قدرات وخبرة وتخصص في البحث والتفتيش فيها عن الأدلة، الأمر الذي خلق صعوبات تعيق وتؤثر على عمل القائمين بالتفتيش في الحصول على الأدلة وضبطها، ونتحدث في هذا المطلب حول أهم هذه الصعوبات والتي تتمثل فيما يلي:

أولاً: صعوبة فهم الدليل المتحصل عن الجرائم الإلكترونية: فالدليل الإلكتروني والذي ينتج عن عمليات التلاعب في نبضات إلكترونية وعمليات أخرى غير مرئية يصعب الوصول إليه وفهم ما يحتويه إلا من قبل خبير متخصص يتمتع بخبرة فنية ومقدرة على معالجة البيانات والمعلومات واختيار أفضل السبل لضبط الدليل[2]، لذلك إن طبيعة هذه الأدلة تثير إشكالية أمام الجهات المختصة في فهمها والتعامل معها ومن الأمثلة على ذلك فيما يتعلق بالمسائل الفنية الدقيقة فإنها تحتاج إلى التمتع بقدرة عالية لفك رموزها وتحليلها، كذلك العمليات الآلية للبيانات التي يقوم بها الحاسب الآلي دون الحاجة إلى إدخال فإنها لا تخلف وراءها أية آثار مادية ملموسة لتكشف عنها فيكون من السهل اختراق النظام والتلاعب فيه وتزوير وتعديل البيانات مما يصعب على الجهات المختصة التعامل مع مثل هذه الجرائم وفهم الأدلة المتحصلة

[1] شاهين، محمد كمال: **الجوانب الاجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي** ، مرجع سابق، ص87+88.

[2] عامر، عادل: **مظاهر صعوبة اثبات الجريمة الإلكترونية**، مقال منشور على موقع دنيا الوطن بتاريخ 2018/9/17 انظر: https://pulpit.alwatanvoice.com/content/print/473131.html

عنها بسبب تعقيدها وصعوبة الوصول إلى مرتكبها، كما أن الجرائم العابرة للحدود تحتاج إلى خبرة فنية وقدرة على معالجة البيانات عن بعد وتحديد مكان وجودها[1].

ثانياً: أن إجراء التفتيش فيه اعتداء على الحقوق: إذ يعتبر اجراء التفتيش من قبيل الاجراءات التي تمسّ بحقوق وحريات وحرمة الحياة الخاصة للأفراد لما فيه من بحث في خصوصياتهم للتفتيش عن الأدلة[2]، لذا فإن هذا الأمر يشكل عقبة أمام الجهات المختصة مما يتوجب عليهم عند القيام به أن يتخذوا كافة الضمانات لحماية الحقوق والحريات والالتزام بحدود إجراء التفتيش وعدم تجاوزه أو التعسف فيه.

ثالثاً: عدم تلقي الجهات المختصة ابلاغ عن الجرائم المرتكبة: في كثير من الأحيان يحجم المجني عليه عن الابلاغ عن الجريمة المرتكبة ضده؛ وذلك خوفاً على سمعته –خاصة في الجرائم الماسّة بالعرض والشرف– وعلى مكانته وعدم اهتزاز ثقته أمام الناس وكذلك لإخفاء أسلوب ارتكاب الجريمة حتى لا يتم تقليده من قبل الآخرين[3]، وفي الحقيقة إن عدم قيام المجني عليه بالإبلاغ عن الجريمة المرتكبة ضده يؤدي إلى تمادي الجناة في أفعالهم فمثلاً في جريمة الابتزاز الإلكتروني إذا لم يتم التبليغ عنها لملاحقة الجاني فإنه سيزداد استغلاله ويطلب مبالغ مالية أكثر، كما أن عدم الإبلاغ عن الجرائم يعمل على تشجيع الآخرين على ارتكاب المزيد من الجرائم.

رابعاً: صعوبات تتعلق بنقص الخبرة لدى جهات الاستدلال والتحقيق: حيث تعتبر نقص الخبرة في التعامل مع الأدلة لدى الجهات المختصة بالتحقيق من الصعوبات التي تؤثر على إجراءات التحقيق وخاصة إجراء التفتيش، فالجرائم الإلكترونية تمتاز بحداثتها وتجددها بالتالي تتطلب من القائمين على التفتيش الإلمام

---

[1] الدبك، رمزي رشدي: **الاثبات في الدعاوى الجزائية باستخدام وسائل التقنية(التكنولوجيا) الحديثة**، إدارة البحث الجنائي، الأردن، ص9.

[2] الجنبيهي، منير محمد: **صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات**، مرجع سابق، ص116.

[3] الكعبي، محمد عبيد: **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت**، القاهرة–مصر: دار النهضة العربية، ص37+38.

الكافي فيها وكيفية التعامل معها وتطوير مهاراتهم بشكل مستمر ومتجدد، إذ لا يكفي أن يكون لديهم فقط خلفية قانونية وإنما يجب أن يتوافر لديهم الخبرة الفنية في مجال الجريمة الإلكترونية[1].

خامساً: صعوبات تتم مواجهتها أثناء القيام بإجراء التفتيش: وتتمثل هذه الصعوبات في التعامل بشكل خاطئ مع الأجهزة الإلكترونية ومن التصرفات الخاطئة التي يتم ارتكابها: أ-إغلاق جهاز الحاسوب بصورة خاطئة مما يؤدي إلى فقدان المعلومات والأدلة الإلكترونية، ب-أن يتم فك الأسلاك والتوصيلات وعدم معرفة كيفية توصيلها بشكل صحيح، ج- عدم تأمين التيار الكهربائي وانقطاعه بصورة مفاجئة عن الجهاز المراد تفتيشه مما يؤدي إلى ضياع المعلومات، د-عدم اتخاذ الإجراءات الفنية والاحتياطات اللازمة في التعامل مع جهاز الكمبيوتر الذي يقوم الجاني بتهيئته للتفجير أو التدمير في حالة القيام بالضغط على زر التشغيل[2].

