مجلة الاجتهاد القضائي: المجلد 12 - العدد 01 (العدد التسلسلي 21) مارس 2020 - (ص ص: 749 – 772)
مخبر أثر الاجتهاد القضائي على حركة التشريع - جامعة محمد خيضر بسكرة

تفتيش المنظومة المعلوماتية في ضوء الفقه والاجتهاد القضائي الأمريكي

Search of Information System
In the light of the American Jurisprudence Doctrine

ط. د. لهوى رابح[1]

باحث دكتوراه - علوم جنائية

كلية الحقوق والعلوم السياسية

جامعة الحاج لخضر – باتنة 1 (الجزائر)

lahoua@gmx.fr

تاريخ الارسال:	تاريخ القبول:	تاريخ النشر
08 أكتوبر 2019	04 جانفي 2020	25 مارس 2020

الملخص:

يعتبر تفتيش نظم المعلومات من أخطر الإجراءات الجنائية انتهاكا للحق في الخصوصية، لكونه ينصب على أنظمة معلوماتية باتت تشكل مستودع سر الأفراد، وإذ هي تحتوي على عالم غير محدود من خصوصياتهم فهي أيضا تتضمن بيانات مجرّمة تشكل موضوعا للدليل الجنائي على نحو يتعذر استرداده من غير أن يكون التفتيش أكثر امتداد عبر الملفات البريئة حيث أضحى التوسع في الاستثناء هو القاعدة، بما يقيم الحاجة للبحث عن حدود جديدة يتفاعل من خلالها هذا الإجراء في بيئة رقمية تنعدم فيها الحدود المادية وتختلط فيها البيانات المجرّمة مع البيانات البريئة، يعمل على كشف الأولى ويصون سرية الأخيرة.

الكلمات المفتاحية: تفتيش، نظام معلوماتي، بروتوكول، امتداد، حدود، الحق في الخصوصية.

Abstract :

Search of Information Systems are considered among the most dangerous criminal procedures in violation of the right of privacy as it set information systems that start to form tank of individuals' secrets. This limitless world of people's privacies includes criminal data that form a theme of criminal evidence in a way that prevents its recapture without being inspected extensively across some innocent files as extension becomes the rule that elicits the need to search for new limits interact through the procedure in a digital environment in which materialistic limits are absent and criminal data amalgamated with innocent ones and then works to unveil the former and keeps privacy of the latter.

key words: *search, Information System, protocol, extension, limits, right of privacy.*

[1] المؤلف المرسل: ط. د. لهوى رابح ـــــــــــــــــــــــ *Email: lahoua@gmx.fr*

مقدمة:

حرص المشرع الدستوري الأمريكي على حماية الحق في الخصوصية إزاء التفتيش الجنائي بقاعدتين وقائيتين، تتطلب القاعدة الأولى لزوم استصدار إذن قضائي مسبب يحدد محل التفتيش ومستهدفه، وتستوجب القاعدة الثانية تنفيذ التفتيش بطريقة معقولة، فبينما ترمي الأولى إلى تجنّب وقوع أي انتهاك غير مبرّر على هذا الحق، تستهدف الثانية قصر نطاق هذا الانتهاك في أضيق الحدود.

غير أنّ تطبيق هذه المبادئ الإجرائية في سياق التفتيش عن الأدلة المعلوماتية يجعلها مجرّد فلسفة سائدة ليس إلا، بسبب القدرة التخزينية الهائلة للوسائط الرقمية التّي تختلط فيها البيانات البريئة مع البيانات المجرّمة التي تشكل موضوعا للدليل الجنائي، مع استحالة معرفة موقع هذه الأخيرة قبل تنفيذ التفتيش، لأنّها عادة ما تكون مخفيّة أو مفخّخة أو مشفّرة بطرق تجعل من المستحيل اكتشافها دون استعراض أعداد كبيرة منها، وهو ما يتجاوز الغاية من التفتيش كأهم ضمان تقوم عليه نظرية التفتيش الجنائي في حماية الحرية الفردية.

ولأنّ القانون العربي والمقارن لا يزال في غيبة من التّعرض لهذه المسألة حتّى الآن ومحاولة منّا لإقامة توازن معقول بين اعتبارات الشرعية والفعالية في مواجهة هذا الإجراء، نطرح على بساط البحث الإشكالية التالية: هل يمكن تطبيق القواعد التقليدية للتفتيش المادي في مجال تفتيش المنظومة المعلوماتية ذات الطابع الافتراضي؟

وللوصول إلى هدف البحث، سوف نستخدم أسلوب التحليل المصغّر للتّعرف على جزئيات المشكلة وتفاصيلها بغية التعمّق فيها، وابتغاء وضع هذه الأفكار في نسق علمي متكامل ارتأينا تقسيم الدراسة إلى مبحثين، نرصد الأول لدراسة قاعدة لزوم تحديد محل التفتيش، بينما نخصص الثاني لقاعدة لزوم تحديد منهجية تنفيذ التفتيش.

المبحث الأول: طبيعة المحل في مجال تفتيش المنظومة المعلوماتية

يثور التساؤل في ضوء هذه القاعدة عن "الشيء" الذي يقتضي لصحة الإذن أن يحدده "محلا للتفتيش"؟ هل يحدد "أجهزة التخزين الرقمية" المراد ضبطها في مرحلة التفتيش المادي؟ أم "البيانات" المراد استردادها في مرحلة تفتيش المنظومة المعلوماتية؟ هل مدلول "مكان التفتيش" ينصرف إلى مكان أجهزة التخزين في البيئة المادية أم مكان البيانات من مساحة التخزين الرقمية؟ والإجابة على ذلك تقضي التطرق إلى إشكالية محل التفتيش (مطلب أول)، ومتطلبات تحديده (مطلب ثاني).

المطلب الأول: إشكالية تحديد المحل في مجال تفتيش المنظومة المعلوماتية

مع التسليم من حيث المبدأ بكون البيانات هي المكان الذي يتم تفتيشه في مرحلة التحليل (فرع أول)، فإنّ هذا المحل لا يكون قائما بذّاته بل دائما ما يكون متصلا بجهاز لا ينفصل عنه، بما يوجب التفتيش عنه أولا قبل تفتيشه (فرع ثاني).

الفرع الأول: إشكالية المنظور المزدوج للمحل في مجال تفتيش المنظومة المعلوماتية

محل التفتيش هو المكان الذي يجري التفتيش فيه، ولزوم قصره على مكان معيّن هو من مستلزمات طبيعته الاستثنائية، فهذا المبدأ الدستوري محل استفسار متزايد حول مدلول المحل في مجال تفتيش نظم المعلومات، باعتبار أن التفتيش يجري في مكان "البيانات" لا يختلف عن مكان تواجد البيانات ذاتها "الأجهزة المادية"[1]، فأيّهما يوجب القانون تحديده كمحل للتفتيش؟ وبعبارة أخرى هل صدور إذن بالتفتيش عن دليل معلوماتي معيّن، يجيز توسيع نطاق التفتيش إلى كافة البيانات التي يحتويها جهاز التخزين الرقمي؟ أم يقتصر نطاقه على ملف معيّن دون جواز امتداده إلى غيره من البيانات؟

لا يجمع القضاء الأمريكي على موقف موحد إزاء المشكلة محل البحث، حيث يعتمد جانب من الفقه المنظور المادي لوسيط التخزين الرقمي وينادي بوجوب التعامل مع وسائط التخزين الرقمية كدليل مادي، بحيث يعتبر القرص الصلب مجرّد "شيء"، وليس"مكانا"، أو بالأحرى هو"شيء واحد" لا يحتوي على أي أشياء أخرى، شأنه شأن أي دليل مادي يتم "فحصه" وليس "تفتيشه" [2]، بحيث يجوز التّوسع في التفتيش عبر كافّة مساحة وسيط التخزين باعتبارها تشكل وحدة واحدة، ومن تطبيقات ذلك ما قضت به الدائرة الخامسة الفيدرالية في قضية *United States v. Runyan*، وتردّد ذات التبرير في قضية *United States v. Slanina* [3].

وعلى العكس هذا المذهب، اتجه جانب آخر من الفقه في محاولة منه لتقليص نطاق امتداد التفتيش المعلوماتي إلى مطالبة القضاء بالتعامل مع ملفات القرص الصلب كمجموعة حاويات مغلقة ومنفصلة، يتطّلب فحص كلّ حاوية إذنا مستقلا بتفتيشها. وبعبارة أخرى، ينبغي أن يُنظر إلى الحاسوب على أنّه الحاوية المادية مع سلسلة من "الحاويات الإلكترونية" وهي المجلدات والملفات التّي يقتضي الاطّلاع عليها والولوج إليها بشكل منفصل دون أن يمتّد إلى مجملها، فكلّ فتح منفصل بمثابة عملية تفتيش جديدة تخضع للقيود الدستورية[4]، ومن هنا يصبح القانون وسيلة "لتنظيم الوصول إلى المعلومات" في "بيئة رقمية" حيث الحواجز المادية غالبا ما تكون مفقودة [5]، وهو الاجتهاد القضائي الذي إنتهت إليه الدائرة العاشرة في قضية *United States v. Carey*[6].

وإجمال ما تقدم، أنّ لزوم تحديد محل التفتيش كضمانة شكلية تحول دون التوسع في نطاقه ينصرف مدلولها إلى البيانات المخزّنة التي تختلط بها "المعلومات" المجرّمة وليست "وسائط التخزين" في وضعها المادي، بحيث يمكن في استعارة المفهوم المادي للمكان وترجمته في العالم المعلوماتي في شكل ملف معيّن أو مجلد ما، على نحو يشكل حيزا محددا ضمن ضمن مساحة التخزين الرّقمي، وذلك التزاما بحدود الشرعية وما توجبه قرينة البراءة، أمّا اعتماد المنظور المادي لمحل التفتيش فهو يعتبر عدوانا على الحق في الخصوصية يتجاوز حقوق المتهم وأفراد أسرته إلى انتهاك حقوق الغير، لذا ينبغي على القضاء أن لا يتردد في تطبيق هذه القاعدة بكل حزم مهتديا في ذلك بروح الدستور في حماية الحريات الفردية.

