التفتيش الجزائي في البيئة الافتراضية

Penal inspection in the virtual environment

طالبة الدكتوراه رجاء أومدور[1]، د/ كمال فرشة [2]

[1] جامعة محمد البشير الابراهيمي، برج بوعريريج، كلية الحقوق و العلوم السياسية، مخبر العدالة السيبرانية، radja.oumeddour@univ-bba.dz

[2] جامعة محمد البشير الابراهيمي برج بوعريريج الجزائر، كلية الحقوق و العلوم السياسية، مخبر العدالة السيبرانية، Kamel363@msn.com

تاريخ الإرسال: 14 / 09 /2019 تاريخ القبول: 09 /01/ 2019 تاريخ النشر 30 / 05 /2020

ملخص:

تهدف هذه الدراسة إلى تسليط الضوء على اشكالية التفتيش عن الجرائم المعلوماتية ومقتضيات الوصول الى الحقيقة، حيث أخضع المشرع الجزائري - في سبيل تعزيز مسار التحقيق الجزائي - هذا الاجراء لضوابط تتماشى وخصوصية البيئة الافتراضية، وطبيعة هذه الجرائم التقنية؛ غير أن التفتيش كإجراء قضائي، قد يمس بالحق في الخصوصية، والمعطيات ذات الطابع الشخصي، وقد يشكل مساسا بسيادة الدول، وهو ما فرض تقييد سلطات التفتيش المختصة بضوابط إجرائية، وإخضاعها لأصول التعاون الدولي، وموائمتها مع مبادئ وأعراف العلاقات الدولية، ومقتضيات السيادة الوطنية.

الكلمات المفتاحية: التفتيش، جرائم معلوماتية، الحق في الخصوصية، سيادة الدول.

Abstract :

The aim of this topic is to highlight the problem of inspecting on cybercrimes and requirement to reach the truth. In order to strengthen the course of criminal investigation, the Algerian legislator has submitted this measure to a set of controls corresponding to the specificity of the virtual environment and the nature of these technical

crimes. However, inspection as a judicial process may encroach on the right to privacy and personal data, and may infringe upon the sovereignty of States; this imposed the restriction of competent inspection authorities with procedural controls, their subjection to the principles of international cooperation and their conformity with the norms of international relations and the requirements of national sovereignty.

Keywords: *inspection, cybercrimes, right to privacy, sovereignty of states*

1- **المؤلف المرسل:** رجاء أومدور، **الإيميل:** radja.oumeddour@univ-bba.dz

مقدمة:

مسايرة للتطورات التكنولوجية الحديثة أضاف المشرع الجزائري ضمن قانون العقوبات سنة 2004 قسما جديدا تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، تلتها تعديلات سنة 2006 على كل من قانون العقوبات وقانون الاجراءات الجزائية، وسدا منه للفراغات القانونية وضع مجموعة ترتيبات من بينها اجراء التفتيش في القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال ومكافحتها، وفي سنة 2018 تم اصدار القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

وفي هذا الاطار نتطرق لموضوع التفتيش عن الجرائم المعلوماتية بإبراز الضوابط القانونية اللازمة لصحته والتجاوزات التي تنجم عن انتهاك الحق في الخصوصية عند معالجة المعطيات ذات الطابع الشخصي، أو في اطار التعاون الدولي اذا كان التفتيش عابرا للحدود.

ولعل الهدف الرئيسي من هذا الموضوع هو إثراء الجانب الاجرائي للقانون الجزائي المعلوماتي، من خلال تحديد ضوابط التفتيش في البيئة الافتراضية وإبراز أهم التحديات التي تواجهه، و المشكلات العملية التي قد يثيرها هذا الإجراء في العالم الافتراضي.

ومن هذا المنطلق نطرح الاشكالية الآتية: كيف يمكن اجراء التفتيش عن الجرائم المعلوماتية دون الاخلال بالضمانات اللازمة لحماية الحق في الخصوصية واحترام سيادة الدول؟

وإجابة على الاشكالية المطروحة: اعتمدنا المنهج التحليلي للسيرورة الاجرائية المعتمدة على القوانين سالفة الذكر، وقمنا بتقسيم خطة العمل الى مبحثين: تضمن المبحث الأول: مفهوم التفتيش عن الجرائم المعلوماتية أما المبحث الثاني تناول: تحديات التفتيش في البيئة الافتراضية.

1.مفهوم التفتيش عن الجرائم المعلوماتية

التفتيش وسيلة للإثبات المادي، تستهدف الحصول على الأدلة المادية المتعلقة بالجريمة، أو تفيد في كشف الحقيقة، وهو ما يتعارض مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي، وشبكة الانترنت؛ فهي بيانات وبرامج الكترونية ليس لها مظهر مادي ملموس في العالم الخارجي.[1] وفي سبيل الحد من التجاوزات التي تطال هذا الاجراء، وتمس بالحق في الخصوصية لدى الأشخاص، والمجتمع أوالدول، وجب احترام مجموعة من الضوابط توضح مسار التحقيق في الجرائم المعلوماتية.

1.1 ضبط المصطلحات

1.1.1 الجرائم المعلوماتية

اعتمد الباحثين و الفقهاء في تعريف هذه الجرائم المعاصرة على عدة جوانب من بينها:

الجانب التقني: " هي نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو كهدف لتنفيذ النشاط الاجرامي المقصود ".[2]
الجانب القانوني: " هي جرائم مستمرة، تتسم بالسرعة والتطور في وسائل ارتكابها، لها عدة صور وأشكال، وهي أقل عنفا ظاهريا في التنفيذ من الجرائم التقليدية، وهي جرائم واسعة الانتشار، عابرة للحدود و يصعب اثباتها ".[3]
وقد تباينت التعاريف القانونية بين منظور القانون الجنائي أو الاتصال بالحياة الخاصة أو حقوق الملكية الفكرية، إضافة إلى معايير أخرى أبرزها:
معيار موضوع الجريمة، وأنماط السلوك محل التجريم: حيث عرفت الجريمة المعلوماتية أنها: "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات. أو هي أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات ".[4]
معيار وسيلة ارتكاب الجريمة بأنها: الفعل غير المشروع المرتكب بواسطة الكمبيوتر أو الانترنت أو أية وسيلة الكترونية.[5]
وقد اعتمد الفقيه الألماني Ulrich Sieher على تعريف خبراء منظمة التعاون الاقتصادي والتنمية OECD، والذي يعتمد على معيارين: أولهما وصف السلوك و ثانيهما اتصال السلوك بالمعالجة الالكترونية للبيانات أو نقلها، حيث عرف الخبراء الجريمة المعلوماتية بأنها: " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الالكترونية للبيانات أو نقلها".[6]
وهناك من يرى أن مصطلح الجرائم المعلوماتية[7] هو المصطلح الأدق وهو ما نرجحه بدليل أنه مصطلح واسع يشمل الحاسب و سائر المبتكرات والتقنيات الراهنة والمستقبلية المستحدثة في التفاعل مع المعلومات، ولأنه يمكن تصور هذه الجرائم من زاويتين؛ الأولى: أن الجاني يستخدم المعلوماتية لتنفيذ جرائمه، سواء المتعلقة بالاعتداء على الأشخاص أو الأموال؛ أما الثانية: فالجاني يجعل المال المعلوماتي محلا وموضوعا لجرائمه.[8]