سادساً: الجريمة الإلكترونية جريمة عابرة للحدود: إذ إن الجريمة غير مقيدة في حدود مكانية معينة وبالتالي يمكن ارتكابها في دولة معينة وتنتج آثارها في دولة أخرى، لذلك يواجه القائمين على التفتيش عليها صعوبة في الوصول إلى الأدلة وتحصيلها مما يدفعهم إلى اللجوء إلى التعاون الدولي وتبادل المساعدة في إجراء التفتيش، إلا أنّ هذا التعاون أيضاً يواجه مجموعة من الصعوبات ومن بينها:

1. عدم وجود نموذج موحد للنشاط الإجرامي: إذ لا يوجد اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت[3]، وذلك نظراً لاختلاف الثقافات والعادات بين الدول فقد يكون الفعل مجرم في دولة ويكون مباحاً في دولة أخرى.
2. مشكلة الاختصاص في الجرائم الإلكترونية: إذ تعدّ الجرائم الإلكترونية من أكثر الجرائم التي تثير إشكالية فيما يتعلق بالاختصاص سواء على المستوى المحلي أو الدولي، إلا أنه يمكن مواجهة المشكلة

---

[1] حجازي، عبدالفتاح بيومي: **مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت**، مرجع سابق، ص123.

[2] الجنبيهي، منير محمد: **صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات**، مرجع سابق، ص 107.

[3] الطحاوي، أحمد يوسف: **الأدلة الإلكترونية ودورها في الإثبات الجنائي**، مرجع سابق، ص164.

على المستوى المحلي بالرجوع إلى القواعد الإجرائية المحددة قانوناً[1]، وتبقى المشكلة الأكبر هي بالنسبة للاختصاص على المستوى الدولي إذ يحدث تنازع في الاختصاص بين الدول لوجود اختلاف في التشريعات والنظم القانونية.

3. عدم وجود قنوات اتصال: يكمن الهدف الأساسي من التعاون الدولي في مجال الجريمة الإلكترونية في جمع المعلومات والبيانات المتعلقة فيها، ولضمان تحقيق هذا الهدف فإنه لا بد من وجود نظام اتصال يسمح بالتواصل بين الجهات المختصة بإجراء التفتيش إلا أنه في الحقيقة لا يوجد مثل هذا النظام مما شكّل صعوبة في عدم القدرة على جمع الأدلة المطلوبة[2].

4. صعوبات خاصة تتعلق بالمساعدات القضائية الدولية: حتى يتم تحقيق المساعدات القضائية فإنه لا بدّ من تقديم طلبات إنابة قضائية دولية والتي يتم تقديمها وتسليمها بوساطة الطرق الدبلوماسية والتي تتمتع بالبطء والتعقيد خاصّة وأنّ الدولة التي تتلقى الطلب غالباً ما تكون متباطئة بالرد على الطلب[3]، وهذا الأمر بالطبع يتعارض مع طبيعة الجرائم الإلكترونية التي تكون بحاجة إلى التعامل بسرعة كبيرة لجمع الأدلة كون أن هذه الأدلة يمكن فقدانها وتدميرها بسهولة ولا تحتمل أي تأخير في جمعها.

5. تنوع النظم القانونية الاجرائية: فالنظم القانونية الاجرائية تتنوع وتختلف من دولة إلى أخرى حيث يمكن أن تكون إجراءات التحري لجمع الاستدلالات والتحقيق قانونية أو تثبت فاعليتها في دولة معينة لكنها تعتبر غير قانونية وغير مسموح اجرائها أو عديمة الفائدة في دولة أخرى مثل المراقبة الإلكترونية[4]، بالتالي لا يوجد هناك أي تنسيق بين الدول فيما يتعلق بالإجراءات الجنائية المتبعة في الجرائم

---

[1] لطفي، خالد حسن أحمد: **جرائم الانترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني**، الطبعة الأولى، الاسكندرية–مصر: دار الفكر الجامعي، 2019، ص173.

[2] حبيباتني، بثينة: *معوقات مكافحة الجريمة المعلوماتية*، **مجلة العلوم الانسانية**، مجلد أ العدد50/ديسمبر 2018، ص91.

[3] الغافري، حسين بن سعيد بن سيف: **الجهود الدولية لمكافحة جريمة الانترنت**، ص54، انظر: https://knowledgemanagements.files.wordpress.com/2014/09/d8a7d984d8aad8b9d8a7d988d986-d8a7d984d8afd988d984d98a-d981d98a-d985d983d8a7d981d8add8a9-d8acd8b1d8a7d8a6d985-d8a7d984d8a7d986d8aad8b1.pdf

[4] خراشي، عادل عبدالعال إبراهيم: **اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها**، ص237.

الإلكترونية سواء في إجراءات الاستدلال أو التحقيق أو المحاكمة[1]، وبالإضافة إلى ذلك يمكن أن تكون دولة تسمح باستخدام دليل إثبات ترى أنه تم جمعه والحصول عليه بطريقة مشروعة إلا أن دولة أخرى تعتبرها غير مشروعة مما يؤدي إلى ضياع الدليل[2].

[1] حشيفة، عبدالهادي: **التعاون الدولي في مجال مكافحة الجرائم الإلكترونية**، جامعة زيان عاشور-الجلفة-الجزائر، 2020/2019،ص50.

[2] الغافري، حسين بن سعيد بن سيف: **الجهود الدولية لمكافحة جريمة الانترنت**، مرجع سابق، ص52.

الخاتمة

خلاصة القول، إن الجرائم الإلكترونية تتنامى وتتزايد وفي تطور مستمر مما جعلها في وقتنا الحالي ظاهرة خطيرة تؤثر بشكل سلبي على المجتمع.