الفرع الثاني: إشكالية ارتباط المحل في مجال تفتيش المنظومة المعلوماتية بمستهدف التفتيش المادي

من البديهي أن تكون أجهزة التخزين الرقمية "مستهدفا للتفتيش" قبل أن تكون "محلا له"، فينبغي التفتيش عليها قبل تفتيشها، وتثير هذه الحقيقة تساؤلا مشروعا يتعلق أساسا بما ينبغي للإذن أن يحدده كشيئي يتعين التفتيش عنّه وضبطه في مرحلة التفتيش المادي لتفتيشه لاحقا؟ هل يحدد الأجهزة المادية ذاتها؟ أم يحدد المعلومات المجرّمة المراد استرداداها؟.

لقد تعرض القضاء لهذا التساؤل في كثير من أحكامه وخلص إلى التميّيز بين الحالة التّي تكون فيها الأجهزة المادية بحد ذاتها مجرّمة أو أدلة عن الجريمة أو أداة للجريمة، وبين الحالة التّي تكون فيها هذه الأجهزة مجرّد حاوية للدليل المعلوماتي، ولا تطرح الحالة الأولى أيّ إشكال إذ لا يتطلب القضاء هنا سوى تحديد وسائط التخزين الرقمية بدلا المعلومات التّي تحتويها[7]، أمّا الحالية الثّانية والتّي تكون فيها أجهزة التخزين الرّقمية مجرّد حاويّة للدليل الجنائي، فإنّ القضاء عالجها بدون تعمق مكتفيا بالإشارة إلى لزوم التّركيز على الملفات المستهدفة وأنّ إغفالها قد يشكل مخالفة للدستور، وعلى نقيض ذلك فقد تطرق الفقه إلى هذه الفرضية بتعمق كبير، ليس بما تستلزم من إجابات بقدر ما تطرح من إشكاليات.

إذ يرى الفقه أنّ هنّاك افتراضان:

أمّا الافتراض الأوّل، فهو تحديد أجهزة التخزين المادية كأدلة يراد ضبطها، ما يجعل الإذن دقيقا، حيث يتم تنفيذ الإذن بالدخول إلى المكان المطلوب تفتيشه والبحث عن أجهزة التخزين الرقمية واسترجاعها، وهو ما يثير إشكالا بالغ التعقيد، ففي الحالة التي يقتصر فيها التخصيص على الأجهزة المادية يصبح الإذن عاما، فمن جهة أولى لا يوجد لدى الضبطية القضائية سبب يبرّر ضبط جميع أجهزة التخزين الموجودة بالمسكن.

ومن جهة أخرى، فإنّ اقتصار التحديد على الأجهزة المادية وإن كان دقيقا من النّاحية التقنّية في مرحلة التفتيش المادي، ولكنّه لا يفصح عن أيّ تفصيل بشأن التفتيش الإلكتروني

اللاّحق، فعندما يطّلع خبراء التّحليل الحاسوبي الشّرعي على محتويات أجهزة التخزين الرقمية لاسترداد الأدلة، لن يكون هناك ما يوجه سلوكهم كون الإذن يجيز الضبط الشامل للأجهزة المادية[8]، فيمتد التفتيش ليصل إلى أقصى مدى له.

أمّا الافتراض الثّاني، فهو تحديد البيانات كالأدلة يتعين ضبطها، وهذا النّهج لا يحدد بدقة ما ستقوم به الضبطية القضائية في مرحلة التفتيش المادي، ولكنّه يحدد الأدلة التي تسعى إليها في مرحلة تفتيش المنظومة المعلوماتية فهو يضع حدا لامتداد التفتيش بأن يصبح الإذن أكثر تحديدا. غير أنه يفضي إلى إشكالية جديدة طالما أن ذات الاذن يفقد شرط التحديد حول كيفية تنفيذ مرحلة التفتيش المادي، فإن كان الإذن يجيز التفتيش عن بيانات محددة وضبطها، إلاّ أن تنفيذ عملية تفتيش المنظومة المعلوماتية يستوجب أولا ضبط جميع أجهزة التخزين الرقمي التي يمكنهم العثور عليها في الموقع وإرسالها إلى مخابر التحليل المتخصصة لفحص محتوياتها، فتنفيذ الإذن يتم بالمخالفة لما يجيزه الإذن نفسه [9].

في اعتقادنا فإنّ هذه الجدليّة تكشف أّن التّحديد الذي ينصب على أجهزة التخزين الرّقمية كأشياء يراد ضبطها يجعل التفتيش واسع النطاق وأكثر توسّعا وشمولا وفي ذلك ما يناقض مبدأ الشرعية، وفي مقابل ذلك فإن التّحديد الذّي يركز على البيانات لا يجيز للضبطية القضائية القيّام بما هو ضرّوري لاسترداد هذه الأدلة، فيفشل الإجراء في تحقيق الفعاليّة، ويقترح الفقه لوضع حد لامتداد التفتيش ضرورة أن يشتمل إذن التفتيش تحديدا للأدلة المادية المراد ضبطها في مرحلة التفتيش المادي وتخصيصا للأدلة التي يتعين ضبطها في المرلحة اللاحقة أي مرحلة تفتيش المنظومة المعلوماتية.

وبدورنا نؤيد هذا الرأي، فتقييد مرحلة التفتيش المادي بأجهزة محددة يجوز ضبطها متى قامت الأسباب التي ترجّح احتوائها على أدلة تفيد في إظهار الحقيقة، مع تضييق نطاق المراجعة في مرحلة التفتيش الألكتروني من شأنه أن يرسم حدودا لنطاق التفتيش توخيا من امتداده إلى جميع الأجهزة في المرحلة الأولى وإلى جميع محتوياتها في المرحلة الثانية لأن وجود سبب يبرر تفتيش ملف معيّن لا يبرر تفتيش محتويات الجهاز ككلّ، فكيّف يكون مبررا لتفتيش كافّة هذه الأجهزة، فعدم تحديد محل التفتيش في المرحلة الثانية يعتبر في نظرنا باطلا، لأنّ القانون إذ أجاز تقيّيد حرّية الأفراد بصفة استثنائية فإنّه يسمح بذلك بالنّسبة لمحل معيّن على وجه التخصيص وليس العمومية منعا من التطاول على الحرّيات الفردية، وإلاّ فقد الإذن مضمونه وحاد عن الشرعية، وانقلبت العلاقة بين الحرية الفردية كحق والتفتيش كقيّد، فكما زاد التخصيص في إذن التفتيش كلما تقلص دور الاستثناء لصالح القاعدة.

المطلب الثاني: متطلبات التحديد الكافي لمحل التفتيش

سبق أن توصلنا إلى أن المشروعية الإجرائية توجب تحديد منطقة معينة ضمن البيئة الرقمية كمحل للتفتيش، وهذه النتيجة تثير لدينا نقطتين، الأولى تتعلق بالمعالجة القضائية لمتطلبات التحديد الكافي لمحل التفتيش(فرع أول) والثانية تتعلق بمدى كفاية هذه المتطلبات في رسم نطاق التفتيش(فرع ثاني).

الفرع الأول: المعالجة القضائية لمتطلبات التحديد الكافي لمحل التفتيش

لكون المحكمة العليا الفيدرالية لم تحن بعد أمامها الفرصة للتعرض لموضوع متطلبات التحديد الكافي لمحل التفتيش المعلوماتي وأثر إغفالها على الدليل الجنائي المستمد من هذا الأجراء، فإن هذا القيد الإجرائي حتى الآن لا يزال يُنظر إليه في إطار المنظور التقليدي، ما فتح المجال للاجتهاد القضائي الذي أبدى انقساما واضحا بين متشدد يرجح اعتبارات الشرعية ويتمسك بالتطبيق الصارم للقاعدة الدستورية، وبين متساهل يراعي متطلبات الفعالية مدفوعا بصعوبة الوفاء بمتطلبات التخصيص الدقيق لهذه البيانات وسط هذا الكم الهائل من البيانات.

ويتجه القضاء الأمريكي في غالبيته إلى تجنب التوسّع في تطبيق هذه القاعدة بسبب صعوبة وصف المكان المراد تفتيشه وتعذر تحديد الوصف الدقيق للبيانات التي يحتويها وسيط التخزين، لذا غالبا ما يتم وصف موضوع التفتيش بمصطلحات مرتبطة بالجريمة الجاري التحقيق فيها، ففي قضية *United States v. Campos* أيّدت الدائرة الفيدرالية التاسعة صحة التفتيش بموجب إذن لا يتضمن سوى الإشارة إلى مواد تتصل مباشرة بالصور الداعرة للأطفال، وهذا التّوجه أيدته الدائرة العاشرة في قضية *United States v. Reyes* وعلّلت قرارها بأنّه: "في عصر التّكنولوجيا الحديثة والتوافر التجاري لأشكال مختلفة من الأشياء، من غير المتوقّع أن تصف الأذون بدقّة الشّكل الذي ستتخذه السجلات، وأن ضبط نوع معيّن من العناصر التي تدخل ضمن الأشياء المحددة في الإذن لا تشكل تفتيشا عاما غير مسموح به، فالإذن الذي يجيز ضبط وثائق معينة يأذن أيضا بتفتيش حاوية يُحتمل أن تحتوي على تلك الوثائق"[(10)]، إذ الضبطية القضائية لا تحتاج إلى إتّباع هذا النّهج في كل قضية لأن المراجعة القضائية لأذون التفتيش ذات طبيعة عقلانية وعملية أكثر من كونها ذات بعد تقني ُبناء على ذلك، فإنّ ما يهم هو جوهر الأدلة وليس شكلها [(11)].