بالرغم من أن المشرع الجزائري لم يعرف هذه الجريمة تاركا الأمر للفقه، الا أن بعض التشريعات و منها القانون الأمريكي عرف الجرائم المعلوماتية بموجب القانون رقم 1213 لسنة 1982 الخاص بمواجهة جرائم الكمبيوتر على أنها: " الاستخدام غير المصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات، أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات، وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية الى جناية من الدرجة الثالثة ".[9]

مما سبق يمكن تعريف الجرائم المعلوماتية على أنها: نمط من الجرائم المعقدة التي تتعلق بالاستخدام غير المشروع وغير المصرح به للبيانات، والمعلومات، أو نقلها، أو تخزينها، أواستعمالها عبر الوسائط الالكترونية، بما يشكل اعتداء على الأشخاص والأموال وحتى أمن الدول واستقرارها.

2.1.1: التفتيش

تتعدد التعاريف الفقهية حول مفهوم التفتيش وتنصب في مجملها على أن:

التفتيش هو: " إجراء من اجراءات التحقيق، يقوم به شخص مؤهل قانونا، في محل يتمتع بالحرمة، بقصد الوصول الى أدلة مادية لجناية أو جنحة، تحقق وقوعها فعلا، لإثبات ارتكابها أو نسبتها الى المتهم".[10]

وقد اختلف الفقه حول مصطلح التفتيش في البيئة الافتراضية، حيث اعتبره البعض ينصب على أنظمة برامج، مواقع وصفحات الكترونية، وبالتالي المصطلح الأدق هو الولوج أو النفاذ، في حين ذهب اتجاه آخر وهو ما نؤيده بالابقاء على مصطلح التفتيش كونه عام يشمل التفتيش التقليدي والتفتيش الالكتروني.[11]

ومن هنا يمكن تعريف التفتيش عن الجرائم المعلوماتية بأنه اجراء من اجراءات التحقيق، يهدف إلى الوصول إلى الادلة المنبثقة من جناية أو جنحة تحقق

وقوعها فعلا داخل نظام المعالجة الآلية للمعطيات لاثبات ارتكابها ونسبتها لمتهم معين وينبغي التعامل مع الأدلة المعلوماتية بحيطة وحذر لتفادي تلفها وضياعها.

2.1 ضوابط التفتيش عن الجرائم المعلوماتية

1.2.1 الضوابط الموضوعية

أحاط المشرع اجراء التفتيش بمجموعة من الضوابط الموضوعية، التي لابد من التقيد بها عند اجراء التفتيش، يرتب تجاوزها بطلان هذا الاجراء، وتتمثل هذه الضوابط أساسا في:

- **وقوع جريمة معلوماتية:**

حيث يشترط أن تكون الجريمة واقعة فعلا، ولا يمكن إجراء التفتيش إذا كانت الجريمة محتملة الوقوع مستقبلا، حتى ولو كانت مؤشرات على احتمال وقوعها، وذلك تأسيسا على طبيعة التفتيش في حد ذاته، كونه عمل من أعمال التحقيق الابتدائي،[12] وباعتبار التفتيش من الاجراءات الخطيرة التي تمس حرية الأشخاص وحرمة حياتهم، فلا يجوز المساس بها ما لم ترتكب الجريمة بالفعل، ولا يكف مجرد احتمال ارتكابها. [13]

- **نسب الجريمة الى مرتكبها:**

ينبغي أن تتوفر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية، سواء بصفته فاعلا أصليا أو شريك، حيث أن الدلائل والامارات لابد أن تكون جدية سابقة على اصدار أمر التفتيش، تؤيد نسبة الجريمة الى شخص معين، بوصفه فاعلا أو شريكا.[14] وتبقى الأدلة الالكترونية موضع اشكال لدى رجال القانون، والقضاء نتيجة امكانية تغيير الدليل والتلاعب به بسهولة، مما يستدعي ابرام اتفاقية على مستوى الأمم المتحدة بشأن قبول الدليل الالكتروني في الاثبات الجنائي، والذي يبقى توجه ذو طابع دولي يأخذ بعين الاعتبار التغيرات المستمرة في تكنولوجيا المعلومات.[15]

- **محل التفتيش:**

يقصد بمحل التفتيش مستودع سر الانسان، الذي قد يكون له حرمة خاصة كالمسكن، أو قد يكون الشخص أو رسائله، هذا بالنسبة للجرائم التقليدية، أما الجرائم المعلوماتية، فالمحل هنا هو الحاسوب بمكوناته وشبكاته، وهذا المحل قد يكون موجود في مكان معين منحه القانون حرمة خاصة، أو بحوزة شخص كالحاسوب المحمول.[16] وفي هذا المجال نتعرض لمجموعة من النقاط تخص محل التفتيش انطلاقا من النصوص القانونية:

- **امتداد التفتيش لجميع المكونات المادية Hardware والمعنوية Software للنظم المعلوماتية:** جعل المشرع الجزائري اجراء التفتيش يمتد ليشمل جميع المكونات سواء مادية أو معنوية، وهو يمتد للبيانات و المعلومات والبرمجيات المخزنة في الحاسب الآلي، فضلا عن الاقراص و الأشرطة وغيره من وسائل الاتصال الحديثة كالهاتف الخلوي، الهاتف الذكي، شرائح الهاتف بطاقات الذاكرة، آلات التصوير الرقمية، و يمتد التفتيش حتى لبطاقات فك التشفير الخاصة بالتلفزيون الرقمي.[17]
- **الحجز الجزئي في المنظومة المعلوماتية:**

أجاز المشرع الجزائري الحجز الجزئي في المنظومة المعلوماتية، بحيث تكتفي السلطة التي تباشر التفتيش، بنسخ المعطيات التي تفيد في كشف الجريمة أو مرتكبيها، على دعامة تخزين الكترونية قابلة للحجز، و الوضع في احراز وفقا لما هو مقرر في قانون الاجراءات الجزائية. [18] لكن ذلك يوجب المحافظة على هذه المعطيات من أي تلف أو ضياع، واستغلالها من قبل السلطات المختصة يكون بالقدر اللازم للتحقيق دون المساس بمحتواها الأساسي، أما في حالة استحالة حجز هذه المعطيات لأسباب تقنية، فلا بد من استعمال التقنيات المناسبة للحفاظ على هذه المعطيات. [19]

- **التفتيش عن بعد:**

عالج المشرع الجزائري بموجب المادة الخامسة من القانون 09 – 04 الدخول بغرض التفتيش، ولو عن بعد لكل المنظومة المعلوماتية، أو إلى جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، وإلى منظومة تخزين المعلومات حيث أجاز للسلطات القضائية و ضباط الشرطة القضائية ذلك في حدود اختصاصهم. و أضاف المشرع عنصر الاعتقاد، حيث أنه بمجرد الاعتقاد بوجود المعطيات يمكن الدخول لها انطلاقا من المنظومة الأولى، و تكون هذه المعطيات مخزنة في أي نظام منفصل أو مجموعة من الأنظمة المتصلة أو المرتبطة ببعضها، و التي يقوم واحد منها أو اكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين. هنا يمكن تمديد التفتيش بسرعة الى هذه المنظومة أو جزء منها بعد اعلام السلطة المختصة مسبقا.

