

إشكالية التفتيش في الجريمة المعلوماتية *problem of electronic inspection*



سهيلة طمين¹ *

كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو – الجزائر.¹
Souhila Temine^{1*}

¹ University of Mouloud Mammeri Tizi-ouzou (Algeria)

تاريخ الاستلام: 2024/12/23 تاريخ القبول للنشر: 2025/04/08 تاريخ النشر: 2025/06/30



ملخص: التفتيش الإلكتروني إشكالية أفرزها التطور الحديث في الجريمة المعلوماتية، الذي يهدف إلى الوصول للأدلة المعلوماتية أو البيانات المخزنة في الوسائط الإلكترونية وأنظمة الحاسوب. وكونه إجراء ينتهك حياة الأفراد الخاصة، خاصة وأنه ينصب على المكونات المادية والمعنوية للحاسب الآلي، والتي تحتوي على كم هائل من أسرار الأشخاص، أخضعته القوانين الإجرائية إلى ضوابط قانونية، يجب على القائمين به مراعاتها خلال التفتيش، وإلا كان إجراءً باطلاً.

الكلمات المفتاحية: التفتيش الإلكتروني، مكونات الحاسوب، ضوابط التفتيش الإلكتروني.

Abstract : Electronic inspection is a problem emerged from the recent development in cybercrime. Which it aims to access information evidence or data stored in electronic media and computer systems. As a procedure that affects the individuals privacy; especially since it affects the material and moral compositions of the computer, which contain a huge amount of people's secrets. The laws subject electronic inspection to legal controls that those conducting it must observe during the inspection; otherwise the procedure is invalid.

Keywords: electronic inspection; computer components; electronic inspection guarantees;

مقدمة:

التفتيش أخطر إجراء من إجراءات التحقيق التي يقوم بها المحقق، لأنه يقع على المتهم في شخصه أو منزله لضبط الأشياء المتعلقة بالجريمة، واحترام شخصية الإنسان وكفالة حياته الخاصة، وأمنه في مسكنه، وأمن سرية مراسلاته واتصالاته من الحقوق والحريات المكفولة دستورياً¹. كما يضمن القانون حريات الأفراد بتشريعه للجرائم ووضع العقوبات، والبحث عن هذه الجرائم يستلزم الحصول على الأدلة التي قد يستحيل الوصول إليها دون البحث عن الحقيقة لإلحاق الاتهام بالجناة الحقيقيين، لذا أوجبت القوانين ضرورة استصدار ترخيص مسبق لإجرائه بطريقة مشروعة².

تطور التكنولوجيا أثر على الحياة إيجاباً باختزال الوقت والجهد، وسلباً بظهور جرائم الحاسوب التي جمعت بين الذكاء الإنساني والذكاء الاصطناعي، وأضحت الجريمة المعلوماتية بشكل وأسلوب جديدين لا تكفي معهما الطرق التقليدية للوصول إلى دليل إثباتها، وصار ضرورياً أن يتم تعديل القواعد القانونية التي تنظم التفتيش، وفرض ضوابط على السلطة المختصة بمباشرة وتسمح بإجرائه، والحالات التي يمكن فيها مباشرته وشروطه.

محل التفتيش في الجريمة العادية هو مستودع السر، لذلك ضمن له القانون حرمة خاصة، كالمسكن، السيارة أو الرسائل، أما مستودع الجريمة المعاصرة هو الحاسوب الذي يتكون من مكونات مادية وأخرى معنوية، كما قد يتصل بشبكات سلكية ولا سلكية، يمكن أن تكون على المستوى المحلي أو الدولي. والتفتيش في كل هذه المعطيات يستدعي التساؤل عن الإطار القانوني للتفتيش في الجريمة المعلوماتية؟

الإجابة على هذا التساؤل يتطلب منا توضيح مفهوم التفتيش في الجريمة المعلوماتية (المبحث الأول)، وضماناته (المبحث الثاني).

¹ - المادتين 47 و48 من دستور الجمهورية الجزائرية الديمقراطية الشعبية، لسنة 2020 الصادر في الجريدة الرسمية للجمهورية الجزائرية /العدد 82 الصادر في 15 جمادى الأولى 1442 الموافق لـ 30 ديسمبر 2020.

² - حسام محمد نبيل الشنراقي، الجرائم المعلوماتية: دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني، دار الكتب القانونية، مصر، 2013، ص 457.

المبحث الأول

الإطار المفاهيمي للتفتيش في الجريمة المعلوماتية

يصنّف التفتيش على أنّه واحد من إجراءات التحقيق الذي تقوم به سلطة التحقيق كقاضي التحقيق أو النيابة العامة، من أجل إثبات الجريمة أو نفيها، كل هذا حسب طبيعة المَحَل، لهذا سنتناول ماذا نقصد بالتفتيش في الجريمة المعلوماتية (المطلب الأول)، وإلى محل التفتيش في الجريمة المعلوماتية (المطلب الثاني).

المطلب الأول: المقصود من التفتيش في الجريمة المعلوماتية

لتحديد المقصود بالتفتيش في الجريمة الحديثة واجب علينا أن نعرّفه (الفرع الأول) ثم نقوم بتحديد خصائصه (الفرع الثاني).

الفرع الأول: تعريف التفتيش في الجريمة المعلوماتية: يتفق الفقه الجنائي على أنّ التفتيش إجراء تحقيق، يتم مباشرة من طرف موظف مختص في البحث عن الأدلة المادية لجناية أو جُنحة، تكون قد انصبت على محل يتمتع بجُرمة، من أجل إثبات حدوثها وإحاقها بالمتهم، على أن يكون كل هذا وفق الضمانات والضوابط المكرّسة قانوناً³.

لا يختلف تعريف التفتيش في الجريمة التقليدية القديمة عن التفتيش في الجريمة المُستحدثة عبر الإنترنت إلا في المَحَل، حيث يُباشر في الجريمة المعلوماتية من قبل السلطة المُتخصّصة التي تلقت تكوين خاص في مجال المعلومات والدُّخول إلى تطبيقات المُعالجة الآلية للمُعطيات، وكل ما تَضُمّه من وسائل للتخزين ومن المُدخلات والمُخرجات، للتحري عن الأفعال غير المشروعة المرتكبة والتي تُشكل جناية أو جُنحة⁴.