في حين تكشف الاجتهادات القضائية الحديثة ميلا نحو التمسك بهذه القاعدة، ولو تعلق الأمر بمحاربة الجريمة في أخطر صورها، ففي قرار حديث لها قررت المحكمة العليا بولاية نيويورك في قضية *People v. Covlin* بطلان الأدلة المعلوماتية في جريمة توبع فيها المتهم بقتل زوجته، معتبرة أن بعض الأذون الصادرة في القضية لا تفي بمعايير"التحديد الكافية" وأن لغة

الإذن وردت عامة وسمحت بتفتيش أي نوع محتمل من السجلات أو الوسائط الإلكترونية أو أي شيء على هاتف المتهم [12].

الفرع الثاني: مدى كفاية متطلبات التحديد الكافي لمحل التفتيش في تضييق نطاقه

في إطار تقييمه للدور الوقائي للقاعدة محل البحث يطرح الفقه تساؤلات تزيد من عمق الإشكالية الرئيسية، وذلك في معرض نقده لها، فيما إذا كان تحديد البيانات التي يتعين ضبطها يمكن أن يكون ضيقا بما فيه الكفاية؟ وهل يمكن فعلا التوصل إلى تحديد نهائي لمكان تواجد أدلة معلوماتية معينة (إن وجدت) [13] ؟ وبالتالي الحد من امتداد عمليات التفتيش بقصر هذا الإجراء على تلك الأماكن أو التطبيقات الموجودة على أجهزة التخزين الرقمية فقط؟

والإشكالية في هذا الصدد عملية بحتة، ففي الحالة التي لا ينجح فيها التفتيش الضيق في الوصول الى الدليل المحدد في إذن التفتيش، فإنّ ذلك لا يحقق اليّقين بإنعدام الدليل فعلا بما يوجب حتما التوسّع في التفتيش باستكشاف كلّ مكان على محرك الأقراص الصلبة حيث يمكن العثور على الأدلة أو التحقق من انعدامها[14]، وفي نظرنا فإن هذه الحالة تعتبر من بين أبرز مظاهرا التعارض بين الاعتبارات القانونية والاعتبارات العملية للقاعدة، فالتمسك بتطبيقها الجامد يؤدي إلى شلل عملية التفتيش، وتجاوزها بهذا الشكل يحدث انتهكا غير معقول للحريات الفردية.

لذا يجمع الفقه على تراجع دور القاعدة في البيئة المعلوماتية بسبب حجم المساحة المراد تفتيشها وكمية البيانات المخزنة بداخلها، ففي الحيز المادي يحدد هذا الشرط نطاق التفتيش بمكان معيّن كالمنزل أو الشقة غير أنّه في حالات تفتيش نظم المعلومات يمكن لشقة واحدة أن تحتوي على عدة أجهزة للتخزين الإلكتروني، والتي بدورها قد تحتوي على أدلة معلوماتية يمكن أن تكون مخبّأة في أيّ مكان على الأقراص الصلبة دون القدرة على تحديد مكان تواجدها مسبقا، بما يستتبع الاطّلاع حتما على أي مكان على الأجهزة، وهكذا يصبح تفتيش المنظومة المعلوماتية معادلا لتفتيش مدينة بأسرها بدلا من منزل فردي، فشرط التحديد في الإذن تقلص دوره في الحد من امتداد عمليات تفتيش نظم المعلومات وقد بات ذلك أكثر وضوحا اليوم نظرا للقدرات التخزينية الكبيرة للحواسيب[15]، لذا عادة ما يجيز القضاء للضبطية القضائية القيام بتفتيش كميات هائلة من البيانات للعثور على"إبرة في كومة قش" فالإفتراض بكون الإذن بالتفتيش من شأنه أن يحدد بتفصيل كبير ما هي الملفات أو التطبيقات التي يمكن للشرطة تفتيشها سيكون افتراضا خاطئا [16].

ورغم وجاهة النقد الموجه للقاعدة، فإنّنا نتحفظ عن المغالاة فيه والمطالبة بالتخلي عن القاعدة في مرحلة التفتيش المادي وجعلها طليقة من غير قيد[17]، أو اعتماد منظور مادي لمحل

التفتيش بشكل مطلق[18]، لأنّ ذلك يفتح باب التوسّع الخطير في امتداد التفتيش ويمنح الضبطية القضائية سلطة غير محدودة فتتوسع عبر الملفات البريئة وفقا لرؤيتها، ومن هذا المنطلق لا يقبل تطبيقا للقواعد العامة أن يجيز الإذن القيام بتفتيش عام لجميع أجهزة التخزين الرقمية التّي يُعثر عليها بحوزة المتّهم أو بمقّر إقامته، لأنّ التفتيش مشروع في نطاق الغايّة منه، ومراعاة لمبدأ التناسب نرى الإصرار على هذا القيّد وعلى وجه التحديد في المرحلة الثانية، منعا من التغول في استعمال هذه السلطة، ولو كان في تطبيقها ما يناهض متطلبات الفعالية، لأنّه لا قيمة للحقيقة التّي يتم التّوصل إليها على مذابح الحرية، فالهيئة الاجتماعية– التي تعتبر مصلحتها أساس مشروعية التفتيش– لا يضيرها إفلات مجرم، بقدر ما يهدم أواصرها تفتيش جنائي على درجة من الشمولية والتوسع يكشف عورات أفرادها وينتهك أسرارهم.

على أن تمسكنا بالقاعدة لا ينكر حقيقة فشلها في إقامة توازن بين هذه المتطلبات المتعارضة، فبينما تعتبر بمثابة سياج مانع من امتداد التفتيش من الناحية النظرية، فإن التجربة العملية كشفت أن متطلبات الوصول إلى الدليل المعلوماتي تفرض في كثير من الأحيان تجاوز ما تأذن به القاعدة ذاتها، وكما رأينا فقد اختار القضاء التضحية بالحرية الفردية في سبيل استرداد ما يستهدفه التفتيش، فكيف يمكن المحافظة على حدود التفتيش التي يفرضها الاذن القضائي أثناء تنفيذه؟ سؤال تجيب عنه القاعدة التّي نتولى معالجتها في المبحث الثاني.

المبحث الثاني: ضوابط عملية تفتيش المنظومة المعلوماتية

ما هي القيود التي يمكن فرضها مسبقا على عملية تنفيذ التفتيش على نحو يسمح بالتوصل إلى البيانات المجرّمة دون تجاوز نطاق الإذن؟ في أي مرحلة تفرض هذه القيود، في مرحلة التفتيش المادي؟ أم في مرحلة تفتيش المنظومة المعلوماتية؟ أم خلال مرحلة ما بعد التفتيش؟ إنّ طرح كل هذه التساؤلات على بساط البحث يفرض علينا أن نتناول هذه القاعدة من حيث مدلولها (مطلب أول) ثم نعكف على تقييمها (مطلب ثاني).

المطلب الأول: قاعدة لزوم تحديد منهجية تفتيش المنظومة المعلوماتية

توصلنا إلى أن قاعدة لزوم تحديد محل التفتيش تحقق هدفها في سياق التفتيش التقليدي، حيث يفرض البعد المادي للدليل بشكل طبيعي نطاق المكان الذي يجري تفتيشه، بينما غياب هذه الحدود في البيئة الرقمية يفقدها قيمتها، ما حذا بالقضاء إلى إرساء قاعدة أخرى تضمن عدم تجاوز الغاية من التفتيش عند التنفيذ، لذا رأينا ضرورة التعرض لمفهومها (فرع أول) ومبرّراتها (فرع ثاني).

الفرع الأول: مفهوم قاعدة لزوم تحديد منهجية تفتيش المنظومة المعلوماتية

لقد قد أدّى الاختّلاف النّوعي بين الأدلة المعلوماتية والأدلة المادية إلى قيّام جانب من القضاء والفقه للمطالبة بإتّباع نهج خاص في تنفيذ إذن تفتيش المنظومة المعلوماتية بتبنّى فكرة ذاتّية هذا الإجراء بشكل كامل، من خلال تقيّيد عملية التفتيش بقيود مسبقة تعرض على القضاء للموافقة عليها، وقد أُصطُلح على تسميتها بمنهجية التفتيش[19]، ويقصد بها إلزام الضبطية القضائية بأن تشرح للقاضي المختص خطة تنفيذ التفتيش، مع مطالبتهم بتبريّرها كشرط مسبق لإصدار إذن يجيز ذلك، إبتغاء تقليل المخاطر المتزايدة على الحق في الخصوصية لأنها تجعل التفتيش أكثر تحديدا، وبذات الوقت تساعد القضاء على مراقبة عمل الضبطية القضائية التي يتعيّن عليها تكيّيف تفتيشها مع البيانات المطلوبة[20].