وتناولت هذه الدراسة موضوع إجراء التفتيش في الجرائم الإلكترونية والذي يعد من أكثر إجراءات التحقيق التي تؤثر بشكل مباشر على حقوق وحريات الأفراد وتمسّ خصوصياتهم، مما يستدعي الأمر إلى ضرورة إحاطة هذا الإجراء بمجموعة من الضمانات التي تعمل على حماية حقوق الأفراد.

وأظهرت هذه الدراسة مدى الحاجة إلى وجود نظام إجرائي يعمل على تنظيم إجراء التفتيش في الجرائم الإلكترونية، وذلك لسد القصور الحاصل في القوانين الإجرائية فيما يتعلق بالتفتيش في الجرائم الإلكترونية، إذ إن القواعد الإجرائية التقليدية لا تكفي لتطبيقها على الجرائم الإلكترونية وإنّما يجب توافر إجراءات خاصّة لذلك.

وتوصلت هذه الدراسة إلى مجموعة من النتائج والتوصيات وهي على النحو الآتي:

أولاً: النتائج

1. يعد إجراء التفتيش من أخطر إجراءات التحقيق كونه يتم فيه الاطلاع على أسرار الأفراد مما يجعله يمسّ بحقوقهم وخصوصياتهم، لذلك لا بدّ من توفير الضمانات ومراعاتها حتى لا يتم التعسف في إجراء التفتيش وتجاوز حدوده.
2. نظراً لاعتبار الجرائم الإلكترونية من الجرائم الصعبة التي تكون بحاجة إلى تعامل خاص معها ومع الأدلة والتمتع بخبرة وقدرة على البحث بشكل فعّال، فإن إجراء التفتيش يتم من قبل سلطة أصلية وهي نيابة مكافحة الجرائم الإلكترونية وسلطة استثنائية تتمثل بوحدة متخصصة يطلق عليها وحدة الجرائم

الإلكترونية والتي تضم عناصر من قوى الأمن وجهاز الشرطة، وتكون هذه السلطات متدربة ومتمتعة بخبرة فنية وتقنية للتعامل مع الوسائل التكنولوجية.

3. إن إجراء التفتيش في الجرائم الإلكترونية يمتاز باستخدام تقنيات وأساليب فنية خاصة للتنقيب والبحث عن الأدلة الإلكترونية والتي قد تكون أدلة مادية وأدلة معنوية.
4. إمكانية امتداد إجراء التفتيش خارج حدود الدولة عند ارتكاب جريمة إلكترونية عابرة للحدود ويجري ذلك من خلال اللجوء إلى تبادل المساعدة القضائية الدولية وطلب الإنابة القضائية في القيام بالتفتيش.
5. خلو التشريع الإجرائي الفلسطيني والمصري من أي تنظيم لعملية الإنابة القضائية الدولية، إلا أن مصر قامت بمعالجة ذلك بإبرام الاتفاقيات الثنائية.
6. حاجة الأدلة الإلكترونية خاصة الأدلة المعنوية إلى إجراءات خاصة لضبطها والتعامل معها بلين وحذر وحفظها في أماكن مخصصة لضمان سلامتها.
7. على الرغم من إصدار القرار بقانون بشأن الجرائم الإلكترونية رقم 10 لسنة 2018 لتنظيم الجريمة الإلكترونية إلا أنه ما زال هناك بعض القصور التشريعي والذي بحاجة إلى معالجة.
8. إن الصعوبات التي يتم مواجهتها أثناء التفتيش في الجرائم الإلكترونية تفوق الصعوبات التي قد تواجه الجريمة التقليدية العادية، وقد تتعلق هذه الصعوبات إما بالجرائم الإلكترونية ذاتها أو بالجهات المسؤولة عن إجراء التفتيش.

ثانياً: التوصيات

1. ضرورة معالجة القصور التشريعي الحاصل في قانون الإجراءات الجزائية من خلال إصدار قرار بقانون يعمل على تعديل بعض النصوص الواردة في القانون والمتعلقة بالتفتيش حتى تصبح شاملة لإجراء التفتيش في الجرائم الإلكترونية.

2. النص صراحةً على إجراء التفتيش للمكونات المعنوية لوسائل تكنولوجيا المعلومات وبيان كيفية إجراء التفتيش عليها.
3. ضرورة النص الصريح على أن يتم إجراء التفتيش من قبل أنثى عندما يكون التفتيش على وسائل تكنولوجية خاصة بأنثى وذلك حفاظاً على خصوصيتها.
4. النص الصريح لضبط أمر حضور المتهم أو الشهود عند إجراء التفتيش في الجرائم الإلكترونية وتوضيح فيما يجب اتخاذه عند عدم حضور المتهم ليتم حماية وضمان حقوق المتهم.
5. ضرورة التزام السلطات المختصة بالتفتيش بكافة الضوابط التي تعمل على تحقيق التوازن بين قيامها بعملها على أكمل وجه لكشف الحقيقة وبين حماية حقوق وحريات الأفراد من جهة أخرى.
6. العمل على تعزيز التعاون بين الدول من أجل تبادل المساعدة القانونية حتى يتم ملاحقة مرتكبي الجرائم الإلكترونية وتنظيم إجراءات التبادل قانونياً.
7. التسريع بالإجراءات واختصار الشكليات عند تقديم طلبات الإنابة القضائية وعلى أن يتم تنفيذها بصورة مباشرة من قبل الجهات المختصة من خلال ربط هذه الجهات بعضها البعض بواسطة قنوات اتصال.
8. مواكبة الجهات المختصة بإجراء التفتيش لكافة التطورات التقنية التي تطرأ على الوسائل التكنولوجية والحصول على التدريبات بصورة دورية حتى يتمكنوا من التعامل مع الجرائم الإلكترونية.
9. وجوب إصدار دليل إرشادي للجهات المختصة لكيفية التعامل مع الجرائم الإلكترونية والأدلة الناجمة عنها والعمل على تحديثه بشكل مستمر ليواكب التطورات في أساليب ارتكاب الجرائم الإلكترونية.
10. تعديل القرار بقانون بشأن الجرائم الإلكترونية لا سيما والمادة 2/52 التي تحدثت عن إمكانية تجديد إذن التفتيش عند وجود مبررات، بالتالي توضيح هذه المبررات حتى لا يتم التوسع فيها وترتيب الانتهاكات عليها.