الفرع الثاني: الخصائص المميزة للتفتيش في الجريمة المعلوماتية: بناءً على العنصر السابق الذي يتضمن تعريف التفتيش، نستنتج الخصائص المُختلفة للتفتيش، والتي نوردّها في التالي:

³ - براهيم جبال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص قانون، جامعة تيزي وزو، الجزائر، 2018، ص 14.

⁴ - علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العالمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، نظمتها أكاديمية شرطة دبي، مركز البحوث والدراسات، دبي، الإمارات العربية المتحدة، ع1، في الفترة الممتدة بين 26-28 نيسان 2003، ص 24. متوفر على الموقع:

<http://www.mohamah.net>

أولاً: هو من إجراءات التحقيق: صنفه تشريع مصر ضمن إجراءات التحقيق وأقرّ أنّ تفتيش المنازل من التحقيق، واشترط للجوء إليه الحصول على أمر أو إذن مسبق صادر من قاضي التحقيق⁵. والمشرع اللبناني أيضاً قد أخذ نفس موقف نظيره المصري، وصنّف دخول المنازل وتفتيشها من أعمال التحقيق⁶.

خوّل قانون الإجراءات الجزائية الجزائري⁷ لقاضي التحقيق، التّنقّل إلى منازل الأشخاص المتهمين، المشتبه في تورطهم بالجريمة أو الذين بحوزتهم أشياء لها علاقة بالجريمة، لإخضاعها للتفتيش والحصول على الأدوات المستعملة في ارتكابها. ونلاحظ أنّ إجراءات التفتيش في مرحلة جمع الاستدلالات هي نفسها إجراءات مرحلة التحقيق القضائي، وبهذا يفهم أنّ المشرع الجزائري قد صنف التفتيش من إجراءات التحقيق.

ثانياً: يتميز أنّه إجراء يهدف إلى البحث عن أدلة مادية: الغاية الأساسية من التفتيش هو الوصول والحصول على الأدلة المادية المستعملة في ارتكاب الجريمة، والمستمدة من مكونات مادية قد تؤثر مباشرة في اقتناع القاضي، وغالباً ما يخلّف الجاني في مكان الجريمة أداة أو أدوات مستعملة في ارتكاب الجريمة، كبصمات الأصابع وغيرها من الأدلة التي يُستعان بها في الإثبات والحكم.

سنّت جُل التشريعات قواعد خاصة بالبحث عن الدليل المادي الملموس، وأغفلت مسألة سنّ قواعد البحث عن الدليل الرقمي اللامادي، إلّا بعض التشريعات الأوروبية، بالرغم من أنّ هذا النوع الجديد من التفتيش بحاجة إلى قواعد إجرائية ذات طبيعة خاصة تتماشى وطبيعته اللامادية. خاصة بعد ثبوت عدم جدوى القواعد التقليدية عليه، وبالأخص ما تعلق بمسألة حرّية وخصوصية البيانات الرقمية للمتهم، التي تحتاج إلى تنظيم قانوني أكثر دقة لتتناسب وخصوصية الدليل اللامادي⁸.

ثالثاً: يتميز بالجبر والإكراه: هو تعرّض قانوني يتعدى وينتهك على حرمة وأسرار الإنسان أياً كان قالبها، خاصة القالب الإلكتروني الذي هو مستودع لكم كبير من البيانات والمعلومات التي لا يُحبذُ الإطلاع عليها، لكن يُقابل هذه الحرمة والجبر النيابة العامة في حدود القانون، تحقيقاً للتوازن بين الحرية الشخصية للمواطنين وحق

⁵ - المادة 1/191 من قانون الإجراءات الجزائية المصري رقم 37 لسنة 1972، متوفر على الموقع:

<http://www.manshurat.org>

⁶ - المادة 91 من قانون أصول المحاكمات الجزائية اللبناني متوفر على الموقع: <http://www.scribd.com>. أنظر أيضاً: غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلومات (الحاسب والإنترنت)، أطروحة أعدت لنيل درجة الدكتوراه في القانون، كلية الحقوق، الجامعة الإسلامية، لبنان، 2004، ص ص 543-544.

⁷ - المواد 79 إلى 81 من الأمر رقم 66-155 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية الجزائري، المعدل والمتمم.

⁸ - مخلوفي علمي وبومحراث ليندة، ضوابط التفتيش في الجرائم الإلكترونية، مجلة المعيار، مجلد 28، عدد 1، 2024، ص



المُجتمع في العقاب، دفاعاً عن مصالح المُجتمع التي يتم انتهاكها عن طريق ارتكاب الجرائم، فيتم التفتيش بقوة القانون وبضمانات إجرائية مُحددة قانوناً.

يجدر بنا أن نشير إلى حالة ما إذا رضي المُتهم بالتفتيش وسمح به، فهنا نكون أمام حالة تنازل منه، ولا يُعتبر هذا الإجراء تفتيشاً بمفهومه القانوني، لأنه يفتقر إلى خاصية الجبر والإكراه التي يَتميّز بها التفتيش، بل هو مجرد مُعانة أو اطلاع، ونتيجة هذا التنازل يفقد المُتهم حقه في الدّفع ببطلان التفتيش كونه لم يوجد أصلاً.⁹

رابعا: **المساس بحق السرية:** ينتهك ويُمس التفتيش حرمة الحياة الخاصة للأفراد والتي هي موضع الأسرار، فبالإضافة إلى تفتيش البيوت لتحريّ الدليل، يطال التفتيش الإلكتروني إلى تفتيش الأجهزة المعلوماتية المتواجدة بداخلها. كما يُمكن أن يتم هذا الإجراء عن بُعد، عن طريق اختراق الحواسيب والشبكات المعلوماتية والبريد الإلكتروني وهو ما يُسمى بالتفتيش عبر الخط، ويُباشر من قبل خبراء مُختصين في مُعالجة البيانات والحسابات إلكترونياً¹⁰.