وقد تباينت هذه القيود تباينا واضحا بين الجهات القضائية، وبشكل عام قسّمها الفقه إلى أربعة أصناف، القيود التي تحد من عملية الضبط في مرحلة التفتيش المادي، والشروط التي تحد من النطاق الزمني لتفتيش المنظومة المعلوماتية، والشروط المتعلقة بكيفية إجراء مرحلة تفتيش المنظومة المعلوماتية والظروف التي ينبغي فيها رد المضبوطات لمالكيها، ويضرب الفقه أمثلة عن منهجيات التفتيش التّي تحقق هذه الغاية، ومن بينها البحث التلقائي باستخدام الكلمات الرئيسية وهي طريقة مفيدة بشكل خاص عندما يركز الاستعلام على مستندات محددة وتكون اللغة المستخدمة متوقعة نسبياً، فعلى سبيل المثال تقوم عمليات البحث عن الكلمات الرئيسية بالعثور على المستندات التي تتضمن فردًا معينًا أو تاريخًا محددا، وهناك برامج أخرى تسمح باستخدام عبارات أو مفاهيم معينّة ومن ثم تحدّد كلّ وثيقة تحتوي على معلومات ذات صلة بتلك البنّود، بما يُمكّن من قصر نطاق التفتيش على تلك المستندات التّي تحتوي على بيانات مرتبطة بتلك العبارات أو المفاهيم بدلاً من فتح كافّة الملفات والاطّلاع على محتوى كل وثيقة [21].

وقد تأكد التطبيق القضائي لهذه القاعدة محل البحث لأول مرة أمام جهة قضائية استئنافية سنة 2010 وكان ذلك من قبل الدائرة التاسعة في قضية *United States v. Comprehensive Drug Testing* عندما واجهت نفس التّحدي مجددا، وهو اختلاط البيانات وتعذر فرزها في الموقع مع إستحالة الوصول إليها من غير امتداد التفتيش إلى عدد كبير من المعلومات البريئة، حيث خلصت في قرارها إلى أنّه مع التّسليم بكون الضبط الموسّع هو جزء لا يتجزأ من عملية التفتيش الإلكرتوني، فإنّه لأجل تحقيق التّوازن الصحيح بين مصلحة الحكومة في التطبيق الفعّال للقانون وحق الأفراد في التّحرر من عمليات التفتيش غير المعقولة، وجب اعتماد قاعدة *Tamura* بخصوص إشكالية الضبط الموسّع، أما بشأن مرحلة التفتيش الإلكرتوني

فإنها قرّرت خمسة قيود جديدة تضيق بشكل كبير من نطاق امتداد التفتيش بحيث اشترطت للموافقة على إذن التفتيش، أن تتنازل الحكومة عن الاعتماد على مبدأ الرؤية الكاملة (*the plain view doctrine*)، وأوجبت أن يتم فرز البيانات من قبل طرف مستقل فإن تمت هذه العملية من قبل متخصص حكومي وجب عليه عدم الكشف سوى عن البيانات المستهدفة، واشترطت أيضا أن تبيّن الإفادة الخطية لطب الإذن عن المخاطر الفعلية التّي قد تفضي إلى تدمير المعلومات، كما شدّدت على ضرورة تقديم منهجية تفتيش مصممًة خصيصا للكشف فقط عن المعلومات التي لها سبب محتمل، وأخيرا أكدت على ضرورة محو البيانات التي لا تستجيب للإذن القضائي دون استعراض محتواها[22].

وهذا القرار يعتبر محاولة غير مسبوقة لوضع قواعد واضحة لحدود تفتيش نظم المعلومات، إذ قيد مرحلة التفتيش المادي بوجوب الكشف عن المخاطر الفعلية لتدمير البيانات في حالة معينة، بدلا من الاعتماد على المخاطر العامة لتبرير الضبط العرضي الشامل، لأن تفتيش المنظومة المعلوماتية خارج الموقع قد لا يكون صحيحا دائما، بسبب التّطورات التكنولوجية التّي أوجدت برامج متطورة تجعل التفتيش في الموقع ممكنا، وقيد المرحلة الثانية بحصر نطاق التفتيش عن طريق إستراتيجية تفتيش تستبعد البيانات الخارجة عن نطاق الإذن من المراجعة، كما قيد مرحلة ما بعد التفتيش بوجوب رد المضبوطات المادية أما في حالة الضبط المعلوماتي، فقد تقرر حذف هذه البيانات مع حضر استخدم الأدلة الجنائية المكتشفة بشكل عرضي.

وهكذا استحدث القضاء الأمريكي مفاهيم إجرائية جديدة يتفاعل فيها هذا الإجراء مع البيئة الرقمية، وأهمها البطلان كجزاء يلحق التفتيش والدليل المستمد منه متى وقع بالمخالفة للشروط التي تقيد تنفيذ عملية التفتيش، بل يتحقق البطلان في مرحلة سابقة عن العثور على الدليل، ويطلق الفقه على هذا المفهوم الجديد للبطلان بالبطلان الاستباقي "*preemptive suppression*"[23]، وفي اعتقادنا فإن هذا المصطلح يعكس الهدف الذي تتوخاه القاعدة بغرض تنّجب انتهاك الحق في الخصوصية، عن طريق إخطار الحكومة مسبقا بلزوم التقيد بحدود الإذن وما فرضه من قيود تحت طائلة بطلان التفتيش، لحملها على الالتزام بالمشروعية التي باتت تسمد من الإذن ذاته، وإذا كان الوضع الطبيعي هو إنهاء الضبط برد المضبوطات للمالك أو الحائز بحسب الأوضاع، فإنّ الضبط المعلوماتي يستلزم محوّ البيانات المضبوطة وهو ما بات يعرف بالحق في الحذف "*The Right to Delete*".

الفرع الثاني: مبررات قاعدة لزوم تحديد منهجية تنفيذ تفتيش المنظومة المعلوماتية

إنّ السؤال الذّي يفرض نفسه عند بحث مبرّرات هذه القاعدة يتعلق مضمونه ببحث منطق التّكامل بين قاعدة لزوم محل التفتيش في الإذن وقاعدة تقييد عملية تنفيذه؟ كيف يمكن لهذه القاعدة الحديثة تحديد المنطقة التي يجري تفشيها في البيئة الرقمية للوصول إلى مستهدف التفتيش دون استعراض البيانات البريئة؟

بتبرير يمتاز بكثير من الدقة تعرضت المحكمة العليا في ماساتشوستس إلى هذا التساؤل وذلك في قضية *Commonwealth v. Keown*، حيث أكدت أنّه في سياق التفتيش الرقمي تتضافر الجهود بين القاضي والقائم بالتفتيش لأجل تحديد المكان الذي سيجري تفتيشه، حيث يتكامل السؤال "المتعلق بكيفية التفتيش" مع مسألة "ما سيجري التفتيش عنه"، لأنّ المفهوم المادي للحدود يصبح مجازيا ومن ثّم فإن البروتوكولات المسبقة التي تحدد كيفيّة القيام بالتفتيش هي الوسيلة الوحيدة لوصف موقع الأماكن والملفات الرقمية التّي سيتم تفتيشها على وجه التحديد[24].

بينما أضافت المحكمة العليا في ولاية فيرمونت مظهرا آخر من مظاهر التلازم بين القاعدتين في معرض فصلها في قضية *Commonwealth v. Keown*، موضّحة بأن القيّود المسبقة هي وسيلة لضمان شرط التحديد في سياق التفتيش التقليدي، حيث يتم قصر التفتيش على جزء فقط مما هو مطلوب، كغرفة بدلاً من منزل بأكمله، أو صناديق تحتوي على علامات معينة بدلاً من مستودع، وكذلك تعتبر القيود المسبقة مقبولة تمامًا في العالم الرقمي، "إذ لا يتم الوصول إلى معلومات معينة من خلال الممرات والأدراج، بل من خلال الأوامر والاستعلامات الموجهة لأجهزة الحاسوب، فعند محاولة وصف الأشياء التي يجب ضبطها، لن تكون هنّاك طريقة لتحديد أشياء محددة أو مساحات معيّنة عن طريق وصف الإحداثيات المادية الخاصة بها ولكن عن طريق وصف كيفيّة تحديد موقعها نتيجة لذلك، فإنّه في العديد من الحالات تكون الطريقة الوحيدة لتحديد منطقة معينّة من الحاسوب هي تحديد كيفية التفتيش"[25].

ومن بين الحجج التّي يستند إليها الاتجاه المساند لهذه القاعدة، أنّ تقييد عملية تنفيذ التفتيش من شأنها الحيلولة دون حصول تجاوز من قبل الضبطية القضائية وإخضاع نشاطها لرقابة قضائية لصيقة، فهي لا تمنع التوسّع غير المعقول للتفتيش فحسب، بل إنّها تعيد أيضًا إحياء دور القاضي كحكم محايد مسؤول عن تحديد مدى دستورية سلوك الضبطية القضائية، وبدون منهجية التفتيش تتمتع هذه الأخيرة بسلطة تقديرية واسعة لتحديد معايير تفتيش حسب ما يتراءى لها، فإذا سُمح للضبطية القضائية بفحص محتويات كلّ ملف بشكل دقيق من

أجل تحديد ما إذا كان هناك مستند معيّن يدخل ضمن نطاق الإذن بالضبط أم لا، فإن حماية الحريات الفردية بهذا الشكل تصبح خاضعة لتقدير الضبطية القضائية[26].

وفي تقديرنا فإنّ القضاء الأمريكي قد خطى بمقتضى هذا الاجتهاد القضائي خطوات أخرى في اتجاه التضييق من نطاق التفتيش، وأهم ما يجعلنا نؤيد هذه القاعدة هو المفهوم الجديد الذي أصبغه على "مبدأ عدم تجاوز الغاية من التفتيش"، فبعد أن كان هذا المبدأ من الضمانات الموضوعية يخضع للمراجعة القضائية اللاّحقة، التفت القضاء إلى التّداعيات السلبية التي يخلفها التوسّع في التفتيش على الهيئة الاجتماعيّة، وهي الضّرورة التّي حذت به إلى اعتباره أيضا من الضمانات الشّكلية التي تحقق الدور للوقائي للحماية، من خلال فرض قيود ضمن إذن التفتيش تضمن تنفيذه في حدود الغاية منه، فأصبحت هذه الضمانة ذات وجهة شكلية وموضوعية.