وما نلاحظه أن التمديد يخضع لشروط محددة و هي - توفر الاعتقاد - السرعة في تمديد التفتيش- الدخول بغرض التفتيش الى المنظومة كاملة أو جزء منها - وجوب اعلام السلطات المختصة قبل القيام بإجراء التفتيش.

- **الاستعانة بذوي الخبرة في المجال المعلوماتي:**

أجاز القانون الاستعانة بأي شخص له كفاءة و دراية بعمل المنظومة المعلوماتية محل البحث، أو بغرض القيام بتدابير معينة لحماية المعطيات المعلوماتية، حيث يمكن للسلطات المكلفة بالتفتيش أن تستعين به بغرض المساعدة أو بغرض التزود بمعلومات مفيدة في تعميق التحقيق.[20]

- **وجود اذن بالتفتيش**

بالرجوع لقانون الاجراءات الجزائية نجد أن المادة الرابعة والأربعون منه، أوردت في فقرتها الثانية، أنه في حالة التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، لا يمكن القيام بالتفتيش الا بعد استصدار اذن بالتفتيش. ويشترط في هذا الأخير: -أن يكون مكتوبا- صادرا عن وكيل الجمهورية أو قاضي التحقيق- استظهاره قبل القيام بالتفتيش- ضرورة أن

يتضمن الاذن وصف الجرم موضوع البحث عن الدليل و عنوان الأماكن التي ستتم زيارتها و تفتيشها واجراء الحجز فيها. - وجوب انجاز عملية التفتيش تحت اشراف القاضي الذي اذن بها. و تجدر الاشارة أنه في حالة اكتشاف جرائم أخرى غير المذكورة في الاذن لا يكون سببا لبطلان الاجراءات العارضة.[21]

2.2.1 الضوابط الشكلية

بالإضافة الى الضوابط الموضوعية سالفة الذكر، فانه زيادة على ذلك اشترط القانون مجموعة ضوابط شكلية لصحة اجراء التفتيش وتتمثل أساسا في ما يلي:

- **حضور صاحب المسكن أثناء التفتيش:**

أوردت المادة الخامسة والأربعون من قانون الاجراءات الجزائية استثناء فيما يخص اجراء تفتيش مسكن المشتبه فيه أو مسكن شخص يشتبه بأنه يحوز ماله علاقة بالجريمة، حيث اذا تعلق الأمر بالجرائم المحددة حصرا و من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فتطبق أحكام هذه المادة فقط فيما تعلق بوجوب كتمان السر المهني و جرد الأشياء و حجز المستندات.[22] أما غير ذلك فضباط الشرطة القضائية هنا غير مقيدين بشرط حضور صاحب المسكن أو من ينوبه أو شاهدين، اذا تم التفتيش بمسكن المشتبه فيه، أو مسكن شخص يحوز ما له علاقة بالجريمة. وباستقراء المادة السابعة والأربعون مكرر نجد انه في حالة التحقيق في الجرائم المعلوماتية اذا كان الشخص المراد تفتيش مسكنه موقوفا للنظر أو محبوس في مكان آخر، و يقتضي عدم نقله الى ذلك المكان لأسباب محددة. في هذه الحالة يمكن لضابط الشرطة القضائية أن يقوم بإجراء التفتيش بعد موافقة مسبقة من وكيل الجمهورية أو قاضي التحقيق بحضور اما شاهدين مسخرين وفقا للأحكام المقررة قانونا، أو بحضور ممثل يعينه صاحب المسكن محل التفتيش. وتتمثل الأسباب التي من شأنها أن تحول دون امكانية نقل الشخص الموقوف للنظر أو المحبوس في مكان آخر الى ذات

المكان محل التفتيش في: وجود مخاطر جسيمة قد تمس النظام العام، أو احتمالية الفرار، أو امكانية اختفاء الأدلة. [23]

- **ميقات التفتيش:**

كاستثناء عن القواعد العامة لتفتيش المساكن والمحددة بأوقات معينة للتفتيش بين الساعة الخامسة صباحا والثامنة ليلا. فإنه من بين الاستثناءات الواردة على ميقات التفتيش: إذا تعلق الأمر بالجرائم المحددة حصرا ومن بينها الجرائم المعلوماتية فإنه في هذه الحالة يجوز إجراء التفتيش في أي وقت من الليل والنهار، حيث منح المشرع الجزائري من خلال المادة السابعة والأربعون من قانون الاجراءات الجزائية، في الفقرة الثالثة والرابعة، صلاحية اجراء التفتيش من قبل السلطات المختصة في أي ساعة من الليل والنهار.[24]

- **تحرير محضر التفتيش:**

يلزم أن يكون القائم بالتفتيش مختصا بإجرائه نوعيا ومكانيا [25]، وبعد انتهائه من اجراء التفتيش يجب أن يحرر محضرا بذلك، يدون فيه تفاصيل عملية التفتيش سواء كان التفتيش قد نجم عنه الحصول على الدليل الذي تم البحث عنه أو لم يتم الحصول عليه.[26] وقد اشترط المشرع الجزائري بموجب المادة التاسعة والسبعون أن يستعين قاضي التحقيق دائما بكاتب التحقيق عند قيامه بعملية التفتيش، و يشترط تحرير محضر بما يقوم به من اجراءات. غير أنه لا يشترط لصحة التفتيش أن يفرغ المحضر في شكل معين، حيث تطبق القواعد العامة في المحاضر بشكل عام، بأن يتضمن كافة البيانات المتعلقة بعملية التفتيش وبيان صفة القائم به و من حضر التفتيش.[27]

2. تحديات التفتيش في البيئة الافتراضية

من أهم التحديات التي تواجه اجراء التفتيش عن الجرائم المعلوماتية هو الحق في الخصوصية الذي كفلت له التشريعات حماية قانونية من أي انتهاك،

وضمانات خاصة، كما أن التفتيش العابر للحدود لابد أن لا يمس بمبدأ السيادة الدولية.