المطلب الثاني: محل التفتيش في الجريمة المعلوماتية

يتكون نظام المعلومات طبقاً للمُذكّرة التفسيرية لاتفاقية بُودابست من مكونات مادية وأخرى منطقية، وموصول بشبكات اتصالات بُعدية سلكية ولا سلكية قد تكون على المُستوى المحلي أو الدّولي، فهل تخضع جميع هذه المكونات للتفتيش؟ وهل تخضع أيضاً هذه الشبكات المتصلة بالحاسوب إلى التفتيش؟

الفرع الأول: التفتيش في مكونات الحاسب الآلي: تنقسم هذه المكونات إلى نوعين، نتناول مسألة التفتيش فيهما على النحو التالي:

أولاً: صلاحية المكونات المادية للحاسوب للتفتيش: إنّ مسألة الدّخول إلى المكونات المادية للحاسوب، للبحث عن أدلة مادية تكشف حقيقة الجريمة المعلوماتية ومن ارتكبتها، يخضع لإجراءات التفتيش العادية، يحكمه أساساً طبيعة المكان المتواجدة فيه عاماً كان أو خاصاً.

1/ تفتيش المكونات المادية للحاسب المتواجدة في مكان خاص: تأخذ المكونات المادية للكمبيوتر محل التفتيش حُكم طبيعة المكان الخاص الموجودة به، كمنزل المُتهم أو مُلحقاته، فلا يُمكن تفتيشها إلا في الحالات وبالإجراءات والحماية التي قررها القانون لتفتيش المساكن ومُلحقاتها.

⁹ سامي جلال فقي، التفتيش في الجرائم الإلكترونية دراسة تحليلية، الطبعة الأولى، دار الكتب القانونية، القاهرة، 2012، ص 57.

¹⁰ هميسي رضا، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، عدد 05، جوان 2012، ص 161.



وضع القانون الجزائري لتفتيش المنازل في الجرائم المُتلبس بها، شرط الحصول على إذن مُسبق ومكتوب من وكيل الجمهورية أو من قاضي التحقيق، مع وجوب استظهاره قبل الوُلوُج إلى البيت والشروع في تفتيشه، على أن يُباشَر في الفترة المُمتدة بين الخامسة صباحاً والثامنة مساءً، مع شرط حضور صاحب المَسكن أو من يُمثله قانوناً، وإن تعذر حضوره أو من يُمثله، يستدعي ضابط الشرطة القضائية القائم بالتفتيش شاهدين على أن يكونا من غير الموظفين الخاضعين لسلطته¹¹.

يجب أن نُميز داخل المكان الخاص، بين ما إن كانت هذه المكونات منفصلة أو كانت مُتصلة بحواسيب وأجهزة أخرى مُتواجدة بمكان آخر كمنزل الغير، ففي هذه الحالة يوجب القانون على المحقق مُراعاة القيود والضمانات المُقررة قانوناً لتفتيش هذه الأماكن.

2/ حالة تواجد المكونات المادية للحاسوب في مكان عام: إذا تواجدت هذه المكونات المادية في أماكن عامة سواء كانت عامة بطبيعتها كالحدايق العامة، أو عامة بالتخصيص كمحلات بيع وصيانة الحواسيب ومقاهي الإنترنت، فإنها تخضع في تفتيشها لنفس أحكام وضمانات تفتيش تلك الأماكن، وكذلك الأمر بالنسبة للمكونات الموجودة لدى شخص ما، فإنها تخضع لأحكام تفتيش الأشخاص والشروط والضمانات القانونية لذلك¹²، بغض النظر عن صفة هذا الشخص مُبرمجاً كان، أو عامل صيانة أو موظفاً في شركة إنتاج برامج الكمبيوتر.

ثانياً: قابلية المكونات المعنوية للحاسوب للتفتيش: تفتقر هذه المكونات للمظهر المادي الذي يهدف إليه من التفتيش والذي هو البحث عن الأدلة المادية، ونتيجة للخاصية اللامادية لهذه المكونات ثار جدل فقهي حول مدى صلاحيتها لأن تكون محلاً للتفتيش.

أقر فريق من الفقه إمكانية أن تكون هذه المكونات محلاً للتفتيش، وحثتهم في ذلك أنه بالرغم من كون نُظم برامج الحاسوب عبارة عن دُبذبات وبصمات إلكترونية أو موجات مغناطيسية، فإنها قابلة للتسجيل والتحميل والتخزين على دغائم مادية يكون لها كيان مادي محسوس، وبالتالي يمكن إخضاعها للقواعد التقليدية للتفتيش. بينما أنكر فريق آخر صلاحية المكونات المعنوية للحاسوب أن تكون محلاً للتفتيش، محتجين بكونها غير مادية، لا يمكن إخضاعها للنصوص التقليدية للتفتيش، بل تتطلب أحكام تفتيش خاصة بها، أو تعديل أحكام التفتيش التقليدية لتتلاءم والتقنية الحديثة¹³.

مسايرةً لهذا التطور، استحدث المشرع الجزائري نصوص قانونية جديدة، يُمكن بموجبها تفتيش المكونات المعنوية والمنظومات المعلوماتية للحاسب الآلي، وهذا وفقاً للمادة الخامسة من القانون رقم 09-04، أين سمح للسلطات القضائية المختصة ولضباط الشرطة القضائية في حدود قانون الإجراءات الجزائية وفي الحالات

¹¹ - المواد من 44 إلى 47 من قانون الإجراءات الجزائية الجزائري، سالف الذكر.

¹² - براهيم جمال، المرجع السابق، ص 16.

¹³ - عربوز فاطمة الزهراء، التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية، مجلة جيل الأبحاث القانونية المعمقة، كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس الجزائر، مجلد 04، العدد 34، 2019، ص 105.

المنصوص عليها في المادة الرابعة من هذا القانون، الولوج بقصد التفتيش ولو عن بعد لمنظومة معلوماتية كلها أو جزء منها، والمعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين المعلومات¹⁴.

أكدت كذلك الاتفاقية الأوروبية للجرائم الإلكترونية حق الدول الأعضاء تفتيش النظم المعلوماتية، وحثت هذه الدول على تجسيد هذا الحق بوضوح في قوانينها الإجرائية، لتتفادى مسبقاً أي إشكال قد يثار حول الموضوع في المادة 19 فقرتها الأولى، أين سمحت بتفتيش أو الدخول لنظام الحاسوب أو لجزء منه والمعلومات المخزنة فيه، والوسائط التي تخزن فيها معلومات الحاسب ما دامت متواجدة في إقليمها¹⁵.