المطلب الثاني: تقييم قاعدة لزوم تحديد منهجية تنفيذ التفتيش وبدائلها

على الرّغم من أهمّيّة هذه القاعدة إلا أنها لقيت معارضة شدّيدة من الفقه وترددا ملحوظا من قبل القضاء في تطبيقها، بما يفرض علينا التّطرق إلى هذّه الانتقادات وتقيّيمها (فرع أول) والتعرض إلى بدائلها (فرع ثاني).

الفرع الأول: تقييم قاعدة لزوم تحديد منهجية تنفيذ التفتيش

إنّ معالجة التّقييم الموضوعي لهذه القاعدة لا يتم سوى في إطار دراسة أوجه النقد الموجهة إليها، ووضعه في إطاره السليم، مقارنة بما يتمسك به المؤيدون لها، وعموما يجمع الاتجاه المناهض لهذه القاعدة من الفقه والقضاء على نقدها من زاويتين قانونية وأخرى واقعية.

فمن ناحية، يرى المعارضون أنّه استنادا إلى التعديل الدستوري الرابع فإنّ فرض برتوكولات التفتيش يعتبر تطبيق قضائي غير دستوري، بحجة أن القضاة لا يتمتّعون بالسلطة القانونية التّي تؤهّلهم لفرضها، فدور قاضي التحقيق عند إصدار أذون الضبط والتفتيش يقتصر فقط على تقدير مدى تحقق شرطي السبب المحتمل وعنصر التحديد في الإفادة الخطية، دون أن يكون له السلطة في رسم حدود كيفيه تنفيذ هذه الأذون، لأنّ تقدير مدى معقوليتها يخضع للمراجعة القضائية اللاحقة بدلا من المراجعة القضائية السابقة على التنفيذ، كما أنّ هذا القيد ليس له أثر قانوني لأنّ تقدير مدى دستورية التفتيش تتوقف على ما إذا كان تنفيذ التفتيش معقولًا استنادا للحكم الصادر بعد التّنفيذ، دون اعتبار لما إذا كانت الحكومة قد امتثلت فعلا للقيّود المسبقة أم لا[27].

وهو ما قررته الدائرة التاسعة في قضية *United States v. Schesso* فصلا في قضية إستغلال الأطفال في المواد الإباحية، حيث رفضت طلب بطلان الأدلة المعلوماتية التّي تم استردادها بموجب إذن قضائي واسع النطاق وخاليا من منهجية تنفيذه، أجاز ضبط وتفتيش حاسوب المتهم وجميع أجهزته الرقمية، وخلصت المحكمة إلى أنّ برتوكولات التفتيش لا يفرضها الدستور كما لا يمكن معاتبة الضبطية القضائية لعدم إتباع أساليب غير ملزمة لهم[28]، وبموجب هذا القرار تكون الدائرة التاسعة قد تراجعت عن الطابع الإلزامي لاجتهادها بأن جعلت تطبيق القاعدة يخضع للسلطة التقديرية للقضاة بدلا من الطابع الإلزامي الذّي كانت تتمتع به.

وفي هذا الصدد يرى الفقيه بول أوهم أنّ القضاة ليس لهم فقط السلطة القانونية لفرض هذه القيود بل يقع واجب عليهم القيام بذلك، معتبرا إياه بمثابة ضمان إجرائي يحل محل السبب المحتمل وعنصر التحديد المفتقدين في أذون التفتيش المعلوماتي وليس فقط لضمان التنفيذ المعقول وذلك في كل حالة تفتيش معلوماتي تقريبًا [29]، ذلك ما خلصت إليه المحكمة العليا في فيرمونت في حكمها المشار إليه سابقا، مؤكدة أنّه لا يوجد في التعديل الدستوري الرابع ما يمنع القضاة من فرض شروط مسبقة تضع حدودا لنطاق التفتيش طالما أنّ هذه القيود تسعى لتحقيق هدف دستوري فما ينبغي على القضاء التّأكد منه لا يتوقف عند مجّرد قيام سبّب محتمل للاعتقاد بأن التفتيش قد يفضي إلى كشف الأدلة الجنائية، بل ينبغي التّأكد من قيّام الأسباب المبرّرة لانتّهاك حقّ الفرد في الخصوصية، فعلى الرغّم من أن القانون أجاز للأفراد الحق في الطعن في التفتيش بعد تنفيذه، فإنّ المراجعة اللاّحقة لا تحقق الغرض الذّي لأجله تم تقنين حماية هذا الحق.

من ناحية أخرى يرى المعارضون أن هذه القاعدة بمثابة قيد يحول دون فعالية التفتيش، لذاعارضت وزارة العدل الأمريكية بشدة اعتماد هذا القيد الإجرائي واصفة إياه بكونه "مرهق" و"غير مجدي" بل و"غير ضروري" يؤدي إلى إعاقة سلطة الحكومة في اكتشاف الأدلة المعلوماتية، لأنّ إجراءات التحليل الحاسوبي الشرعي تتطلب من القائم بالتحليل الاعتماد على حدسه واتخاذ الخطوات المناسبة بناء على الحقائق التي تواجهه وقت التحليل[30].

ولقد لقيت هذه الحجة تأيدا واسع النطاق من قبل القضاء ومن تطبيقات ذلك ما أكدته الدائرة العاشرة في قضية *United States v. Burgess* حين أبدت رفضا شديدا لهذا القيد وخلصت إلى القول بأنه: "من غير الواقعي توقع وجود إذن قضائي يقيد نطاق تفتيش المنظومة المعلوماتية عن طريق اسم المجلد أو اسم الملف أو اسم الامتداد أو محاولة هيكلة أساليب التفتيش بشكل مسبق، فهذه العملية يجب أن تظل ديناميكية ومن غير المعقول أن يحاول إذن التفتيش تقييد آليات التفتيش بفرض مثل هذه الحدود التّي من شأنها أن تقيّد أهداف

التفتيش المشروعة بدون مبرّر...من غير المعقول أن يكون هناك إذن بالتفتيش يضيق عملية البحث بالتفتيش عن الأدلة فقط ضمن "خزانات ملفات في الطابق السفلي" أو "ملف المجلدات المسماة بالعملاء"، لذلك لا يوجد سبب للحد من نطاق عمليات التفتيش الإلكتروني"[31].

رغم ذلك ثمة محاولات قضائية لوضع هذا النقد في إطاره الحقيقي، بحيث يرى القاضي جون فاسيولا أنّ هذه القيود لا تشكل نهائيا إعاقة غير مبررة للكشف عن الجريمة أو الحد من قدرة الحكومة على إجراء تفتيش بشكل ديناميكي لسببين. أولا، تستطيع الحكومة دائما الرجوع إلى المحكمة لتقديم طلب آخر للحصول على إذن إضافي حسب ما تستدعيه الحاجة وثانيا، لا يقتضي الطلب سوى توضيح أن بعض عمليات التفتيش تتطلب تقنيات إضافية، وأن ما هو مقترح هو مجرّد ما تعتزم الحكومة القيام به وقت تقديم هذا الطلب، استنادا إلى المعرفة التي اكتسبتها أثناء تفتيش هذه الأجهزة، وفي ضوء البيانات المحددة التي تسعى إلى ضبطها[32].

وذات التبرير اعتمده زميله دافيد واكس مضيفا أنه سعيا لتحقيق توازن بين حق الفرد في الخصوصية وقدرة الحكومة على التحقيق في الجرائم بفعالية وكفاءة فإنه بالإمكان دائما الحصول على إذن إضافي بناء على عرض لاحق تتقدم به هذه الأخيرة وتبيِّن من خلاله ما يستدعي ذلك، أفضل من الموافقة على الطلب الأول الذي يمنح الحكومة سلطة غير دستورية واسعة النطاق في إجراء التفتيش[33].

ومن أهم الاعتراضات التي يسوقها المناهضون لهذا القيد الإجرائي، أنّه لا يمكن تحديد محتويات أيّ مستند حاسوبي إلاّ من خلال فتحه وفحصه باستعراض ما تضمنه، وقد تأكد ذلك في قضية *United States v. Gray*، أين رفضت المحكمة طلب بطلان التفتيش الذّي كان أكثر امتدادا عبر ملفات لا صلة لها بالتحقيق رغم أن الفحص تم باستعمال برنامج حاسوبي يضمن قصر التفتيش على الملف المستهدف، وأشارت المحكمة إلى أنّه بالرغم من وجوب توخي الحذر لضمان عدم التوسع الكبير في التفتيش، فإنّ هذه العملية لا تقل دستورية عن عمليات التفتيش في السجلات المادية، فعند البحث عن العناصر المدرجة في الاذن القضائي يجوز فحص جميع ملفات المتهم لتحديد ما إذا كانت تحتوي على عناصر تدخل في نطاق الاذن القضائي أم لا [34].

في تأييدها لهذا الوقف المتساهل عبّرت الدائرة العاشرة عن موقفها من عدم جدوى منهجية التفتيش صراحة في قضية *United States v. Burgess* مصرحة "بشكل عام قد لا يمنح بروتوكول التفتيش سوى أوهام لحماية الحق في الخصوصية، خاصةً عندما يكون هدف التفتيش هو ملفات الصور، ففي الحالة التي يكشف التفتيش الإلكتروني- الذي يستهدف أصلا التنقيب عن أدلة متعلقة بجريمة المخدرات- عن أسماء ملفات تشير إلى مواد إباحية للقصر، لا يُطلب

من الضابط سوى الحصول على إذن آخر لمتابعة التفتيش عنها، مما يؤدي إلى استعراض أغلب الملفات للتّأكد من أنها لا تحمل عنوانا مظلّلا، وفي النّهاية سيتم الكشف عن المواد الإباحية، فالفرق الوحيد هو أنّه سيتم اكتشافها لاحقا، وليس في وقت سابق، خاصة في حالة التفتيش عن ملفات الصور، والتّي يمكن دفنها في أيّ مكان على وسيط التّخزين".