11. عدم التردد أو الخوف عند الوقوع كضحية جريمة إلكترونية من أن يتم اللجوء الى الجهات المختصة لرفع دعوى كون أن من الصعوبات التي تواجهها الجهات المختصّة هو عدم الابلاغ عن الجريمة.

قائمة المصادر والمراجع

أولاً: المصادر

لسان العرب، لابن منظور الجزء السادس.

أ. التشريعات

الدستور المصري لعام 2014 والمعدّل في سنة 2019.

القانون الأساسي الفلسطيني المعدّل لسنة 2003.

القانون الكويتي رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات.

القرار بقانون الفلسطيني رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

القوانين النموذجية للإجراءات الجنائية.

قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

قانون الإجراءات الجنائية المصري رقم 150 لسنة1950.

قانون العقوبات الفلسطيني رقم 16 لسنة 1960.

قانون العقوبات المصري رقم 58 لسنة 1937 والمعدّل لسنة 2021.

قانون المحامين المصري المعدّل رقم 17 لسنة 1983.

قانون المحامين النظاميين الفلسطيني المعدّل رقم 3 لسنة 1999.

قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.

قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري لسنة 2012.

نظام مكافحة الجرائم المعلوماتية السعودي الصّادر في العام 2007.

ب. الاتفاقيات

اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

اتفاقية الرياض العربية للتعاون القضائي.

اتفاقية بودابيست لمكافحة الجرائم المعلوماتية لسنة 2001.

اتفاقية فيينا للعلاقات الدبلوماسية.

الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية.

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن جامعة الدول العربية لسنة 2010.

ثانياً: المراجع

أ. الكتب

إبراهيم، خالد ممدوح: **الجرائم المعلوماتية**، الإسكندرية–مصر: دار الفكر الجامعي، 2019.

إبراهيم، خالد ممدوح: **إجراءات التفتيش في الجرائم المعلوماتية**، مصر: دار الفكر الجامعي، 2022.

أحمد، حسام الدين محمد: **الإذن بالتفتيش والضبط**، الطبعة الثالثة، مصر: دار النهضة العربية، 2003.

أحمد، طارق عفيفي صادق: **الجرائم الإلكترونية جرائم الهاتف المحمول "دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي"**، الطبعة الأولى، القاهرة–مصر: المركز القومي للإصدارات القانونية، 2015.

الجنبيهي، منير محمد: **صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات**، الطبعة الأولى، الإسكندرية–مصر: دار الفكر الجامعي، 2019.

الجوخدار، حسن: **التحقيق الإبتدائي في قانون أصول المحاكمات الجزائية "دراسة مقارنة"**، عمان–الأردن: دار الثقافة للنشر والتوزيع، 2008.

الحسيني، سامي حسني: **النظرية العامة للتفتيش في القانون المصري والمقارن**، القاهرة–مصر: دار النهضة العربية، 1972.

الحلبي، محمد علي السالم: **شرح قانون العقوبات–القسم العام–**، عمّان–الأردن: دار الثقافة للنشر والتوزيع، 2011.

الخن، طارق: **الجرائم المعلوماتية**، سوريا: منشورات الجامعة الافتراضية السورية، 2018.

الديربي، عبد العال و اسماعيل، محمد صادق: **الجرائم الإلكترونية دراسة قضائية مقارنة**، الطبعة الأولى، القاهرة–مصر: المركز القومي للإصدارات القانونية، 2012.

الرومي، محمد أمين: **جرائم الكمبيوتر والإنترنت**، الإسكندرية–مصر: دار المطبوعات الجامعية، 2003.

الزاملي، إبراهيم سالم: **فلسطين في التقارير البريطانية 1919–1947**، دار ابن رشد.

السعيد، كامل: **شرح قانون أصول المحاكمات الجزائية**، الطبعة الثالثة، عمان–الاردن: دار الثقافة للنشر والتوزيع،2010.

الشهاوي، قدري عبدالفتاح: **مناط التفتيش قيوده وضوابطه في التشريع المصري، العربي والأجنبي**، الطبعة الأولى، القاهرة–مصر: دار النهضة العربية، 2006.

الشواربي، عبدالحميد: **إذن التفتيش في ضوء القضاء والفقه**، الإسكندرية–مصر: منشأة المعارف.

الطحاوي، أحمد يوسف: **الأدلة الإلكترونية ودورها في الإثبات الجنائي "دراسة مقارنة"**، مصر: دار النهضة العربية، 2015.

الطوالبة، علي حسن: **التفتيش الجنائي على نظم الحاسوب والانترنت دراسة مقارنة**، إربد–الأردن: عالم الكتب الحديث، 2004.

الطوالبة، علي حسن محمد: **التفتيش الجنائي على نظم الحاسوب والإنترنت**، البحرين،2010.

العبادي، محمد عبدالكريم: **القناعة الوجدانية للقاضي الجزائي ورقابة القضاء عليها**، الطبعة الأولى ، عمان–الاردن: دار الفكر، 2010

العبيدي، صدام حسين ياسين: **جرائم الإنترنت وعقوباتها في الشريعة الإسلامية والقوانين الوضعية**، الطبعة الأولى، مصر: المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع،2019.

العريان، محمد علي: **الجرائم المعلوماتية**، الإسكندرية–مصر: دار الجامعة الجديدة للنشر، 2004.