الفرع الثاني: مدى قابلية الشبكات المتصلة بالحاسوب للتفتيش: يشكل إخضاع شبكات المعلومات المتصلة بجهاز الحاسوب للتفتيش صعوبات كثيرة، نظراً لطبيعتها اللامادية والرقمية التي يمكنها توزيع البيانات والأدلة محل البحث والتحري عبر شبكات حاسوبية في أماكن مجهولة ومختلفة قد تكون بعيدة تماماً عن الموقع المادي للتفتيش، فقد يكون الموقع المادي للبيانات في إقليم الدولة أو في إقليم دولة أو عدة دول أخرى، فما مدى قابلية هذه الشبكات للتفتيش؟

أولاً: حالة اتصال جهاز المتهم بجهاز آخر داخل إقليم الدولة: يُحوّل المتهم في هذه الحالة معلومات أو بيانات الجريمة الإلكترونية من حسابه الخاص إلى حساب آخر، أو منظومة معلوماتية أخرى يملكها للغير، متواجدة في مكان آخر لتُخزن فيها¹⁶. وسمحت في هذه الحالة المادة 19 الفقرة الثانية من الاتفاقية الأوروبية لسلطات التحري بتوسيع مشروع التفتيش أو الدخول بطريقة مُماثلة لنظام معلوماتي آخر أو جزء منه كلما وُجدت أسباب يعتقد فيها أنّ البيانات المطلوبة مُخزنة في هذا النظام الآخر أو جزء منه على إقليم الدولة¹⁷. وأخذ به أيضاً المشرع البلجيكي في نص المادة 88 من قانون تحقيق الجنايات.

وسّع المشرع الجزائري أيضاً في الفقرة الثانية من المادة الخامسة من قانون التصديق والتوقيع الإلكتروني إجراءات التفتيش بوجه السرعة إلى منظومة معلوماتية أخرى، متصلة بالحاسب أو جزء منها، واشترط إعلام السلطة القضائية المختصة بذلك مسبقاً وضرورة الحصول على إذن منها.

أجاز المشرع الجزائري بتمديد التفتيش بسرعة نظراً للطبيعة المعلوماتية للبيانات الإلكترونية، التي يسهل نقلها وتحويلها أو إتلافها أو تشفيرها بسرعة، كون الجاني المعلوماتي عادةً ما يملك خبرة واحترافية في المجال. واشترط كذلك في التمديد، إعلام السلطة القضائية المختصة مسبقاً والحصول على إذن مسبق منها، حمايةً

¹⁴ - أنظر المادة 05 من القانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 47، صادر بتاريخ 25 شعبان 1430 الموافق لـ 16 أوت 2009.

¹⁵ - براهيم جبال، المرجع السابق، ص 20.

¹⁶ - جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، مصر، 2001، ص 113.

¹⁷ - للمزيد من المعلومات أنظر: حسام محمد نبيل الشنراقي، المرجع السابق، ص ص 504-505.

للحياة الخاصة للأفراد، لكننا نرى أنه يُستحسن تمديد إجراءات التفتيش في حالات الاستعجال والسماح بالولوج إلى نظام معلوماتي آخر، دون الحصول على إذن مسبق بذلك.

ثانياً: حالة اتصال جهاز المتهم بجهاز آخر خارج إقليم الدولة: قانوناً لا تستطيع السلطات المختصة بالتحقيق أن تباشر أي إجراء تفتيش يعبر حدود الدولة المنتمي إليها، لأنه يُعد انتهاكاً واعتراضاً لمبدأ سيادة دولة أخرى. ونتيجة لتمسك كل الدول بسيادتها، ظهرت لنا إشكالية مدى جواز تمديد إجراءات التفتيش إلى خارج إقليم الدولة مصدرة الإذن بالتفتيش ودخول إقليم دولة أخرى؟

اتفق الفقه الجنائي على أنه لا يجوز لسلطات التحقيق التابعة لدولة ما أن تلجأ إلى التفتيش الإلكتروني العابر للحدود إلا في حدود وإطار اتفاقيات تعاون خاصة ثنائية أو جماعية تُنظم وتجزئ هذا الامتداد، أو في حدود الإنابة القضائية¹⁸ المتبادلة، أو على الأقل أن تحصل على إذن مسبق وصريح من الدولة الأجنبية. وأجازت في هذا الشأن اتفاقية بودابست سالفة الذكر في مادتها 25 في الفقرة الثالثة منها، للدول الأعضاء في الحالات المُستعجلة، المطالبة بالمساعدة المتبادلة أو بوثائق عن طريق وسائل الاتصال العاجلة، بما في ذلك الفاكس و البريد الإلكتروني، شرط أن توفر هذه الوسائل مستويات الأمن، ويمكن بها التحقق من صحة البيانات (بما فيها استعمال التشفير للضرورة). وسمحت نفس الاتفاقية في المادة 32 منها، في حالة ما إذا كانت المعلومات أو البيانات مُتاحة للجمهور أو رضي صاحبها أو حائزها (المعلومات والبيانات)، الولوج بهدف التفتيش والضبط في أجهزة أو منظومة معلومات تابعة لدولة أخرى دون حاجة للحصول على إذن مسبق من هذه الأخيرة.

اقترحت لجنة دول أطراف الاتفاقية الأوروبية للجرائم الإلكترونية سنة 2009، إضافة حالات أخرى لتمديد التفتيش إلى خارج إقليم الدولة دون الحصول على إذن مسبق منها وهي: حالة التفتيش بحسن نية، وحالة الاستعجال القصوى أو الحالات الإستثنائية، أو طبقاً لمعيار مشروعية التفتيش أي سلطة الاستعمال.

تطرق المشرع الجزائري للتفتيش الإلكتروني عن بعد في الفقرة الثالث من المادة الخامسة من القانون 04-09 سالف الذكر، وسمح فيها للسلطات القائمة بالتفتيش أن تُوسع نطاق التفتيش عن بعد حتى لو كانت البيانات المبحوث عنها موجودة أو مُخزّنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، لكن التوسيع لا يتم إلا في نطاق المساعدات القضائية المتبادلة بين البلدين، وفي حدود الاتفاقات الدولية المبرمة في هذا الشأن، وهو ما قصده المشرع بمبدأ المعاملة بالمثل.

¹⁸ - الإنابة القضائية أو التكليف هي كل تصرف إجرائي صادر ممن له سلطة التحقيق، حيث بموجبه يفوض واحد من مأموري الضبط القضائي ليقوم خلفاً عنه. أنظر محمودي سماح، مشكلات التفتيش الجنائي عن المعلومات في الكمبيوتر والإنترنت، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، العدد 08، الجزء 1، 2017، ص 338.