وعلى هذا الاعتراض يرد المؤيدون بأنّ هذه التّوجه القضائي يعبر عن فهم خاطئ للغرض الذّي لأجله تصمم برتوكولات التفتيش، إذ هي لا تحدد المعلومات التّي يحتويها المستند وليس ذلك هو الهدف من فرضها، فهي ببساطة أساليب ترمي إلى استبعاد المعلومات التّي لا صلة لها بالتحقيق من نطاق التفتيش، فعلى سبيل المثال، إذا حددّت الضبطية القضائية سببا محتملا للاعتقاد بأن حاسوبا معينا يحتوي على صور سرقة حدثت بتاريخ ما، فقد تستخدم المحكمة البيانات الوصفية لوضع بروتوكول تفتيش يحد من نطاق التفتيش بقصره على المستندات التي تم إنشاؤها بعد تاريخ وقوع الجريمة فلا يمتد التفتيش إلى غيرها من البيانات[35].

لعلّ أهم اعتراض وجه لهذه القاعدة من قبل الفقه، هو نقص الخبرة الفنية لدى القضاة في فرض منهجية تفتيش معينة، إذ تعتمد القدرة على صياغة إستراتيجية تفتيش مفيدة والموافقة عليها على الخبرة التقنية للقضاة، غير أن هؤلاء غير مؤهلين بشكل كاف لتقييم ما إذا كان بروتوكول تفتيش معيّن هو أفضل الطرق وأكثرها استهدافا لتحديد مكان الأدلة المخزنة على أجهزة التخزين الرقمية أم لا، ويرى المؤيدون، أن هذه الانتقادات المعبر عنها منذ عقد مضى بدأت تتراجع أهميتها مع مرور الوقت، ببروز قضاة قادرين على التعامل مع بروتوكولات تفتيش الأكثر تعقيدا، علاوة على ذلك، فانّه يمكن للقضاة الذّين يفتقرون إلى المعرفة الضّرورية المطالبة من الضبطية القضائية أو النيابة العامة تقديم بروتوكولات تفتيش مقترحة كما يمكن لوزارة العدل وضع برتوكولات نموذجية لوجود موارد بشرية مؤهلة لذلك [36]، وقد درج القضاة على اللّجوء إلى هذا الحل [37].

بالرغم مرور ما يقارب عشرة سنوات على صدور هذا الاجتهاد القضائي لا يزال القضاء الأمريكي يبدي ترددا ملحوظا حيال الالتزام بهذا القيد الاجرائي وفي تقديرنا فإنّ هذه القاعدة لا غنى عنها لاحترام التعديل الدستوري الرابع، فهناك تكامل بين المراجعة القضائية السابقة والمراجعة القضائية اللاّحقة ولا تلغي إحداهما الأخرى فالأولى هدفها تقدير مدى دستورية التفتيش المقترح كشرط مسبق للإذن به والثانية هدفها مدى احترام حدود التفتيش المأذون به عند التنفيذ، لأن مشروعية الإذن لا تنفي عدم معقولية تنفيذه، على أن المراجعة المسبقة تبدو في نظرنا أبلغ أهمية، لأنها تعبر عن تحقيق أقصى مدى من الشرعية فهي بمثابة خط دفاع أولي ضد أي مسّاس بهذا الحق بل هي سيّاج لحمايته، فإذا ما تم تسور هذا السياج

فقد الحق قيمته ويظهر ذلك بشكل جلي في حالة ما إذا كان التفتيش أكثر توسعا وامتداد عبر ملفات الغير الذي تواصوا مع المتهم دون أن تربطهم أي رابطة بالجريمة أو في حالة انتهاء التفتيش بعدم الجدوى أين يظهر الفارق البليغ بين ما يحققه الإشراف القضائي السابق عن التنفيذ، وما يمكن أن يستدركه الإشراف القضائي اللاّحق وهو ما عبرنا عليه سابقا بالمفهوم المزدوج لمبدأ عدم تجاوز الغاية من التفتيش كضمانة شكلية وموضوعية خلع عليها القضاء الأمريكي قيمة دستورية.

المطلب الثاني: بدائل قاعدة لزوم تحديد منهجية تنفيذ التفتيش

وفي ضوء النقد الموجه للقاعدة، خاصة النقد المبني على مناقضتها لمتطلبات الفعالية واحتمال ضياع الأدلة المعلوماتية جراء شلل عملية التفتيش بحكم القيود الضيقة التي تفرض عليها، نادى الكثير من الفقه بعدم التوسع في تطبيقها مع الاكتفاء بالمراجعة القضائية اللاحقة لكل قضية على حدة لتقدير مدى معقولية تنفيذ التفتيش في نطاق الغاية منه، وأهم البدائل المقترحة لحد الآن من قبل الفقه الأمريكي هو النهج القائم على وضع حد لامتداد التفتيش المعلوماتي من خلال حضر استّخدام أي دليل جنائي يكتّشف خارج نطاق الاذن القضائي.

وفي نظر هذا الجانب من الفقه، فإّن هذه المقاربة من شأنها استعادة الحدود المطلوبة على نطاق الضبط بما يحافظ على فعالية عمليات التفتيش من خلال تزويد الحكومة بالسلطة اللازمة للتفتيش عن الأدلة المحددة في الاذن القضائي وضبطها ويؤدي بذات الوقت إلى تجنب صيرورة الاذن بالتفتيش عاما، بتقييد سلطة الحكومة في استغلال الأدلة المحدّدة في الاذن القضائي بشكل خاص [38].

وتقوم هذه المقاربة على ثلاثة أسئلة رئيسية. أولا، خلال مرحلة التفتيش المادي، ما هي حدود سلطة الضبطية القضائية في ضبط أجهزة التخزين المادية لتفتيشها لاحقا؟ ثانيا، أثناء مرحلة التفتيش الإلكتروني، ما هي حدود سلطة الضبطية القضائية في تحليل البيانات المخزنة على للوصول على الأدلة المطلوبة؟ وثالثا، بعد مرحلة التفتيش الإلكتروني ما هي حدود سلطة الضبطية القضائية في استخدام المعلومات المكتشفة أثناء مرحلة التفتيش الإلكتروني؟ [39].

بخصوص مرحلة التفتيش المادي، يرى هذا الجانب من الفقه أنّ كل من القانون والقضاء يسلمان في الوقت الراهن بضّرورة الضبط العرضي الشامل يليه إجراء تفتشيم المنظومة المعلوماتية لاحقا لأنّ وسائط التخزين الإلكترونية تحتوي على كميات كبيرة من المعلومات والتّي غالبا ما يكون من غير العملي مراجعتها في الموقع، لذا ينبغي عدم فرض أي قيود على هذه المرحلة رغم الاعتراف بتجاوز الضبط لحدود الإذن نظرا لعدم وجود أي بديل آخر[40]، والأمر كذلك بالنسبة لمرحلة تفتيش المنظومة المعلوماتية يبنغي تركها من غير قيد لعدم جدوى قاعدة

لزوم تحديد محل التفتيش في تضييق نطاقه ولعدم دستورية قاعدة تحديد منهجية تنفيذ التفتيش[41].

أما المرحلة الأخيرة، وهي مرحلة استخدام الأدلة، خلالها يتم فرض قيّود تمنع استخدام أي دليل جنائي خارج نطاق الإذن القضائي لكون الضبط الإجمالي في المرحلة الأولى هو ضبط معقول ومبرّر بضرورة تنفيذ الاذن القضائي، كما أنّ ضرّورة التحقيق تستوجب الاطّلاع حتما على الملفات البريئة في سياق التفتيش عن البيانات المستهدفة، بما يجعل الضبط الأولي والاطلاع اللاّحق ضروري لتجنّب جعل الإذن مجرد حبر على ورق، بيد أن الضبط المتواصل للبيانات التي لا تستجيب للإذن القضائي أو استخدامها لإثبات جرائم أخرى غير تلك التي استهدفت بإذن التفتيش يجعل الإذن عاما ويلغي تماما دور قاعدة لزوم تحديد مستهدف التفتيش في الاذن [42].

و قد تم تبني هذه المقاربة الفقهية مؤخرا من قبل المحكمة العليا في أوريغون وذلك في قضية *United States v. Mansor*، حيث أشارت المحكمة إلى أنّ هذا المذهب يشكل قاعدة من قواعد قبول الأدلة الجنائية فبينّما تسمح هذه القاعدة للحكومة بإجراء تفتيش معلوماتي واسع النطاق، فإنّها في نفس الوقت تحدّ من مقبولية الأدلة المتأتّية من هذا الإجراء بحيث تستبعد الأدلة التّي لا علاقة لها بالأسباب المحتّملة التي من أجلها صدر إذن التفتيش [43]، والحقيقة أن التكريس القضائي لهذه القاعدة يرجع إلى سابقة الدائرة الفيدرالية الثانية في قضية *United States v. Ganias* والتي أُقرت مظهرا جديدا من مظاهر تطبيق قاعدة استبعاد الأدلة غير المشروعية في سياق التفتيش المعلوماتي[44].

الواقع أنّ هذا البديل المقتّرح لا يتعلق أصلا بالهدف الوقائي الذي تتوخاه القاعدتين محل البحث بل يرمي إلى التخفيف من الضّرر اللاحق بالفرد جراء تفتيش يتجاوز الغاية منه باستعباد أي دليل جنائي لا يستهدفه التفتيش، ومن جهة أخرى فإن ترك مرحلتي التفتيش المادي وتفتيش المنظومة المعلوماتية من غير قيّد وإتاحة سلطة واسعة للضبطية القضائية بهذا الشكل هو أمر غير معقول تماما بل يناقض مقتضيات التعديل الدستوري الرابع ويؤدي إلى إهدار كافة الضمانات التي تقوم عليها نظرية التفتيش.