الفقي، عمرو: **الجرائم المعلوماتية جرائم الحاسب الآلي والانترنت في مصر والدول العربية**، مصر: المكتب الجامعي الحديث، 2006.

الكعبي، محمد عبيد: **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت**، القاهرة–مصر: دار النهضة العربية.

المرّي، بهاء: **شرح قانون مكافحة جرائم تقنية المعلومات وحجية الدليل الرقمي في الإثبات**، مصر: العربية للنشر والتوزيع، 2019.

الملط، أحمد خليفة: **الجرائم المعلوماتية دراسة مقارنة**، الطبعة الثانية، الإسكندرية–مصر: دار الفكر الجامعي، 2006.

المناعسة، أسامة أحمد والزعبي، جلال محمد: **جرائم تقنية نظم المعلومات الإلكترونية دراسة مقارنة،** عمّان–الأردن: دار الثقافة للنشر والتوزيع، 2017.

المومني، نهلا عبدالقادر: **الجرائم المعلوماتية،** عمّان–الأردن: دار الثقافة للنشر والتوزيع،2008.

الهيتي، محمد حمّاد مرهج: **جرائم الحاسوب ماهيتها موضوعها أهم صورها والصعوبات التي تواجهها،** الطبعة الأولى، عمّان –الأردن: دار المناهج للنشر والتوزيع، 2006.

الوليد، ساهر إبراهيم شكري: **شرح قانون الإجراءات الجزائية الفلسطيني،** الطبعة الأولى، غزة–فلسطين: بدون ناشر، 2012.

برّاك، أحمد و جرادة، عبدالقادر: **الجرائم الإلكترونية في التشريع الفلسطيني دراسة تحليلية تأصيلية مقارنة،** رام الله–فلسطين: دار الشروق للنشر والتوزيع، 2019.

بن يونس، عمر: **الاتفاقية الأوروبية حول الجريمة الافتراضية (المذكرة التفسيرية)،** الطبعة الأولى المعربة، 2005.

ثروت، جلال: **نظم الإجراءات الجنائية،** مصر: دار الجامعة الجديدة، 2003.

ثروت، جلال و عبدالمنعم، سليمان: **أصول المحاكمات الجزائية الدعوى الجنائية،** الطبعة الأولى، بيروت–لبنان: المؤسسة الجامعية للدراسات والنشر والتوزيع، 1996.

جابر، محمود محمد محمود: **الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقّالة–جرائم نظم الإتصالات والمعلومات–**، مصر: المكتب الجامعي الحديث، 2018.

حجازي، عبدالفتّاح بيومي: **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت،** الإسكندرية–مصر: دار الفكر الجامعي،2006.

حجازي، عبدالفتّاح بيومي: **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت**، مصر: دار الكتب القانونية،2007.

حجازي، عبدالفتّاح بيومي: **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي**، الطبعة الأولى، الإسكندرية–مصر: دار الفكر الجامعي، 2006.

حجازي، محمد: **جرائم الحاسبات والإنترنت الجرائم المعلوماتية**، 2005.

حسين، سامي جلال فقي: **التفتيش في الجرائم المعلوماتية دراسة تحليلية**، مصر: دار الكتب القانونية، 2011.

راسخ، إبراهيم: **التحقيق الجنائي العلمي**، الطبعة الأولى، دبي–الإمارات: أكاديمية شرطة دبي كلية القانون وعلوم الشرطة، 1991.

سلامة، محمد عبدالله أبو بكر: **جرائم الكمبيوتر والإنترنت**، الإسكندرية–مصر: المكتب العربي الحديث، 2007.

شاهين، محمد كمال: **الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الإبتدائي**، الإسكندرية–مصر: دار الجامعة الجديدة، 2018.

طنطاوي، إبراهيم حامد: **الدفع ببطلان إذن النيابة العامة بالتفتيش**، الطبعة الثانية، الإسكندرية–مصر: دار النهضة العربية، 1997.

طه، وليد: **التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابيست**، مصر، بدون ناشر.

عبدالباقي، مصطفى: **شرح قانون الإجراءات الجزائية الفلسطيني**، بيرزيت–فلسطين: وحدة البحث العلمي والنشر كلية الحقوق والإدارة العامة، 2015.

عبدالستّار، فوزية: **شرح قانون الإجراءات الجنائية وفقاً لأحدث التعديلات**، القاهرة–مصر: دار النهضة العربية، 2010.

عبد الستّار، فوزية: **شرح قانون العقوبات القسم العام**، القاهرة–مصر: دار النهضة العربية، 1987

عبدالمطلب، ايهاب: **تفتيش الأشخاص والأماكن**، الطبعة الأولى، مصر: المركز القومي للإصدارات القانونية، 2009.

عطاالله، إمام حسين: **جرائم تقنية المعلومات في التشريعات والصكوك العربية**، الرياض–السعودية: دار جامعة نايف للنشر ، 2017.

عطية، طارق إبراهيم الدسوقي: **الأمن المعلوماتي للنظام القانوني للحماية المعلوماتية**، الإسكندرية–مصر: دار الجامعة الجديدة للنشر، 2009.

عيّاد، سامي علي حامد: **الجريمة المعلوماتية وإجرام الإنترنت**، الإسكندرية–مصر: دار الفكر الجامعي، 2007.

فضل، سليمان أحمد: **المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية(الإنترنت)**، القاهرة–مصر: دار النهضة العربية، 2013.

فكري، أيمن عبدالله : **الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية**، الرياض–السعودية: مكتبة القانون والاقتصاد، 2014.

كيروز، جيمس وروس، كيت: **شبكات الحاسب والانترنت أسس ومبادئ الشبكات والإنترنت**، السعودية: دار العبيكان للنشر، 2012.