المبحث الثاني

الضمانات القانونية للتفتيش في الجريمة المعلوماتية

يشترط في التفتيش ليمارس بشكل قانوني أن يضمن حقوق الأفراد وحياتهم وأن تُراعي السلطة القائمة به ضمانات قانونية أثناء ممارسته، وهذه الضمانات يوجد منها نوعان: ضمانات موضوعية (المطلب الأول) وضمانات شكلية (المطلب الثاني).

المطلب الأول: الضمانات الموضوعية الواجبة في تفتيش الجريمة المعلوماتية

حتى يكون التفتيش في الجريمة المعلوماتية صحيحا يجب أن هناك سبب للتفتيش وإلا كان التفتيش غير شرعي، كما يجب أن يرد هذا التفتيش على محل حيث لا يمكن تصور إجراء تفتيش بدونه، وأخيرا يجب أن يباشر التفتيش من طرف سلطة مختصة بالتفتيش. كلها ضمانات موضوعية عامة وأساسية يجب أن تتوفر في التفتيش حتى يكون صحيحا.

الفرع الأول: سبب التفتيش: السبب ضمان قانونية ضرورة لصحة عملية إجراء التفتيش ومشروعيته، فلا يمكن للسلطة المختصة إصدار الإذن بالتفتيش إلا إذا تحقق وقوع جريمة ما وتم اتهام شخص أو عدة أشخاص بأنهم ارتكبوها، إعمالاً لمبدأ الشرعية الجزائية التي تقضي أن لا تحريم ولا عقاب إلا ما كان وفقاً لنص قانوني. فلا يسمح القيام بإجراء التفتيش على مكونات الحاسوب والشبكات المتصل بها، إلا إذا وقعت فعلاً جريمة معلوماتية. وسبب التفتيش في هذه الجرائم لا يتحقق إلا بتوفر عناصره وهي:

أولاً: أن تحمل الجريمة الإلكترونية وصف جنائية أو جنحة: لا يمكن مباشرة عملية إجراء التفتيش إلا بعد التحقق من الوقوع الفعلي لجريمة عبر النت، ويكون منصوباً عليها في القانون، فلا يجوز إجراء التفتيش في جريمة مُحتملة الوقوع مستقبلاً. ولا يكفي وقوع جريمة إلكترونية لمشروعية التفتيش، بل يجب أن تحمل هذه الجريمة وصف جنائية أو جنحة بنظر القانون، وتُستثنى المخالفات من التفتيش لأنها ضعيفة الخطورة، لا تستحق انتهاك حرمة الحياة الخاصة للأشخاص والتعرض لسرية اتصالاتهم أو حرمة منازلهم من أجلها.

ثانياً: اتهام شخص أو أكثر بمساهمتهم في ارتكاب الجريمة: يجب أن تتوفر ضد الشخص المُراد تفتيشه أو تفتيش حاسوبه أو منزله، دلائل كافية للاعتقاد بأنه قد ساهم في ارتكاب الجريمة، سواء كان بصفته فاعل أصلي أو شريك، يستوجب اتهامه بها، ويقصد بالدلائل الكافية الإشارات التي تقوم عادة على المضمون العقلي والمنطقي لوقائع وملابسات الجريمة، وكذا خبرة وحرفية القائم بالتفتيش والتي يمكن بها تأكيد نسبة الجريمة لفاعلها سواء كان فاعلاً أصلياً أو شريكاً¹⁹. ويعتبر عدم اكتشاف قاضي التحقيق لهوية المتهم في الشكاوي ضد مجهولين، سبباً لحفظ الملف وإصدار أمر أن لا وجه للمتابعة.

¹⁹ - حسام محمد نبيل الشنراقي، المرجع السابق، ص 465.

ثالثاً: توافر إشارات ودلائل قوية توحى إلى تواجد أدلة تفيد في كشف الجريمة: قبل أن يقوم المُحقق بعملية التفتيش أو يأذن بها، يجب أن تتوفر دلائل قوية على أن المَحَل المُراد تفتيشه أو الحاسب الآلي المراد تفتيشه تتواجد فيهم وسائل أو برامج استعملت في اقتراف الجريمة أو مستمدة منها، أو فيه مستندات معلوماتية تساعد على اكتشاف الحقيقة²⁰.

الفرع الثاني: محل التفتيش: المحل في الجريمة المعلوماتية لا يكون قائماً بذاته، بل يكون دائماً مُقترناً بمكان معين وهو المكان الذي يتواجد فيه كمسكن المُتهم، أو شخص معين سواء كان مالكا أو حائزاً، كما هو الشأن في الحاسب المحمول أو الهاتف النقال، وقبل مباشرة عملية التفتيش يجب عدم إغفال طبيعة المكان المتواجدة فيه تلك الوسائل الإلكترونية محل التفتيش، وكذا الضمانات القانونية المنصوص عليها بشأنه.

تتوقف الأحكام المُتبعة في حالة تفتيش المحل اللامادي غالباً على طبيعة المكان الذي يتواجد فيه، لذلك يُشترط في المحل الذي يقع عليه التفتيش أن يكون:

أولاً: تعيين المحل تعييناً نافياً للجهالة: للحفاظ على حقوق وحريات الأفراد من الانتهاك، يُشترط أن يَعيّن المَحَل الإلكتروني المراد تفتيشه تعييناً دقيقاً نافياً للجهالة، لذلك لا يُمكن القيام بتفتيش كل أجهزة الحواسيب الموجودة في شركة أو مؤسسة ما، كما لا يحق للمفتش أن يقوم بتفتيش كل الحواسيب المحمولة أو الهواتف الخاصة بباقي أفراد عائلة المتهم.

ثانياً: أن يكون المَحَل مما يجوز تفتيشه: تم اعتماد هذا الشرط نتيجة لاستثناء القانون بعض الأشخاص وبعض الأماكن من إجراءات التفتيش، حيث لا يجوز تفتيش أعضاء السلك الدبلوماسي ومساكنهم وسياراتهم، المجالس النيابية ومكاتب المحامين لتمتعهم بالحصانة، إلا من قبل القاضي المختص بكل فئة ووفق إجراءات استثنائية نصت عليها القوانين الأساسية لكل من هذه الفئات. وبذلك كل تفتيش يجري على الوسائل الإلكترونية الموجودة بحيازة هذه الفئة المذكورة من الأشخاص، في مساكنهم أو على متن وسائل تنقلهم، بشكل يخالف هذه الأحكام الاستثنائية يعد مخالفاً لنص القانون ومصيره البطلان²¹.