ما نخلص إليه في النّهاية أنّه وإلى غاية الوقت الراهن لا يوجد أيّ اقتراح فقهي أو اجتهاد قضائي نجح في إرساء قاعدة عامة –قابلة للتطبيق في كافة الظروف والوقائع– تكفل وضع حدود واضحة لنطاق التفتيش المعلوماتي فتطبيق قاعدة لزوم تحديد محل التفتيش في مرحلة التفتيش المادي يؤدي إلى طغيان عنصر الفعالية، بينما تطبيق هذه القاعدة في مرحلة تفتيش المنظومة المعلوماتية تحقق الشرعية، وبذات الوقت تفضي إلى شلل عملية التفتيش لأنّه

لا يمكن التنبؤ مسبقا بمكان تواجد الأدلة المعلوماتية قبل إجرائه بما يوجب الاطّلاع على أسرار الأفراد قبل التّوصل إلى الدليل المستهدف.

ومن ناحية أخرى، فإنّ التطبيق الصارم لقاعدة لزوم تحديد منهجية تنفيذ التفتيش هي الأخرى تفرض حدودا ضيقة على عملية تنفيذ هذا الاجراء خاصة إذا اقتصرت المنجهية على أسلوب واحد فقط، على نحو يناقض متطلبات الفعاليّة نتيجة لجوء المجرمين إلى إخفاء الملفات المجرّمة في أيّ مكان على وسيط التخزين الرقمي، مع جعل الملف البريء حجابا للملف المجرّم بإعطاء الملفات اسما مضلّلا أو امتداد خاطئا أو حمايتها بواسطة طرق التشفير، وهذا الذّي دفع بالقضاء إلى التردّد في تطبيقها، فضلا على ذلك فانّ المغالاة في الدفاع عن هذه القاعدة بتطبيقها الجامد، يجافي المنطق إذ كشف الواقع العملي أنّها جد مرهقة وتتطلب وقتا طويلا نتيجة المطالبة بأذون تفتيش جديدة في كل مرة تفشل فيها المنهجية المقترحة في استرداد الدليل المستهدف.

إن الجدال الذي دار حول حدود امتداد تفتيش المنظومة المعلوماتية إمّا أنّه يميل إلى ترجيع اعتبارات الفعاليّة بالدعوة إلى عدم وضع حدود لعملية التفتيش في مرحلتيه والاكتفاء فقط بتقييد استخدام الأدلة المكتشفة بشكل عرضي في مرحلة التفتيش الإلكتروني بحضر استغلال أي دليل جنائي خارج نطاق الاذن القضائي، وإمّا الالتزام المطلق بمبدأ الشرعية عن طريق تقييد حدود التفتيش في جميع مراحله، وفي ذلك إهدار للفعاليّة، لذا نعتقد أنه يجب اعتماد حل توفيقي وسط يتبنى كلا القاعدتين على نحو مرن يحقق التوفيق النسبي بين الاعتبارات القانونية والعملية.

خاتمة:

نخلص في نهاية البحث إلى ضرورة التركيز على أهم الملاحظات الختامية، نود لو أنّ بعضها يصبح محل اهتمام للمشرع العربي عند التفكير في إجراء أي تعديل تشريعي ينظم بصفة خاصة حدود امتداد التفتيش الجنائي المعلوماتي لتحقيق القدر الكافي من الضمانات الكفيلة بحفظ الحرية الفردية والتي تتلخص في مايلي:

أولا – تقتضي الشرعية الإجرائية ضرورة قصر نطاق تفتيش المنظومة المعلوماتية على محل معيّن منعا من التفتيش العشوائي العام، بالنص على وجوب استصدار إذن قضائي مسبق يحدد بدقة أجهزة التخزين الرقمية المراد ضبطها في مرحلة التفتيش المادي، والأدلة المعلوماتية المراد استردادها خلال مرحلة تفتيش المنظومة المعلوماتية، كل ذلك في ضوء طبيعة الجريمة الجاري التحقيق بشأنها.

ثانيا – مراعاةً لمبدأ التناسب، يجب أن يتضمن الإذن القضائي أساليب متعددةً لتنفيذ التفتيش والتي تعزم السلطة الإجرائية استخدامها للوصول إلى البيانات المستهدفة وعند فشلها في التوصل إلى الدليل الجنائي ينبغي الرجوع إلى القاضي المختص للحصول على إذن آخر في ضوء المعطيات المتحصل عليها إثر عملية التفتيش الأولى على أن تقدم هذه الجهة محضرا يثبت تسلسل إجراءات التفتيش المتَّبعة.

ثالثا – احتراما لمبدأ الغاية من التفتيش، يجب على السلطة القائمة بالتفتيش وقف التفتيش فورا بعد الوصول إلى الدليل الجنائي من غير استعراض باقي البيانات ولا يجوز لها استعمال أي دليل جنائي عرضي مكتشف أثناء مرحلة تفتيش المنظومة المعلوماتية باستثناء الأدلة المحددةً في الإذن القضائي.

رابعا – يجب النص على حق المتهم في المطالبة بالحذف الكلي للبيانات عند انتهاء عملية تفتيش المنظومة المعلوماتية بعدم الجدوى أو عند تقرير بطلانه وحقه في الحذف الجزئي للبيانات الخارجة نطاق الاذن القضائي بعد العثور على الدليل الجنائي المستهدف.

خامسا – يتعيّن اعتبار كافة الأدلة المعلوماتية التي يتم استردادها عن طريق توسيع نطاق التفتيش دون مراعاةً الحدود التي يفرضها الإذن القضائي سواء بتجاوز محل التفتيش أو بعدم التقيد بشروط تنفيذه باطلة ولا يمكن الاعتماد عليها.

قائمة المراجع:

أ- المراجع باللغة العربية:

1- عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب توصلا إلى الدليل الالكتروني في التحقيقات الجنائية – ترجمة ودراسة وتحقيق- الطبعة الثانية، دار النهضة العربية، مصر، 2006.

ب- المراجع باللغة الإنجليزية:

A-Books:

1. *H. Marshall Jarrett, Michael W. Bailie, Ed Hagen , Nathan Judish, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations , Computer Crime and Intellectual Property Section Criminal Division Published by office of Legal Education Executive office for United States Attorneys, 3d ed. (2009).*

B - Articles:

1. *Adam M. Gershowitz, The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches, Vanderbilt law review, Vol 69, (2016).*
2. *Christina M. Schuck, Note & Comment, A Search for the Caselaw to Support the Computer Search "Guidance" in United States v. Comprehensive Drug Testing, Lewis & Clark L. Rev,Vol 16, (2012).*

3. *Derek Haynes, Comment, Search Protocols: Establishing the Protections Mandated by the Fourth Amendment Against Unreasonable Searches and Seizures in the World of Electronic Evidence, Mc George Law Review, Vol 40, (2009).*
4. *Josh Goldfoot, the Physical Computer and the Fourth Amendment, Berkeley J. Crim. L. Vol 16, Issue 1, (2011).*
5. *Orin S. Kerr , Ex Ante Regulation of Computer Search and Seizure, Virginia Law Review, Vol 96, Issue 6, (2010).*
6. *Orin S. Kerr, Search Warrants in an Era of Digital Evidence, Mississippi Law Journal, Vol 75, Issue 1, (2005).*
7. *Orin S. Kerr, Searches and Seizures in a Digital World, Harvard Law Review, Vol 119, Issue 2, (2005).*
8. *Orin S. Kerr, Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data, Texas Tech Law Review, Vol 48, Issue 1, (2015).*
9. *Paul Ohm, Massive Hard Drives, General Warrants, and the Power of Magistrate Judges, Virginia Law Review, Vol 97, (2011).*
10. *Simpson, Bob, "Preemptive Suppression" Judges Claim the Right to Find Digital Evidence Inadmissible Before It Is Even Discovered," Journal of Digital Forensics, Security and Law, Vol 7, (2012).*
11. *Thomas K. Clancy, the Fourth Amendment Aspects of Computer Searches and Seizures, Miss. L.J, Vol 75, (2005).*

C - Web sites:

1. *www.casetext.com.*
2. *www.courtlistener.com.*
3. *www.law.justia.com.*
4. *www.leagle.com.*

الهوامش:

[1] – يرى جانب من الفقه الأمريكي أنّه يمكن النظر إلى وسائط التخزين من زاويتين داخلية وأخرى خارجية، فوفقا للمنظور الداخلي لوسيط التخزين الرقمي، فإنّ دعامة التخزين الرقمية تمثل مجموعة من البيانات مجمّعة ضمن ملفات حاسوبية أو وحدات أصغر كجدول البيانات، وأن هذه "الأشياء" مستقلة عن بعضها البعض وبذات الوقت منفصلة عن جهاز التخزين الرقمي والتي بدورها تبدو مثل "مكان" افتراضي يحتوي على تلك "الأشياء". بخلاف ذلك، فإنّ المنظور الخارجي لوسيط التخزين الرقمي لا يعتبر الملفات بمثابة "أشياء" على الإطلاق فهي لا تعدو أن تكون مجرد مجموعات من البيانات، مرتبطة بشكل يجعلها لا تنفصل عن وسيلة التخزين وهي بهذا المعنى ليست "مكانا" بل "شيئا". أنظر:

Josh Goldfoot, The Physical Computer and the Fourth Amendment, *Berkeley J. Crim. L.* Vol 16, Issue 1, *2011* , p 113.

[2] –*Ibid, p 117.*

[3] – عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب توصلا إلى الدليل الالكتروني في التحقيقات الجنائية – ترجمة ودراسة وتحقيق- الطبعة الثانية، دار النهضة العربية، مصر، 2006، ص 61.