1.2 احترام سيادة الدول

قد يلجأ بعض مرتكبي الجرائم تهربا من امكانية الخضوع للتفتيش الى تخزين بياناتهم في أنظمة تقنية المعلومات خارج اقليم الدولة، عن طريق ادراجها في شبكة الاتصالات البعدية، مما قد يثير صعوبات أمام جهات التحقيق فيما يتعلق بإجراء التفتيش وجمع الأدلة. [28] وفي هذه الحالة فإن امتداد الإذن بالتفتيش إلى خارج الاقليم الجغرافي للدولة التي صدر من جهتها المختصة الإذن ودخوله في المجال الجغرافي لدولة أخرى، وهو ما يسمى بالولوج أو التفتيش عبر الحدود، قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها. [29]

أجازت بعض التشريعات حق التفتيش عن المعلومات المخزنة في أنظمة معلوماتية تابعة للدولة، في حين سمحت بعض التشريعات بالتفتيش داخل الأماكن الموجودة بها بيانات مطلوب التفتيش عنها، ولو كانت موجودة في نهاية طرفية خارج الدولة، غير أن ذلك قد يعد خرقا للقوانين الثنائية الخاصة بالتعاون الدولي في مجال مكافحة الجريمة. [30]

1.1.2 تمديد التفتيش عن بعد الى خارج الاقليم الوطني

لقد أصبحت الجرائم المعلوماتية في وقتنا الراهن أكثر جدية من أي وقت مضى، وهو ما تظهره النتائج المتوصل إليها من خلال المسح الخاص بهذه الجرائم ابتداء من 2002 إلى اليوم في مختلف دول العالم، حيث لابد من مكافحتها على جميع الأصعدة. [31]

وقد وسع المشرع الجزائري من نطاق التفتيش عن بعد الى خارج الاقليم الوطني، فإذا كانت هناك أسباب تدعو الى الاعتقاد بوجود المعطيات محل البحث، والتي يمكن الدخول اليها انطلاقا من منظومة معلوماتية أو جزء منها، أو انطلاقا من المعطيات المعلوماتية المخزنة فيها، خارج الاقليم الوطني، فإن

السلطات القضائية المختصة وكذا ضباط الشرطة القضائية، يمكنهم الحصول على المعطيات المبحوث عنها، في اطار مساعدة السلطات الأجنبية طبقا للاتفاقيات الدولية ومبدأ المعاملة بالمثل.[32]

تضمنت المادة الثانية والثلاثون من المرسوم الرئاسي المتضمن المصادقة على الاتفاقية [33] مجموعة من الشروط لابد أن تتقيد بها الدول الأطراف في سبيل المساعدة المتبادلة، لغرض التحقيق أو أي إجراء متعلق بالجرائم المعلوماتية. حيث أضافت شرط وجوبي تلتزم به كل دولة طرف فيما يتعلق بالإجراءات المتعلقة بطلب التعاون والمساعدة المتبادلة، وتأسيس رفض المساعدة في حالة الرفض، مع ضمان:

- السرية عند عدم وجود معاهدة أو اتفاق للمساعدة القضائية؛
- الحفظ العاجل والكشف العاجل للمعلومات؛
- جميع الأحكام المتعلقة بالتعاون و المساعدة الثنائية فيما يخص الوصول إلى المعلومات المخزنة، أو بخصوص الجمع الفوري لمعلومات تتبع المستخدمين، أو تلك المتعلقة بالمحتوى؛

وأوجبت الاتفاقية تقديم المساعدة من الدولة الطرف المطلوب منها المساعدة، واستثنت من ذلك الجرائم المالية، أين يمكنها رفض تقديم المساعدة.

- **طلب المساعدة القضائية في حالة الاستعجال**

مكن المشرع الجزائري بموجب المادة السادسة عشر من قانون 09 - 04 السلطات المختصة من تبادل المساعدة القضائية الدولية مراعاة للاتفاقيات الدولية و مبدأ المعاملة بالمثل، بغرض جمع الدليل الخاص بالجريمة في الشكل الالكتروني، و في حالة الاستعجال يمكن قبول طلب المساعدة القضائية الدولية عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني.

كما ألزم المرسوم الرئاسي المتعلق بالمصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على تقديم طلب المساعدة الثنائية والاتصالات المتعلقة بها بشكل خطي، مع جواز تقديم الطلب في شكل عاجل في الحالات الطارئة عن طريق الفاكس أو البريد الالكتروني على أن تضمن هذه الاتصالات القدر المعقول من الأمن والمرجعية؛ بما في ذلك استخدام التشفير، وتأكيد الإرسال حسبما تطلب الدولة الطرف، ويجب على الدولة الطرف المطلوب منها المساعدة أن تقبل، وتستجيب للطلب بوسيلة عاجلة من الاتصالات.[34]

وما يستنتج في هذا الصدد أنه وفي اطار المساعدة القضائية المتبادلة وفي حالة الاستعجال يمكن للسلطات المختصة طلب تفتيش المنظومة المعلوماتية في دولة أخرى بالسرعة الممكنة، وهذا من شأنه التقليل من فرص ضياع أو تلف أو فقدان المعلومات التي تفيد في عملية التحقيق الجنائي.

2.1.2 تقييد المساعدة القضائية الدولية

اللجوء الى المساعدة المتبادلة في نظر المشرع الجزائري ليس مطلق بل مقيد بشروط منها ما تضمنته المادة التاسعة والعشرون من القانون 05 -01 الصادر في 06-02-05 المتعلق بالوقاية من تبييض الأموال وتمويل الارهاب ومكافحته، حيث تخضع المساعدة لمبدأ المعاملة بالمثل، كذلك لابد أن تتم المساعدة وفقا للاتفاقيات الدولية التي أبرمت في مجال تبادل المعلومات واتخاذ الاجراءات التحفظية أو تسليم المجرمين فيما هو مرتبط بالجريمة المعلوماتية.[35]

أولا: حالات رفض طلب المساعدة:

حصرت المادة الثامنة عشر من القانون 09 - 04 حالات رفض طلب المساعدة القضائية في حالة ما كان الطلب يمس بالسيادة الوطنية، أو النظام العام، في حين أضافت امكانية الاستجابة للطلب، أي عدم الرفض مع التقييد بشرط المحافظة على سرية المعلومات المبلغة أو شرط عدم استعمالها في غير ما هو موضح في الطلب.

كما تضمنت المادة الخامسة والثلاثون من المرسوم الرئاسي الذي يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات حالات رفض الطلب و هي:

- الجرائم السياسية: فاذا كان الطلب متعلق بجريمة يعتبرها قانون الدولة الطرف المطلوب منها المساعدة جريمة سياسية، يرفض طلب المساعدة القضائية؛
- التعدي على مصالح الدول أو سيادتها أو أمنها: فاذا كان طلب المساعدة القضائية، من الممكن أن يشكل انتهاكا لسيادة أو أمن أو نظام أو مصالح أساسية للدولة يرفض.