الفرع الثالث: السلطة المختصة بالتفتيش: الجهات المختصة بالتفتيش في عالم الجريمة الافتراضية يمكن أن تكون هي نفسها المختصة بالتفتيش في الجريمة التقليدية مثل جهة التحقيق (أولاً) أو رجال الضبط القضائي (ثانياً)، كما يمكن أن تكون جهة مستحدثة ومُتخصصة في مجال المعلومات كمركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية (ثالثاً).

²⁰ - حسام محمد نبيل الشنراقي، نفس المرجع، ص 465.

²¹ - نص على هذا الاستثناء في المادة 22 من القانون رقم 07-13 المؤرخ في 24 ذي الحجة عام 1434 الموافق لـ 29 أكتوبر 2003، يتضمن تنظيم مهنة المحاماة. تفاصيل أكثر راجع: براهيم جمال، المرجع السابق، ص 36.



أولاً: التفتيش من طرف جهة التحقيق: وفقاً للقواعد الإجرائية العامة في نطاق وحدود قواعد الاختصاص المكاني، الذي يُحدّد إما بمكان وقوع الجريمة، أو مكان إقامة المتهم أو مكان القبض عليه، إضافة إلى ضرورة احترام قواعد الاختصاص النوعي، فالأصل أنّ عملية التفتيش تتم وتباشر من جهة التحقيق أو بناءً على إذن منها، والمُحقق هو الجهة المختصة بمباشرة عمليات التفتيش بصفة أصلية، مع حقه في تفويض أو نذب أحد رجال الضبط القضائي في الحالات الاستثنائية ومتى اقتضت الضرورة ذلك. والأمر لا يختلف في الجرائم الإلكترونية عن ذلك، كون إجراء التفتيش في العالم الافتراضي يخضع لنفس الأحكام والقيود العامة التي تُطبق على الجريمة التقليدية²².

ثانياً: التفتيش من طرف رجال الضبط القضائي: أجازت القوانين الإجرائية العامة بجواز تمديد إجراء التفتيش لمرحلة الاستدلال في بعض الحالات الاستثنائية المعينة، ويقوم بالتفتيش رجال الضبط القضائي سواء في العالم المادي أو العالم الافتراضي، ويمكن إجمالها فيما يلي:

1- النذب بالتفتيش في العالم الافتراضي: تسهياً لعمليات التحقيق والتفتيش، وسعياً منها لعدم ضياع الأدلة وضمان شرعيتها، سمحت القوانين الإجرائية لجهة التحقيق أن تنذب رجال الضبط القضائي للقيام بعمليات التفتيش بدلاً عنها، متى توفر شرط صدور الإذن المسبق بالتفتيش وكذا توفر شرط تحرير محضر التفتيش.

2- التفتيش في حالة القبض على الأشخاص: يقوم رجال الضبط القضائي دائماً بتفتيش المتهم المقبوض عليه (متى توفرت أدلة كافية على ارتكابه الجريمة)، وهذا ينطبق على كل ما هو بحوزة المتهم من أدوات ودلائل مادية تقليدية أو حديثة، كالأجهزة المحمولة والهواتف النقالة وغيرها من أجهزة التخزين الإلكترونية²³.

ثالثاً: مركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية: هو مركز تابع لمديرية الأمن للدرك الوطني، تأسس بموجب المرسوم الرئاسي رقم 15-261²⁴، الذي حدّد في المادة الأولى منه تشكيلة وتنظيم سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. وتمارس هذه الهيئة العديد من المهام والاختصاصات من أجل الوقاية والتصدي للجريمة الإلكترونية، والتي ورد النص عليها في المادة 14 من القانون رقم 04-09 السالف الذكر، ومن هذه المهام: ضمان المراقبة الدائمة والمتواصلة لشبكات الإنترنت كما

²² - لدغش رحيمة ، المرجع السابق، ص 135.

²³ - مرجع نفسه، ص 136.

²⁴ - المرسوم الرئاسي رقم 15-261 مؤرخ في 24 ذي الحجة عام 1436 هـ الموافق لـ 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج عدد 53 لسنة 2015.



يتولى المركز القيام بمراقبة الاتصالات الإلكترونية في حدود ونطاق ما يسمح به القانون لمصلحة وحدات الدرك الوطني، كما تُشارك إضافةً إلى هذه المهام في عمليات البحث والتحري عن الجرائم الإلكترونية²⁵.

المطلب الثاني: الضمانات الشكلية للتفتيش في الجريمة المعلوماتية

يستوجب على السلطة المختصة بالتفتيش، إضافةً إلى الضوابط الموضوعية التي تناولناها سابقاً لتفتيش الحاسوب، أن تراعي أيضاً القيود الشكلية عند مباشرتها لعملية التفتيش، والتي يُمكن أن تتحول في بعض الحالات خاصة الاستعجالية منها، إلى عقبات وعراقيل قد تحول دون تحقق الوصول إلى القصد من إجراء التفتيش، نظراً لخصوصية وطبيعة الجريمة المعلوماتية دون أن ننسى الخبرة والاحترافية العالية عند الجاني في هذا المجال، وتتمثل هذه الضوابط أو الضمانات فيما يلي:

الفرع الأول: حضور بعض الأشخاص أثناء التفتيش الإلكتروني: تشترط القوانين الإجرائية عند القيام بالتفتيش في الجرائم التقليدية إلزامية حضور بعض الأشخاص بعينهم كالمتهم أو من يقوم مقامه، حرصاً منها على تضيق نطاق الاعتداء على حرمة وخصوصيات الأفراد ومساكنهم المضمونة قانوناً، وحضور هؤلاء الأشخاص من القواعد الأساسية التي يترتب عن مخالفتها بطلان التفتيش، إعمالاً لمبدأ الحضور عند تفتيش المنزل. أما في حالة تفتيش الأشخاص، فقد ذهبت التشريعات إلى عدم اشتراط وجود أشخاص معينين عند إجرائه²⁶، كونه يمارس على شخص المتهم بذاته.