لطفي، خالد حسن أحمد: **القانون الواجب التطبيق على الجريمة المعلوماتية**، الإسكندرية–مصر: دار الفكر الجامعي، 2020.

لطفي، خالد حسن أحمد: **آليات التحقيق الجنائي في جرائم تقنية المعلومات**، الإسكندرية–مصر: دار الفكر الجامعي، 2019.

لطفي، خالد حسن أحمد: **جرائم الإنترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني**، الطبعة الأولى، الإسكندرية–مصر: دار الفكر الجامعي، 2019.

محمود، عبدالله ذيب و درّاج، أسامة اسماعيل: **الوجيز في الجرائم الإلكترونية القواعد الموضوعية والإجرائية**، عمّان–الأردن: دار الثقافة للنشر والتوزيع، 2022.

موسى، مصطفى محمد: **التحقيق الجنائي في الجرائم الإلكترونية**، الطبعة الأولى، مصر: مطابع الشرطة، 2009.

نجم، محمد صبحي: **قانون العقوبات القسم العام النظرية العامة للجريمة**، الطبعة الخامسة، عمّان–الأردن: دار الثقافة للنشر والتوزيع،2014.

نمور، محمد سعيد: **شرح لقانون أصول الإجراءات الجزائية**، الطبعة الأولى، عمان–الأردن: دار الثقافة ، 2005.

هروال، نبيلة هبة: **الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات دراسة مقارنة**، الإسكندرية–مصر: دار الفكر الجامعي، 2007.

هورنجور، تشالز: **الجرائم الإلكترونية والمعلوماتية–بطاقات الائتمان– الكمبيوتر والإنترنت**، مصر: مؤسسة شباب الجامعة، 2018.

ب. الرسائل الجامعية

أبو الرب، نبيل محمود فريد: **مفهوم الجرائم المعلوماتية وتحدياتها التشريعية في فلسطين**، رسالة ماجستير، جامعة النجاح الوطنية، نابلس–فلسطين، 2018.

أبو داسر، عبدالله بن سعيد: **إثبات الدعوى الجنائية**، رسالة دكتوراة، جامعة الإمام محمد بن سعود الإسلامية، 1443هـ.

البرايسة، حسين محمد فلاح: **الركن المعنوي للجرائم الإلكترونية وفقاً لقانون العقوبات الأردني**، رسالة ماجستير، جامعة الشرق الأوسط، عمّان–الأردن، 2021.

البغو، ابتسام: **اجراءات المتابعة الجزائية في الجريمة المعلوماتية**، رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي، الجزائر،2015–2016.

الخضري، سمر خضر صالح: **أحكام تسليم المجرمين في فلسطين**، رسالة ماجستير، جامعة الأزهر، غزة–فلسطين، 2010.

الزبن، هايل صالح: **الأساس القانوني لمنح الحصانات والامتيازات الدبلوماسية**، رسالة ماجستير، جامعة الشرق الأوسط، عمّان–الأردن، 2011.

الشعّار، خالد علي نزّال: **التحقيق الجنائي في الجرائم الإلكترونية**، رسالة دكتوراة، جامعة المنصورة–مصر.

العجمي، عبدالله دغش: **المشكلات العملية والقانونية للجرائم الإلكترونية**، رسالة ماجستير، جامعة الشرق الأوسط، عمّان–الأردن، 2014.

العفيفي، يوسف خليل يوسف: **الجرائم الإلكترونية في التشريع الفلسطيني دراسة تحليلية مقارنة**، رسالة ماجستير، الجامعة الإسلامية، غزة–فلسطين، 2013.

المصري، نداء نائل فايز: **خصوصية الجرائم المعلوماتية**، رسالة ماجستير، جامعة النجاح الوطنية، نابلس–فلسطين، 2017.

الهيتي، بلال محمود مرهج: **الجرم المشهود وأثره في توسيع سلطات الضابطة العدلية دراسة مقارنة بين القانونين الأردني والعراقي**، رسالة ماجستير، جامعة الشرق الأوسط للدراسات العليا، الأردن، 2010–2011.

اليماحي، عبدالله راشد سعيد: **إجراءات تفتيش وضبط نظم الحاسب الآلي والإنترنت**، رسالة ماجستير، أكاديمية شرطة دبي، الإمارات، 2014.

باشي، علا شكيب: **التحفظ على المعاهدات الدولية متعددة الأطراف**، رسالة ماجستير، جامعة الشرق الأوسط للدراسات العليا: عمّان–الأردن، 2008.

بخي، فاطمة الزهراء: **إجراءات التحقيق في الجريمة الإلكترونية**، رسالة ماجستير، جامعة المسيلة، الجزائر، 2013–2014.

براهيمي، جمال: **التحقيق الجنائي في الجرائم الإلكترونية**، رسالة دكتوراة، جامعة مولود معمري، الجزائر، 2018.

بغدادي، أدهم باسم نمر: **وسائل البحث والتحري عن الجرائم الإلكترونية**، رسالة ماجستير، جامعة النجاح الوطنية، نابلس–فلسطين، 2018.

حبيب، معن إبراهيم جبّار: **الحصانات الخاصة لمقر البعثة الدبلوماسية والاستثناءات الواردة عليها في ضوء اتفاقية فيينا**، رسالة ماجستير، جامعة الشرق الأوسط، عمّان–الأردن، 2012.

حسن، آمال عبدالرحمن يوسف: **الأدلة العلمية الحديثة ودورها في الإثبات الجنائي**، رسالة ماجستير جامعة الشرق الأوسط، عمان–الأردن، 2011–2012.

حشيفة، عبدالهادي: **التعاون الدولي في مجال مكافحة الجرائم الإلكترونية**، رسالة ماجستير، جامعة زيان–عاشور، الجلفة–الجزائر، 2019–2020.