ثانيا: حالات عدم وجود معاهدة أو اتفاق على المساعدة المتبادلة

في حالة عدم وجود معاهدة أو اتفاق على المساعدة المتبادلة، تتفق كلتا الدولتين على احترام مجموعة شروط: الحفاظ على عنصر السرية، عدم استخدام المعلومات في تحقيقات غير مذكورة في الطلب، في حالة عدم امكانية الالتزام بالشرطين السابقين لابد على الدولة الطرف اعلام الدولة الأخرى بذلك.

يجوز للدولة المطلوب منها تقديم معلومات أن تطلب من الدولة الطالبة تبرير استخدام المعلومات.[36]

2.2 الحق في الخصوصية كأحد تحديات التفتيش عن الجرائم المعلوماتية

في المفهوم الحديث الذي يوضح التعاملات بين الأفراد من خلال معالجة المعلومات الخاصة بهم الكترونيا: يعرف الحق في الخصوصية على أنه: " حق الأفراد و المؤسسات في تحديد مدى وصول المعلومات المرتبطة بحياتهم للغير، وأن تضبط عملية حصر المعلومات الشخصية و معاملتها آليا، دون التطاول عليها من قبل الغير ".[37]

يعتبر الحق في الخصوصية أحد الحقوق المكرسة في الدساتير الوطنية والقوانين الداخلية للدول، ومناط حماية هذا الحق هي علاقته الوطيدة بحرمة المواطن الخاصة، وحرمة شرفه واعتباره، وقد كرس هذا الحق في الفصل

الرابع من الدستور الجزائري؛ تحت عنوان الحقوق والحريات، والمندرج تحت الباب الأول المتضمن المبادئ العامة التي تحكم المجتمع الجزائري.

أكدت المادة السادسة والأربعون من الدستور الجزائري على عدم جواز انتهاك حرمة المواطن الخاصة وحرمة شرفه، وأن سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، ولا يمكن المساس بهذا الحق، دون امر معلل من السلطة القضائية بالإضافة الى وجود عقوبات مقررة في حالة انتهاك هذا الحق. كما أن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب انتهاكه.[38] وكمثال تعتبر الهوية الرقمية من بين المعطيات ذات الطابع الشخصي وقد تم الاعتراف بها كمفهوم قانوني وتجاري، و حدد تأثيرها وأهميتها بالنسبة للأفراد و الحكومات و القطاع الخاص.[39]

وقد استحدث المشرع الجزائري قانون جديد سنة 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.[40] حيث أكدت المادة الثانية من هذا القانون على أن معالجة هذه المعطيات مهما كان مصدرها أو شكلها، لا يتم الا في اطار احترام الكرامة الانسانية والحياة الخاصة و الحريات العامة و الا تمس بحقوق الأشخاص و شرفهم وسمعتهم.

- **الاستثناءات الواردة على معالجة المعطيات ذات طابع شخصي**

لقد اشترط القانون 18-07 الموافقة المسبقة من الشخص الطبيعي الذي تكون المعطيات ذات الطابع الشخصي المتعلقة به محل معالجة، ويمكنه التراجع عن موافقته في أي وقت، كما لا يمكن اطلاع الغير على المعطيات محل المعالجة الا بعد الموافقة المسبقة منه. واذا كان عديم أو ناقص الأهلية تكون الموافقة وفق القواعد المقررة قانونا.[41] و لا يمكن القيام بالمعالجة للمعطيات ذات الطابع الشخصي المتعلقة بالطفل الا بعد حصول موافقة من ممثله الشرعي، أو بترخيص من القاضي المختص.[42]

غير أن الموافقة من الشخص المعني حسب ما جاءت به المادة السابعة من نفس القانون لا تكون واجبة اذا كانت المعالجة ضرورية للأسباب التالية:
- لاحترام التزام قانوني يخضع له الشخص المعني أو المسؤول عن المعالجة؛
- حماية لحياة الشخص المعني، أو حفاظا على مصالحه الحيوية اذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه؛
- تنفيذ عقد يكون الشخص المعني طرفا فيه أو لتنفيذ اجراءات سابقة للعقد بناء على طلبه؛
- لتنفيذ مهمة محددة أو تحقيقا لمصلحة مشروعة.

- الاستثناءات التي تخرج من مجال تطبيق القانون 18-07

بالرجوع للمادة السادسة من نفس القانون نجدها نصت على مجموعة من الاستثناءات التي تخرج عن مجال تطبيق القانون 18-07 في مجال المعطيات ذات الطابع الشخصي: و تتمثل في ما يلي:

أ- المعالجة من طرف شخص طبيعي لغايات لا تتجاوز الاستعمال الشخصي أو العائلي، شرط عدم احالتها للغير أو نشرها؛

ب- المعطيات ذات الطابع الشخصي المحصل عليها والمعالجة لمصلحة الدفاع و الأمن الوطنيين؛

ج- المعطيات ذات الطابع الشخصي المعالجة لأغراض الوقاية من الجرائم و متابعة مرتكبيها وقمعها، كذلك المحتوية في قواعد البيانات القضائية التي تخضع إلى النص الذي أحدثت بموجبه وإلى أحكام المادة العاشرة من القانون 18-07.حيث وضحت المادة العاشرة شرطين هامين يجب التقيد بهما و يتمثلان في أنه:- لا يمكن معالجة المعطيات ذات الطابع الشخصي المتعلقة بالجرائم و العقوبات وتدابير الأمن، الا من قبل السلطة القضائية والسلطات العمومية و الأشخاص المعنوية المسيرة لمصلحة عمومية، و مساعدي العدالة في اطار اختصاصاتهم القانونية. - يجب تحديد المسؤول عن المعالجة والغاية منها

والأشخاص المعنيين بها، والغير الذي يمكنه الاطلاع على المعلومات ومصدرها والاجراءات الواجب اتخاذها لضمان سلامة المعالجة.

بإسقاط هذه المواد على أحكام التفتيش عن الجرائم المعلوماتية، نجد أنه لا يشترط الموافقة المسبقة للشخص المعني عند اجراء التحقيق في الجرائم المعلوماتية، والتفتيش باعتباره اجراء من اجراءات التحقيق تراعي فيه السلطات المختصة الضوابط الشكلية والموضوعية للتفتيش المحددة قانونا، ولمقتضيات التحقيق وصحته يمكن تفتيش المعطيات ذات الطابع الشخصي اذا كانت تفيد في الكشف عن الجريمة ومرتكبيها. وهذا لا يعد انتهاكا للحق في الخصوصية وانما استثناء غرضه كشف المتهم واثبات الجريمة.