كرّس التشريع الجزائري هو الآخر مبدأ الحضور في المادة الخامسة من قانون الوقاية من الجرائم التكنولوجية والاتصال والإعلام ومكافحتها، والتي تحيل في هذا الشأن إلى الأحكام العامة في قانون الإجراءات الجزائية المادة 45 منه²⁷، واشترط لتفتيش المساكن حضور صاحب المنزل المشتبه به، وإذا تعذر حضوره أثناء القيام بعملية التفتيش، فإن القانون يلزم ضابط الشرطة القضائية وكلّفه بأن يعين ممثلاً له، وإذا امتنع عن ذلك أو كان هارباً، فيجب أن يستدعي ضابط الشرطة القضائية شاهدين على أن يكونا من غير الموظفين الخاضعين لسلطته، للحضور أثناء مزاولة عملية التفتيش، وإذا جرى التفتيش في منزل شخص آخر بحوزته أوراقاً أو أشياء لها علاقة بالجريمة، فيلزم حضوره الشخصي وإلا اتبعت في حقه نفس الإجراءات السابقة.

خلال عملية التفتيش في الجرائم الإلكترونية لا تطبق الأحكام العامة السابقة، ولا يتم مراعاتها نظراً لخصوصية وطبيعة جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، وما يتطلبه الأمر من السرعة والسرية أثناء عملية جمع الدليل التقني المشار إليه في الفقرة الأخيرة من المادة 45، واستثنت هذه الجرائم من تطبيق

²⁵ - فلاح عبد القادر، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث في الدراسات القانونية والسياسية، جامعة الجبالي بونعامة، خميس مليانة، المجلد 04، العدد 02، لسنة 2020، ص ص 1696-1697.

²⁶ - مخلوفي علمي وبومحراث ليندة، المرجع السابق، ص 397.

²⁷ - المادة 45 من الأمر رقم 66-155، سالف الذكر.



أحكام المادة نفسها، وأجازت للضبطية القضائية بإجراء التفتيش في هذه الجرائم دون التقيد بشرط حضور المتهم أو من يُؤوب عنه أو حتى ضرورة حضور الشهود²⁸.

الفرع الثاني: زمان التفتيش: لم تتفق التشريعات الإجرائية للدول في تنظيمها للوقت الذي يسمح فيه مباشرة التفتيش، فمنها من ضيقته وحددته بشكل عام على أن يتم التفتيش نهاراً فقط كقانون الإجراءات الجنائية القطري، وأخرى حددت وقت التفتيش بشيء من التفصيل، وحددت الساعة التي يمكن فيها البدء بالتفتيش، والساعة التي يجب التوقف عندها من ساعات النهار. ومنها كذلك من لم يقيّد القيام بهذا الإجراء بوقت معين، وترك الأمر لتقدير القائم بعملية التفتيش لاختيار الوقت الملائم من الليل أو النهار لتنفيذه، شرط أن يحترم المدة المحددة في الإذن بالتفتيش كقانون الإجراءات الجنائية المصري والعراقي والقانون الأردني أيضاً.

أما المشرع الجزائري فقد وضع حدوداً وقيوداً زمنية على تفتيش المنازل وما يدخل في حكمها، ولم يسمح به بمقتضى المادة 47 من الأمر رقم 66-155، إلا في الوقت المحصور بين الساعة الخامسة صباحاً و الساعة الثامنة مساءً. وفي الوقت نفسه أقر استثناءات سمح فيها الخروج عن هذا الميقات، ليسمح بإجراء عملية التفتيش في أي ساعة من ساعات النهار أو الليل، عندما يتعلق الأمر بالتحقيق في الجرائم المنصوص عليها في المواد 342 إلى 348 من قانون العقوبات والمركبة في أماكن معينة، وفي حالة الرضا الصريح من صاحب المسكن. واشتمل هذا الاستثناء الجرائم الإلكترونية، بحيث استغنى المشرع الجزائري نهائياً عن شرط الميقات الزمني وسمح لرجال الضبطية القضائية بإجراء التفتيش في مثل هذه الجرائم في أي ساعة من ساعات الليل أو النهار، كما جاء في الفقرة الأخيرة من نص المادة 47 قانون الإجراءات الجزائية الجزائري.

الفرع الثالث: ضرورة تحرير محضر التفتيش: باعتبار التفتيش إجراء تحقيق، فإنه يجب تحرير محضر خاص به، تُقيد فيه كل الخطوات والإجراءات التي تم اتخاذها أثناء القيام وممارسة عملية التفتيش، وما نتج عنها من أدلة لتكون حجة على الجميع. فلم يستوجب القانون شكلاً معيناً أو شروطاً خاصة في محضر التفتيش، بل يكفي أن يتوفر فيه ما تفرضه القواعد العامة في المحاضر عموماً، كالكتابة باللغة الرسمية للدولة، تاريخ تحريره وتوقيع محرره، وأن يتضمن كافة إجراءات التفتيش التي اتخذت بشأن الوقائع التي يشبته.

يتعين على المحقق القائم بالتحقيق أن يستعين بكاتب، ويصطحبه معه لتحرير المحضر، حيث يسجل في المحضر كل ما اتخذ من إجراءات والتأشير عليه، وهو ما نصت عليه المادة 68 الفقرة الثانية من قانون الإجراءات الجزائية الجزائري. ولا يختلف محضر التفتيش في مجال الجرائم الإلكترونية عن محضر التفتيش في الجرائم التقليدية، سوى أنه بالإضافة إلى الشكليات السابقة، لابد من إحاطة القائم بالتفتيش في الجرائم الإلكترونية بالتقنية المعلوماتية الرقمية، أو استعانت به بالخبرة الفنية والاختصاص في هذا المجال، ليساعد في صياغة وتحرير محضر يشمل كل النقاط الفنية والتقنية للتفتيش²⁹.

²⁸ - للمزيد أنظر: براهيمي جمال، المرجع السابق، ص 44.

²⁹ - براهيمي جمال، المرجع السابق، ص 45.

حرصت الدول على تضمين تشريعاتها الإجرائية نُصوص تمنع فيها الإطلاع خلال عملية التفتيش على الأشياء والأوراق والوثائق المخبوءة، والتي تتضمن وتمس الأسرار الخاصة والشخصية للعائلة، وتلزم على القائم بعملية التفتيش اتخاذ الاحتياطات الضرورية لتفادي إفشاء وانكشاف مثل هذه الأسرار، ومن بين هذه التشريعات نجد قانون الإجراءات الجنائية المصري في مادته 52، ونص المادة 140 من قانون الإجراءات الجنائية اليمني، وتناول المشرع الجزائري هو الآخر هذه الضمانة في المادة 84 من الأمر 66-155.