عموري، أشرف أحمد مصطفى: **التفتيش في الجرائم الإلكترونية**، رسالة ماجستير، جامعة القدس، فلسطين، 2018.

غانم، محمد علي مصطفى: **تفتيش المسكن في قانون الإجراءات الجزائية الفلسطيني دراسة مقارنة**، رسالة ماجستير، جامعة النجاح الوطنية، نابلس–فلسطين، 2008.

قدواري، ابراهيم: **التفتيش في قانون الإجراءات الجزائية الجزائري**، رسالة ماجستير، جامعة محمد خيضر، الجزائر، 2015–2016.

هروال، نبيلة هبة: **جرائم الإنترنت دراسة مقارنة**، رسالة دكتوراة، جامعة أبي بكر بلقايد، تلمان– الجزائر، 2013–2014.

ج. **الأبحاث**

الدبك، رمزي رشدي: **الإثبات في الدعاوى الجزائية باستخدام وسائل التقنية التكنولوجية الحديثة**، إدارة البحث الجنائي، الأردن.

الغافري، حسين بن سعيد بن سيف: **الجهود الدولية لمكافحة جريمة الإنترنت.**

خراشي، عادل عبدالعال إبراهيم: **إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها.**

عبدالمطلب، ممدوح عبدالحميد: **استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم على الكمبيوتر**، 2008.

د. **المجلات**

ابراهيم، محمد فوزي: *دور مأمور الضبط القضائي في الحصول على الدليل الإلكتروني*، **مجلة البحوث القانونية والاقتصادية**، الشارقة، العدد66/اغسطس/ 2018.

أحمد، إيناس محمد: *الحماية الجنائية للبعثات الدبلوماسية*، **مجلة جامعة تكريت للحقوق**، المجلد1، العدد2/2017.

الأنصاري، وحيد حسين: *طرق نظم الإنترنت باستخدام Visual Basic*، **مجلة كلية التراث الجامعة**، العدد7.

البشري، محمد الأمين: *التحقيق في جرائم الحاسب الآلي والانترنت*، **المجلة العربية للدراسات الأمنية والتدريب**، المجلد15، العدد30.

الحجار، عدنان إبراهيم و بشير، فايز خضر: *الأدلة الرقمية واثبات الجرائم السيبرانية ما بين التأصيل والتأويل*، **مجلة جامعة الاستقلال للأبحاث**، المجلد6، العدد1/2021.

الذنيبات، محمد جمال مطلق و العناسوة، معن أحمد: *التفتيش في الجرائم الإلكترونية ماهيته وشروطه الشكلية*، **المجلة الأردنية في القانون والعلوم السياسية**، مجلد13، العدد3/2021.

العبيدي، أسامة بن غانم: *التفتيش عن الدليل في الجرائم المعلوماتية*، **المجلة العربية للدراسات الأمنية والتدريب**، المجلد 29، العدد58.

العتيبي، زياد بن محمد عادي: *دراسة استطلاعية حول حجية الأدلة الرقمية في اثبات الجرائم المعلوماتية*، **المجلة الإلكترونية الشاملة متعددة التخصصات**، العدد2020/29.

العدواني، فهد دخين: **مشروعية الدليل الإلكتروني الصادر عن التفتيش الجنائي دراسة مقارنة**، دراسات في التعليم الجامعي، العدد 2017/36،

الفيل، علي: *إجراءات التحقيق الابتدائي في الجريمة المعلوماتية دراسة مقارنة*، **مجلة الحقوق**، المجلد8.

الكساسبة، فهد يوسف و الطراونة، مصطفى: *الضوابط القانونية للتفتيش بغير إذن في القانونين الأردني والمصري دراسة مقارنة*، **مجلة علوم الشريعة والقانون**، المجلد42، العدد2015/2.

حبيباتي، بثينة: *معوقات مكافحة الجريمة المعلوماتية*، **مجلة العلوم الإنسانية**، المجلد أ، العدد50/ ديسمبر 2018.

حسنية، أحمد أسامة: *الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية*، **مجلة جامعة الأزهر**، غزة– فلسطين، المجلد19، 2017.

خلف، جاسم خربيط: *التفتيش في الجرائم المعلوماتية*، **مركز دراسات البصرة والخليج العربي**، مجلد41، العدد2013/4.

رشاد، نوال محمد: *التفتيش القضائي*، **مجلة البحوث القانونية والاقتصادية**، المجلد 21، العدد2012/36.

زواوي، شنّة: *أحكام تفتيش المساكن والأشخاص والمركبات في القانون بين النظرية والتطبيق*، **مجلة الاجتهاد للدراسات القانونية والاقتصادية**، المجلد7، العدد2018/2.

زيدات، حابس يوسف: *مدى استيعاب النصوص التقليدية للسرقة الإلكترونية دراسة مقارنة*، **مجلة مركز حكم القانون ومكافحة الفساد**، العدد2019/2.

شكر، نجيب: *الحصانة البرلمانية ضد الإجراءات الجنائية*، **مجلة المحقق الحلّي للعلوم القانونية والسياسة**، العدد1 للسنة الخامسة.

شهاب، أحمد عبدالحكيم عبدالرحمن: *شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي المصري*، **مجلة الاجتهاد للدراسات القانونية والاقتصادية**، مجلد7، عدد2/2018.

قرون، نورهان و بوضياف، جهاد و العيفة، رحيمة: *تكنولوجيا المعلومات والاتصال كركيزة أساسية لعملية التدريب الإلكتروني*، **مجلة التعليم عن بعد**، جامعة بني سويف، اتحاد الجامعات العربية، المجلد8، العدد15/ديسمبر 2020.

محمودي، سماح: *مشكلات التفتيش الجنائي عن المعلومات في الكمبيوتر والانترنت*، **مجلة الحقوق والعلوم السياسية**، العدد8/2017 الجزء الأول.