غير أن التساؤل هنا يثور حول الاجراءات التي يمكن أن يتخذها الشخص اذا تم الاعتداء من قبل سلطات التفتيش على حقوقه الشخصية؛ ففي حالة تجاوزسلطة التفتيش في ممارسة حقها القانوني وتعدي ذلك على الحق في الخصوصية لم يشر القانون صراحة لآلية اجرائية واضحة غير تلك المتعلقة بالتمسك بالبطلان باعتبار التفتيش اجراء جوهري، ومن بين الاجراءات التي يمكن أن يتخذها الشخص لمواجهة الاعتداء الممارس عليه من قبل سلطات التفتيش على حقوقه الشخصية هو التقدم أمام القضاء بدعوى الاعتداء على الحريات الشخصية طبقا لما جاء في الدستور وذلك من خلال تبيان أن التفتيش الممارس عليه شكل نوع من الاعتداء على حرمته كشخص وانتهاك لحق السر. حيث يبين أن التفتيش باطل بعد اظهار تخلف شرط أو مجموعة من الشروط الاجرائية والموضوعية المنظمة لعملية التفتيش، والتي جاء النص عليها من خلال المواد 44-47 قانون اجراءات جزائية جزائري، فالأجدر على الجهات القضائية المختصة أن تعمل وفقا للقانون والذي يحمي الحريات الفردية من التعسف واساءة استعمال السلطة، مما يرتب على عدم توفر الضوابط الأساسية للتفتيش بطلان هذا الاجراء.

ولعل أهم الوسائل التي كرسها المشرع الجزائري حديثا هو الدفع بعدم دستورية القوانين، و هو من الآليات التي أتاحها القانون للأفراد كوسيلة لتكريس حق الدفاع من خلال تبيان أن الشخص قد تعرض لتعدي غير مشروع و مخالف للقانون و الدستور.

3.2 معالجة المشكلات التي يثيرها التفتيش الجزائي في العالم الافتراضي

من بين المشكلات العملية التي يثيرها التفتيش الجزائي في العالم الافتراضي هو طبيعة الاذن الذي يشترط لصحة اجراء التفتيش، حيث أن التفتيش الالكتروني يشترط اذن مسبق و منفصل عن اذن تفتيش المسكن، ما يعني أنه بعد الحصول على اذن النيابة، وتفتيش مسكن المشتبه فيه، وحجز أجهزة الحاسوب والهواتف ودعامات التخزين الالكترونية، يقوم ضابط الشرطة القضائية بتقديم طلب للنيابة للحصول على اذن كتابي من أجل تفتيش الأجهزة المحجوزة بمسكن المشتبه فيه، للحصول على أدلة تفيد في عملية التحقيق، حيث أن المسكن مثله مثل أجهزة المشتبه فيه دائما تحتوي على أشياء خصوصية تستدعي اذن الاطلاع عليها؛ فمثلا لو قام ضابط الشرطة القضائية بتفتيش مسكن دون اذن مسبق يتابع بجنحة انتهاك حرمة مسكن، وهو نفس الشيء بالنسبة لأجهزة المشتبه فيه، فاذا تم تفتيشها دون اذن مسبق يمكن للمعني متابعة ضابط الشرطة القضائية بجنحة المساس بحرمة الحياة الخاصة للأشخاص، وذلك عن طريق تقديم شكوى للنيابة.

وتجدر الاشارة أن المشتبه فيه لايمكن أن يعترض على تفتيش حاسوبه أو هاتفه بعد حصول ضابط الشرطة القضائية على اذن بالتفتيش، حيث يتم حجز الأجهزة و تحرير محضر حجز وتعرض الأجهزة على المخبر الجهوي لتفتيشها، فإذا اعترض المشتبه فيه، هنا سيكون متهم بجنحة ثانية و هي عرقلة سير التحقيق.

غير أنه في سبيل ضمان عدالة التفتيش المعلوماتي يخول القانون للمتضرر من هذا الاجراء الحق في رفع دعوى قضائية، أمام الجهات القضائية المختصة، أساسها مساس سلطات التفتيش بحقه في الخصوصية، متى اختُرقت منظومته المعلوماتية الخاصة، على غير الأشكال التي يحددها القانون، وذلك وفقا لما تقتضيه أحكام المواد 303 مكرر وما بعدها من قانون العقوبات الجزائري، التي ترتب عقوبات جنحية على تلك الانتهاكات، متى لم يتوافر فيها شرطا الاباحة، وهما: الاذن القضائي، ورضا المجني عليه، هذا من الناحية الموضوعية، أما من الناحية الاجرائية فيترتب على تلك الانتهاكات بطلان اجراء التفتيش بطلانا مطلقا، ذلك أن الاذن القضائي يشترط الالتزام بحدوده الشخصية والعينية، ويعتبر من الشروط الجوهرية التي لايستقيم التفتيش إلا بها، متى لم ينص القانون على خلاف ذلك حيث يوجب قانون الاجراءات الجزائية على الجهات القائمة بالتفتيش السهر على احترام أحكامه الموضوعية، وجوانبه الاجرائية، وإلا وقع تحت طائلة البطلان.

إضافة الى ماسبق هناك مجموعة من المشكلات الأخرى التي يثيرها التفتيش في البيئة الافتراضية من بينها:

- في بعض الأحيان يتعذر حجز الأجهزة عندما تكون عبارة عن خوادم تحتوي على قاعدة بيانات ضرورية لسير شركة ما، لكن يمكن تفتيشها في عين المكان ونسخ المعطيات الضرورية طبقا لأحكام القانون 09-04 سالف الذكر؛

- المدة الطويلة التي يتطلبها التفتيش الالكتروني مقارنة بقصر مدة التوقيف للنظر؛

- نقص الخبرة الفنية في رفع الأدلة الالكترونية وصعوبة تحليلها وسهولة محوها والتلاعب فيها يشكل معيقا للتحقيق في الجرائم المعلوماتية، ويصعب اكتشاف المجرم المعلوماتي؛

- عدم استيعاب التشريعات الداخلية للكم الهائل من الجرائم المعلوماتية التي تبقى دائما في تطور مستمر وفي كل مرة تخلق وسائل وأساليب جديدة تستدعي تطوير أساليب واجراءات مواجهتها؛
- المشكلات المتعلقة بالنطاق المكاني لارتكاب الجرائم المعلوماتية لكن المادة 586 قانون اجراءات جزائية فصلت في المسألة، حيث يطبق القانون الجزائري وفقا لمبدأ الاقليمية على الجرائم التي يكون عمل من الأعمال المرتبط بأحد أركانها قد تم في الجزائر، أما في حالة ارتكاب الجريمة خارج اقليم الدولة مع مساسه بأمن الدولة أو أحد مصالحها الأساسية، أو تزييف العملة الوطنية فقد فصلت في ذلك المادة 588 من نفس القانون وأكدت المادة 53 من القانون 18-07 على اختصاص الجهات القضائية في الجرائم المتعلقة بمعالجة المعطيات ذات طابع شخصي التي ترتكب خارج اقليم الجمهورية وهنا تحيلنا على المادة 588 حيث يطبق القانون وفقا لمبدأ العينية رجوعا للقواعد العامة فيما يخص ارتكاب الجرائم خارج اقليم الدولة.