خاتمة:

التفتيش في الجرائم المعلوماتية إجراء من أعمال التحقيق، وهو إشكالية أفرزها التطور الحديث في الجريمة، التي أصبحت عابرة لحدود الدولة وترتكب في عالم افتراضي غير ملموس. ونظراً للطبيعة الخاصة للجريمة الإلكترونية، وسهولة إتلاف أو إخفاء الدليل الرقمي، وخبرة واحترافية المجرم المعلوماتي، كل هذا ساهم في الإفلات من العقاب لعدم توفر بيئة تفتيش ملائمة وعدم كفاءة القائمين بالتفتيش، رغم سعي الدول إلى تدريب أشخاص ذوي كفاءة وتمديد إجراء التفتيش لأي وقت من الليل أو النهار.

كما أن محل التفتيش الإلكتروني يتمتع بالحماية القانونية كونه يمس مباشرة بحرمة الحياة الخاصة للأشخاص، لذلك نجد أن مختلف التشريعات وضعت ضوابط قانونية شكلية وموضوعية يتعين على القائمين بالتفتيش مراعاتها وإلا كان التفتيش باطلاً. كما استتبت القوانين بعض الأشخاص من التفتيش لتمتعهم بالحصانة، وبالتالي لا يمكن تفتيشهم أو تفتيش الحواسيب الموجودة في مكاتبهم أو منازلهم أو على متن سياراتهم إلا وفق إجراءات استثنائية تخص كل فئة من هذه الأشخاص، وكل تفتيش مخلف لهذه الإجراءات الإستثنائية يكون مصيره البطلان.

بادرت الدول إلى إصدار قوانين جديدة والتعديل من قوانينها الإجرائية التقليدية وإبرام اتفاقيات جماعية. والمشرع الجزائري وعلى غرار التشريعات الدولية الأخرى قام بوضع قانون خاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وأنشأ بموجبه هيئات خاصة بالتحقيق والتفتيش في هذا النوع من الجرائم. كما عدل من قانون الإجراءات الجزائية ونص على الجرائم الإلكترونية وطبيعتها الخاصة.

رغم كل هذه الجهود تبقى الجريمة المعلوماتية والمجرم المعلوماتي في تقدم مستمر مقارنة بهذه القوانين الإجرائية، لذا خلصنا إلى بعض الاقتراحات والتي هي:

- 1- سن قواعد إجرائية خاصة بالجرائم الإلكترونية تتلاءم والطبيعة الخاصة لهذه الجرائم وإخضاع كل مخرجات الحاسوب للتفتيش.
- 2- عقد اتفاقيات دولية جماعية لمحاربة الجرائم الإلكترونية وموضوع الإنابة القضائية.
- 3- تكوين وتدريب قضاة وضبطية قضائية مختصين وذوو كفاءة عالية للبحث والتفتيش في الجرائم الإلكترونية.



قائمة المراجع والمصادر

أولاً: الكتب:

- 1- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، مصر، 2001.
- 2- حسام محمد نبيل الشنراقي، الجرائم المعلوماتية: دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، مصر، 2013.
- 3- سامي جلال فقي، التفتيش في الجرائم الإلكترونية دراسة تحليلية، دار الكتب القانونية، القاهرة، 2012.

ثانياً: الرسائل والمذكرات الجامعية

- 1- أحمد محمود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 04/09، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 2013.
- 2- براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص قانون، جامعة تيزي وزو، 2018.
- 3- غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلومات (الحاسب والإنترنت)، أطروحة أعدت لنيل درجة الدكتوراه في القانون، كلية الحقوق، الجامعة الإسلامية، لبنان، 2004.

ثالثاً: المقالات العلمية

- 1- عربوز فاطمة الزهراء، التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية، مجلة جيل الأبحاث القانونية المعمقة كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس، مجلد 04، العدد 34، 2019، ص ص 103-117.
- 2- فلاح عبد القادر، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث في الدراسات القانونية والسياسية، جامعة الجيلالي بونعامة، خميس مليانة، المجلد 04، العدد 02، 2020، ص ص 1689-1708.
- 3- محمودي سماح، مشكلات التفتيش الجنائي عن المعلومات في الكمبيوتر والأنترنت، مجلة الحقوق والعلوم السياسية جامعة خنشلة، الجزء 1، العدد 08، 2017، ص ص 326-339.
- 4- مخلوفي علمي وبومحراث ليندة، ضوابط التفتيش في الجرائم الإلكترونية، مجلة المعيار، مجلد 28، عدد 1، 2024، ص ص 389-402.
- 5- هميسي رضا، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، مجلد 03، عدد 02، جوان 2012، ص ص 157-182.

رابعاً: المداخلات:

- علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العالمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، نظمتها أكاديمية شرطة دبي، مركز البحوث

والدراسات، دبي، الإمارات العربية المتحدة، في الفترة الممتدة بين 26-28 نيسان 2003. متوفر على الموقع:

<http://www.mohamah.net>

خامسا: النصوص القانونية

أ- الدستور:

- دستور الجمهورية الجزائرية الديمقراطية الشعبية، لسنة 2020 الصادر في الجريدة الرسمية للجمهورية الجزائرية /العدد 82 الصادر في 15 جمادى الأولى 1442 الموافق لـ 30 ديسمبر 2020.

ب- النصوص التشريعية:

1. أمر رقم 66-155 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966 ، يتضمن قانون الإجراءات الجزائئية الجزائري، المعدل والمتمم.
2. قانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والاتصال ومكافحتها، ج ر عدد 47 ، صادر بتاريخ 25 شعبان 1430 الموافق لـ 16 أوت، 2009.
3. قانون رقم 13-07 مؤرخ في 24 ذي الحجة عام 1434 الموافق لـ 29 أكتوبر 2003، يتضمن تنظيم مهنة المحاماة

ت-النص التنظيمي:

- 1-مرسوم رئاسي رقم 15-261 مؤرخ في 24 ذي الحجة عام 1436 هـ الموافق لـ 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج عدد 53 لسنة 2015.