ملالحة، عبدالرحمن عوض رجا وفتيحة، عمارة: *التفتيش كإجراء تحقيق بين القانون الفلسطيني والجزائري*، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، المجلد5، العدد2/2020.

موسى، منى عبد العالي وهادي، مصطفى كريم: *وسائل اثبات جريمة الإزعاج بواسطة الرسائل السلكية واللاسلكية*، **مجلة جامعة بابل للعلوم الانسانية**، المجلد26، العدد9/2018.

نجيب، هند: *ضبط الأدلة في الجرائم الإلكترونية بين الإجراءات التقليدية والإجراءات الحديثة*، **المجلة الجنائية القومية**، المركز القومي للبحوث الاجتماعية والجنائية، المجلد61، العدد3/2018.

نصيف، صفاء حسن: *التحديات الإجرائية المتصلّة بالجرائم المعلوماتية*، **مجلة العلوم القانونية والسياسية**، مجلد 5، العدد2/2016.

هـ. المقالات

شمس الدين، أشرف توفيق: **مدى دستورية تفتيش الهاتف المحمول كأثر للقبض دراسة مقارنة**، مقال منشور على موقع منشورات قانونية، 2021.

عامر، عادل: **مظاهر صعوبة اثبات الجريمة الإلكترونية**، مقال منشور على موقع دنيا الوطن.

عربوز، فاطمة الزهراء: *التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية*، **مركز جيل البحث العلمي**، العدد2019/34.

كمال، صابر: *التلبس في الجريمة المعلوماتية*، **مقال منشور في مجلة القانون والأعمال الدولية-جامعة الحسن الأول-، المغرب**، 2019.

و. المحاضرات

بعلي، حمزة وقدوم، أزهر: **دور الشبكات المعلوماتية في الحد من أخطار المخدرات من خلال مواقع التواصل الاجتماعي**، الملتقى الوطني الأول حول تعاطي المخدرات في المجتمع الجزائري، الأسباب الآثار طرق الوقاية والعلاج، جامعة قالمة، الجزائر، 2018.

خلف، مازن: **محاضرة بعنوان تنفيذ التفتيش والبيانات التي يتضمنها أمر التفتيش**، الجامعة المستنصرية، العراق، 2015.

ز. المواقع الإلكترونية

الموقع الرسمي للنيابة العامة في فلسطين: http://pgp.ps/ar/SP/Pages/TheAnti-CyberCrimesProsecution.aspx

موقع بوابة مصر للقانون والقضاء:

https://www.laweg.net//Default.aspx?action=ViewActivePages&ItemID=36537&Type=6

موقع المقتفي القانوني:

http://muqtafi2.birzeit.edu/yamen2/ar/legislations/act_card/JTJGZGIlMkZtdXF0YWZpJTJGYWN0JTJGeG1sJTJGMTkzNCUyRmFnbW50X0hpZ2hDb21t=aXNzaW9uZXJfMTkzNC0wNy0yNl9hciUyRjg2NTBfMTkzNC54bWw

موقع بوابة وزارة العدل المصرية: departmentic.jp.gov.eg/competence_m

موقع الموسوعة العربية الشاملة: https://www.mosoah.com/computer-and-electronics/networking/%D8%AA%D8%B9%D8%B1%D9%8A%D9%81-%D8%A7%D9%84%D8%B4%D8%A8%D9%83%D8%A7%D8%AA-%D9%88%D8%A7%D9%86%D9%88%D8%A7%D8%B9%D9%87%D8/%A7

ح. المراجع الأجنبية

Federal Guidelines for searching and seizing computers/July 1994/USA Department of Justice Criminal Division – office of Professional Development and Training.

Searching and Seizing Computers and Obtaining Electronic Evidence In Criminal Investigations، office of legal education executive office for United States Attorneys، USA، 1979.

An-Najah National University

Faculty of Graduate Studies

INSPECTION OF ELECTRONIC CRIMES: A COMPARATIVE ANALYTICAL STUDY

By

Nadine Mahmood Mohammad AL-Shayeb

Supervisor

Dr. Ahmad Barak

This Thesis is Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Public Law, Faculty of Graduate Studies, An-Najah National University, Nablus - Palestine.

2023

INSPECTION OF ELECTRONIC CRIMES: A COMPARATIVE ANALYTICAL STUDY

By

Nadine Mahmood Mohammad AL-Shayeb

Supervisor

Dr. Ahmad Barak

Abstract

Cybercrimes are contemporary crimes that have unique technical specificities. Their unique nature creates the need to follow special methods in dealing with these crimes, including how to search for them and collect relevant evidence. The inspection process is generally followed to uncover the truth by searching and excavating for evidence.

This study has a critical role in revealing how the inspection process in cybercrimes is conducted by the competent authorities, which typically have high technical expertise in dealing with these crimes. In addition, this study highlights the methods used in obtaining, controlling and preserving evidence resulting from these crimes.

This study explores whether the Palestinian legislator was able to issue a law decree on cybercrimes to organize the investigation procedure and allow for effective prosecution of these crimes. The objective of this study is to clarify the cybercrimes investigation process, its conditions, as well as the implementation mechanism, including how to collect, control and preserve evidence, and the difficulties that are encountered during its implementation.

In order to conduct this study and achieve its objectives, the researcher used the comparative descriptive analytical approach. This approach is based on analyzing the legal provisions regulating the conduct of cybercrimes investigation and comparing the Palestinian and Egyptian legislations in an attempt to find similarities and differences between the relevant governing laws.

The study concludes that the investigation procedure in cybercrimes requires more intense procedural organization in Palestine, as it is considered one of the most significant and dangerous investigation procedures considering its role in detecting and

proving crimes. Currently, the existing Palestinian laws, whether procedural laws or those laws that regulate cybercrimes, suffer from a deficiency in organizing this procedure.

Keywords: Electronic crimes; Electronic Inspection; Criminal Evidence; Electronic Evidence.