الخاتمة:

يعتبر التفتيش عن الجرائم المعلوماتية، اجراء في غاية الخطورة، تلجأ اليه السلطات المختصة في مجال المعلومات، قصد التوصل للأدلة التي تفيد في كشف الجريمة، إلا أن ذلك قد يمس بالحق في الخصوصية والمعطيات ذات الطابع الشخصي وقد يمس بخصوصية الدول. و علاجا لمشكلة الدراسة، ومعوقات التفتيش الجزائي في العالم الافتراضي، توصلنا الى مجموعة من النتائج و الاقتراحات التي نوردها على النحو الآتي:

- **النتائج:**

1-يمكن اجراء التفتيش عن الجرائم المعلوماتية دون الاخلال بالضمانات اللازمة لحماية الحق في الخصوصية عن طريق لجوء السلطات المختصة في مجال المعلومات الى اعتماد الضوابط القانونية الشكلية و الموضوعية، قصد

التوصل للأدلة التي تفيد في كشف الجريمة، وهنا تثار اشكالية تخلف أحد الشروط اللازمة لصحة الاجراء: في هذه الحالة يترتب البطلان؛ فمثلا عند تجاوز حدود الاذن مما يشكل انتهاكا لخصوصية الأفراد، يمكن للمتضرر رفع دعوى قضائية قوامها المساس بحقه في الخصوصية و يدفع ببطلان اجراءات التفتيش.

2-استحدث المشرع الجزائري سلطة وطنية لحماية المعطيات ذات الطابع الشخصي بموجب القانون 18-07 و قد تضمن هذا الأخير شرط مهم يتمثل في الموافقة المسبقة للشخص المعني قصد معالجة أي من المعطيات ذات الطابع الشخصي، غير أنه و لمقتضيات التحقيق يمكن القيام بالتفتيش من قبل السلطات المختصة دون هذه الموافقة، وهنا تمت معالجة اشكالية اعتداء السلطات المختصة على الحقوق الشخصية للفرد حيث لم يشر القانون لآلية اجرائية واضحة غير تلك التي تستدعي التمسك بالبطلان أمام الجهات القضائية.

3-قد يمتد التفتيش لخارج الحدود الوطنية، مما يستدعي مساعدة قضائية متبادلة، أو تماشيا مع مبدأ المعاملة بالمثل من قبل المجرم الذي أخفى الأدلة في أنظمة معلوماتية تابعة لدولة أخرى. وفي هذا الاطار صادقت الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي تضمنت أطر المساعدة القضائية و كيفيتها.

- **الاقتراحات:**

1- مسايرة التطورات التكنولوجية السريعة من خلال استحداث قانون خاص يوضح القواعد القانونية التي تحكم محل التفتيش عن الجرائم المعلوماتية.

2- التكوين النوعي لضباط الشرطة القضائية، و رجال القضاء بتقنيات الحاسب الآلي، مع توظيف أشخاص أكفاء في هذا المجال لضمان التفتيش دون ضياع الأدلة أو تلفها؛

3

3- انضمام الجزائر الى مجموعة الاتفاقيات الدولية التي تهدف للمساعدة القضائية المتبادلة و مكافحة الجريمة المعلوماتية بوجه عام.

التهميش و الإحالات :

[1]- أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية و التدريب، المجلد 29، العدد 58، جامعة نايف العربية للعلوم الأمنية، السعودية، ديسمبر 2013، صفحة 87.

[2]- محمد الأمين البشري، التحقيق في الجرائم المستحدثة، مركز الدراسات و البحوث، جامعة نايف للعلوم الأمنية العربية، الرياض، سنة 2004، صفحة 88.

[3]- عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مركز دراسات الكوفة، العدد السابع، سنة 2008، صفحة 112.

[4]- يونس عرب، جرائم الكمبيوتر و الانترنت، ورقة عمل مقدمة الى مؤتمر الأمن العربي، المركز العربي للدراسات و البحوث الجنائية، أبو ظبي، 2002، صفحة 8.

[5]- نمديلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري و القوانين المقارنة، المؤتمر الدولي الرابع عشر، طرابلس 24-25 مارس 2017، صفحة 99.

[6]- فهد عبد الله العبيد العازمي، الاجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الاسكندرية، 2016، صفحة 42.

[7]- و يطلق على الجريمة المعلوماتية أيضا: الجريمة السيبرانية أي جريمة الانترنت أو الجريمة المرتكبة بواسطة الحواسيب و غيرها من أشكال تكنولوجيا المعلومات و الاتصالات. أنظر

S. Broadhead, The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law and Security Review, 34 (6), 2018, 1180.

[8]- خلدون عيشة، الطبيعة الخاصة للجريمة الالكترونية و صورها، مجلة دراسات و أبحاث، مجلد 04، عدد09، الجلفة، سنة 2012، صفحة 115.

[9]- فهد عبد الله العبيد العازمي، المرجع السابق، صفحة 42.

[10]- خالد عياد الحلبي، اجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، دار الثقافة للنشر و التوزيع، الطبعة الأولى، سنة 2011، صفحة 151.

[11]- سلمى مانع، التفتيش كإجراء للتحقيق في الجرائم المعلوماتية، مجلة العلوم الانسانية، عدد 22، جامعة محمد خيضر بسكرة، جوان 2011، صفحة 229.
[12]- رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية و السياسية، عدد 05، الوادي، الجزائر، جوان 2012، صفحة 164.
[13]- سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية (دراسة تحليلية)، دار الكتب القانونية، مصر، 2011. صفحة117.
[14]- فهد عبد الله العبيد العازمي، الاجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الاسكندرية، 2016، صفحة 262.
[15]- S. Mason, Electronic Evidence: A proposal to reform the presumption of reliability and hearsay, Computer Law and security Review, 30 (1), 2014, 80.
[16]- سامي جلال فقي حسين، المرجع السابق، صفحة 127.
[17]- رضا هميسي، المرجع السابق، صفحة 167.
[18]- أنظر المادة 06 من القانون 09-04، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال ومكافحتها، الجريدة الرسمية عدد 47، الصادرة في 16 أوت 2009.
[19]- أنظر المادة 07 قانون 09-04 سالف الذكر.
[20]- أنظر الفقرة الأخيرة من المادة 05 من القانون 09-04 سالف الذكر.
[21]- أنظر المادة 44 الامر 66-155 المؤرخ في 8 جويلية 1966 المتضمن قانون الاجراءات الجزائية المعدل و المتتم بالقانون 18- 06 المؤرخ في 10 يونيو 2018، الجريدة الرسمية، عدد 34 الصادرة في 10 جويلية 2018.
[22]- أنظر الفقرة الأخيرة من المادة 45 قانون اجراءات جزائية سالف الذكر.
[23]- أنظر المادة 47 مكرر قانون اجراءات جزائية سالف الذكر.
[24]- المادة 47 قانون اجراءات جزائية سالف الذكر.
[25]- مصطفى محمود موسى، التحقيق الجنائي في الجرائم الالكترونية، طبعة أولى، مطابع الشرطة، القاهرة، 2009، صفحة 204.
[26]- سامي جلال فقي حسين، المرجع السابق، صفحة 171.
[27]- رضا هميسي، المرجع السابق، صفحة 170.
[28]- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، طبعة أولى، دار الفكر الجامعي، الاسكندرية، 2011، صفحة81.

[29]- علي عدنان الفيل، اجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)، دار الكتب و الوثائق القومية، الاسكندرية، 2012، صفحة46.

[30]- وقد جاء الحث على التعاون الدولي في القرار الصادر عن المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات حول القواعد الاجرائية في بيئة جرائم الكمبيوتر. انظر: زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى، عين مليلة، الجزائر، 2011، صفحة 144.

[31]- W. Chung, H. Chen, W. Chang, S. Chou, Fighting cybercrime: a review and Taiwan experience, Decision Support Systems, 43(3), 2006, 669.

[32]- أنظر المادة 05 من القانون 09-04.

[33]- صادقت الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، بموجب المرسوم الرئاسي رقم 14-252، المؤرخ في 08 سبتمبر 2014. أنظر الجريدة الرسمية عدد 57، الصادرة بتاريخ 28 سبتمبر 2014.

[34]- أنظر المادة 32 من المرسوم الرئاسي، 14-252، المؤرخ في 08 سبتمبر 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، الجريدة الرسمية عدد 57، الصادرة بتاريخ 28 سبتمبر 2014.صفحة10.

[35]- زبيحة زيدان، المرجع السابق، صفحة 145.

[36]- أنظر المادة 36 من المرسوم الرئاسي 14-252، المؤرخ في 08 سبتمبر 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، الجريدة الرسمية عدد 57، الصادرة بتاريخ 28 سبتمبر 2014.صفحة 10.

[37] - الدهبي خدوجة، حق الخصوصية في مواجهة الاعتداءات الالكترونية (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، العدد 08، المجلد الأول، ديسمبر 2017

[38]- المادة 47 من القانون رقم 16-01، المؤرخ في 06 مارس 2016، يتضمن التعديل الدستوري، الجريدة الرسمية، عدد 14، الصادرة في 07 مارس 2016، صفحة 11.

[39] - C. Sullivan, Digital identity- From emergent legal concept to new reality, Computer Law and Security Review, 34 (4), 2018, 723.

[40]- وفي هذا الاطار حفاظا على المعطيات ذات الطابع الشخصي، تم استحداث سلطة وطنية تسهر على مطابقة معالجة هذه المعطيات و تضمن عدم انطواء استعمال تكنولوجيات الاعلام و الاتصال على أي أخطار تجاه حقوق الأشخاص و الحريات العامة و الحياة الخاصة. و هي عبارة عن سلطة ادارية مستقلة توضع لدى رئيس الجمهورية وذلك بهدف حماية المعطيات ذات الطابع الشخصي. و قد أسندت لها عدة مهام ضمانا للحق في الخصوصية اضافة الى حقوق الأشخاص و الحريات العامة من أي خطر قد يطالها. و تتمتع هذه السلطة ب: - الشخصية المعنوية -الاستقلال المالي -الاستقلال الاداري.

[41]- أنظر المادة 07 من القانون 18-07 سالف الذكر.

[42]- أنظر المادة 08 من القانون 18-07 سالف الذكر.

قائمة المراجع:

- **المؤلفات**

1- بكري، يوسف بكري، (2011)، التفتيش عن المعلومات في وسائل التقنية الحديثة، الاسكندرية، طبعة أولى، دار الفكر الجامعي.

2- زبيحة، زيدان، (2011)، الجريمة المعلوماتية في التشريع الجزائري و الدولي، عين مليلة، الجزائر، دار الهدى.

3- حسين، سامي جلال فقي، (2011)، التفتيش في الجرائم المعلوماتية (دراسة تحليلية)، مصر، دار الكتب القانونية.

4- علي، عدنان الفيل، (2012)، اجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)،الاسكندرية، دار الكتب و الوثائق القومية.

5- حجازي، عبد الفتاح، (2006)، مكافحة جرائم الكمبيوتر (دراسة معمقة في القانون المعلوماتي)، الاسكندرية، طبعة أولى، دار الفكر الجامعي.

6- مصطفى، محمود موسى، (2009)، التحقيق الجنائي في الجرائم الالكترونية، القاهرة، طبعة أولى، مطابع الشرطة.

7- العازمي، فهد عبد الله العبيد، (2016)، الاجراءات الجنائية المعلوماتية، الاسكندرية، دار الجامعة الجديدة.

8- البشري، محمد الأمين، (2004)، التحقيق في الجرائم المستحدثة، الرياض، طبعة أولى، مركز الدراسات و البحوث، جامعة نايف للعلوم الأمنية العربية.

9- الحلبي، خالد عياد، (2011)، اجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، عمان، دار الثقافة للنشر و التوزيع.

- **المقالات العلمية باللغة العربية:**

1- الشكري، عادل يوسف عبد النبي، (2008)، الجريمة المعلوماتية و أزمة الشرعية الجزائية، مركز دراسات الكوفة، العدد 07، الكوفة.

2- العبيدي، أسامة بن غانم، (2013)، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية و التدريب، المجلد 29، العدد 58، جامعة نايف العربية للعلوم الأمنية، السعودية.

3- الدهبي خدوجة، (2017)، حق الخصوصية في مواجهة الاعتداءات الالكترونية (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، المجلد 01، العدد 08، المسيلة.

4- خلدون، عيشة، (2012)، الطبيعة الخاصة للجريمة الالكترونية و صورها، مجلة دراسات و أبحاث، المجلد 04، العدد 07، الجلفة.

5- هميسي، رضا، (2012)، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية و السياسية، عدد 05، الوادي، الجزائر.

6- مانع، سلمى، (2011)، التفتيش كإجراء للتحقيق في الجرائم المعلوماتية، مجلة العلوم الانسانية، عدد 22، جامعة محمد خيضر بسكرة.

باللغة الانجليزية:

1-W. Chung , H. Chen, W. Chang, S. Chou, (2006), Fighting cybercrime: a review and Taiwan experience, Decision Support Systems, 43(3).

2-S. Mason, (2014), Electronic evidence: A proposal to reform the presumption of reliability and hearsay, Computer Law and security Review, 30 (1).

3-C. Sullivan, (2018), Digital identity- from emergent legal concept to new reality, Computer Law and Security Review, 34 (4).

4- S. Broadhead, (2018), The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law and Security Review, 34 (6).

- **المداخلات:**

1- عرب، يونس، (2002)، جرائم الكمبيوتر و الانترنت، مؤتمر الأمن العربي، المركز العربي للدراسات و البحوث الجنائية، أبو ظبي.
2- نمديلي، رحيمة، (2017)، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، المؤتمر الدولي الرابع عشر، طرابس، لبنان.