[4] - *Thomas K. Clancy, the Fourth Amendment Aspects of Computer Searches and Seizures, Miss. L.J, Vol 75 2005, p 240.*

[5] - *Orin S. Kerr, Searches and Seizures in a Digital World, Harvard Law Review, Vol 119, Issue 2, 2005,p 535.*

[6] - *United States v. Carey, 172 F.3d 1268, 1275 n.8 10th Cir. 1999.*

مذكور لدى: عمر محمد بن يونس، المرجع السابق، ص 62.

[7] – **اعتمادا على طبيعة الجريمة التي يجري التحقيق فيها، فإنّ أجهزة الحاسوب قد تكون بحدّ ذاتها مجرّمة أو أداة لجريمة، ومن ثم يمكن ضبطها فعليا، فعلى سبيل المثال، يعتبر الحاسوب بحد ذاته مجرما متى استُغِل في تخزين مواد إباحية متعلقة بالأطفال، ويمكن اعتباره أداة للجريمة في الأحوال التي يُستعمَل فيها لارتكاب قرصنة أو إرسال تهديدات، أو نشر وتوزيع مواد فاحشة. على الرغم من أنّه يمكن القول بأن أيّ جهاز حاسوب يستخدم لتخزين أدلة الجريمة هو أداة بنفس الوقت، فإن القضاء انتهى إلى القول بأنّه لكي يعتبر جهاز الحاسوب أداة للجريمة وجب أن يكون استخدامه أمر ضرّوري في ارتكاب الجريمة وقد أشارت الدائرة العاشرة إلى معيار التمييز بينها إلى أن "أجهزة الحاسوب كانت أكثر من مجرّد "حاوية " للملفات، بل كانت أداة للجريمة".**

لمزيد من التفصيل راجع:

H. Marshall Jarrett, Michael W. Bailie, Ed Hagen , Nathan Judish, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations , Computer Crime and Intellectual Property Section Criminal Division Published by office of Legal Education Executive office for United States Attorneys, 3d ed. 2009,p 71.

[8] - *Orin S. Kerr , Search Warrants in an Era of Digital Evidence, Mississippi Law Journal, Vol 75, Issue 1, 2005,pp 101-102.*

[9] - *Orin S. Kerr, Search Warrants in an Era of Digital Evidence, Loc.Cit.*

[10] - *United States v. Campos, 221 F.3d 1143,1147 10th Cir.2000*
United States v. Reyes 798 F.2d 380, 383 10th Cir.1986
United States v. Giberson, 527 F.3d 882, 887 9th Cir. 2008

هذه التطبيقات القضائية وأخرى مذكورة لدى:

H. Marshall Jarrett, et al, op cit, pp71-72.

[11] - *H. Marshall Jarrett, Michael W. Bailie, Ed Hagen , Nathan Judish ,op cit. p 75.*

[12] - *People v Covlin 2018 NY Slip Op 28011 Decided on January 22, 2018 Supreme Court, New York Country.[Available online].Retrieved April 3,2019,from:https://law.justia.com/cases/new-york/other courts/2018/2018-ny-slip-op-28011.html*

[13] - *Orin S. Kerr, op cit, p 100.*

[14] - *Josh Goldfoot, op cit , p 141.*

ينتقد هذا الفقيه المفهوم الغامض لمتطلبات هذه القاعدة المنبثقة من منظور "الحاوية الفرعية" التّي تعني كما سلف بيانه أنّ وسيط التخزين كدعامة مادية يحتوي على عدة حاويات رقمية فرعية ينبغي تحديد أيّ منها تكون محل للتفتيش دون غيرها، متسائلا عن المقصود بالحاوية الفرعية؟ من أين تبدأ ومن أين تنهي؟ إذا كان المقصود هو تقسيم الملفات داخل مساحة التخزين الرقمية، فإن هذا التقسيم لا يأخذ صورة واحدة بل يخضع لابتكار المستخدم فكيف يمكن تحديدها في الإذن، ويزداد الوضع تعقيدا فيما لو كان ملفا واحدا يحمل قدرا كبيرا من المعلومات أين تصبح "الملفات" و"الحقائق" مفهومان مختلفان لتصور "الأشياء" الموجودة بوسيط التخزين الرقمي، علاوة على ذلك فإنّ الدليل المعلوماتي المستهدف بالتفتيش لا يكون دائما في شكل ملف داخل مساحة التخزين الظاهرة للمستخدم، بل قد يكون في شكل بيانات مدفونة داخل المساحة الفارغة *slack space* **أو عبارة عن بيانات وصفية.**

[15] - *Kerr,Orin S ,Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data, Texas Tech Law Review, Vol 48, Issue 1, 2015, p 15.*

[16] - *Adam M. Gershowitz, The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches, Vanderbilt law review, Vol 69, 2016, p 599.*

[17] - *Orin S. Kerr, Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data, op cit, p 11.*

[18] - *Josh Goldfoot, op cit , p166.*

[19] – درج كل من الفقه والقضاء للدلالة على هذا الضابط الإجرائي استعمال مصطلحات عديدة منها برتوكول التفتيش " *search protocol*"، ومصطلح منهجية التفتيش " *Search Methodology* "، وكذا مصطلح إستراتيجية أو خطة التفتيش " *search strategy* " ويعتبر المصطلح الأول هو الأكثر تداولا في التطبيقات القضائية، حيث تعزى فكرة وضع إستراتيجية تفتيش محددة توضح الخطوات المسبقة التي يجب على السلطة القائمة بالتفتيش إتباعها للحد من نطاق امتداد التفتيش إلى القرار الصادر سنة 1982 عن الدائرة التاسعة في قضية *United States v. Tamura* التّي تصدى فيها القضاء إلى بيان موقفه بشأن الضبط الإجمالي العرضي والتفتيش الشامل للوثائق الورقية التي تتشابك فيها الوثائق الخارجة عن نطاق الاذن القضائي مع تلك التي تعد موضوعا للدليل الجنائي، وفي هذه القضية أجرى مكتب التحقيقات الاتحادي تحقيقا بشأن جريمة رشوة بعد الحصول على إذن يسمح بضبط وثائق الشركة سعيا للوصل إلى دليل الجريمة، وبحكم المدة التي تستنفذها عملية التفتيش، قامت هذه الأخيرة بضبط عدة صناديق مليئة بوثائق ورقية مختلطة ومن بينها تلك المستندات التي لا علاقة لها بالتحقيق، وتم نقلها خارج الموقع لتفتشيها لاحقا، وعلى الرّغم من أن هذه الجهة القضائية أشارت إلى أن الضبط الإجمالي يعتبر مخالفا للتعديل الدستوري الرابع، إلّا أنها لم تقرر بطلان الدليل غير أنّها قرّرت ضمانات جديدة منعا من التوسع في التفتيش، مؤداها أنّه في الحالات التّي تكون فيها الوثائق متشابكة بحيث لا يمكن تصنيفها عمليا في الموقع، ينبغي تحريز المضبوطات ريثما يتم الحصول على إذن قضائي آخر يسمح بتوسيع نطاق التفتيش، وبناءً على هذه الضمانات التّي تقررت بقاعدة *Tamura* نشأ مذهب فقهي سنة 1994 يتقدمه الفقيه *Raphael Winick*، يطالب بضرورة إخضاع التفتيش المعلوماتي إلى هذه القاعدة بموجبها ينبغي على الجهات القضائية أن تشترط إستراتيجية تفتيش تفسر بالتحديد كيف تنفيذعملية التفتيش، وخلال سنة 1999 وبالضبط في قضية *United States v. Carey* اقترحت الدائرة العاشرة الجمع بين قاعدة *Tamura* ومقاربة Raphael Winick ابتغاء تجنب كشف أدلة جنائية تقع خارج نطاق الإذن القضائي وهو ما اصطلح عليه قضاء بمقاربة *Carey-Tamura* "*approach*" يقوم على مطالبة الضبطية القضائية التّي تتصادف مع وثائق مختلطة يتطلب فرزها خارج الموقع، أن تقوم بحفظها في انتظار ما يفرضه القضاء من قيود على مواصلة عملية تفتيش المنظومة المعلوماتية.

لمزيد من التفاصيل راجع:

Christina M.Schuck,Note & Comment, A Search for the Caselaw to Support the Computer Search "Guidance" in United States v. Comprehensive Drug Testing, Lewis & Clark *L.* Rev. *Vol 16, 2012,pp 755-756.*

[20] - *H. Marshall Jarrett, et al, op cit. p 75.*

[21] - *Derek Haynes, Comment, Search Protocols: Establishing the Protections Mandated by the Fourth Amendment Against Unreasonable Searches and Seizures in the World of Electronic Evidence,* Mc George Law Review,*Vol 40, 2009, pp 768-769.*

[22] - *United States. V. Comp. Drug Testing, Inc., 621 F.3d 1162, 1177 9th Cir. 2010.*

مذكور ومعلق عليه لدى: *Christina M. Schuck, op cit ,p 743*

[23] - *Simpson, Bob,"Preemptive Suppression" Judges Claim the Right to Find Digital Evidence Inadmissible Before It Is Even Discovered," Journal of Digital Forensics, Security and Law,Vol 7 ,2012, p 22.*

[24] - *Commonwealth v. Keown, 478 Mass. 232, 240-41 2017 [Available online]. Retrieved April 3, 2019, from: http://masscases.com/cases/sjc/478/478mass232.html.*

[25] - *In re Search Warrant, 71 A.3d 1158, 1169* n.*11* Vt. 2012*[Available online]. Retrieved August 20, 2019, from https://www.leagle.com/decision/invtco20121226c38.*

[26] - *Derek Haynes, op cit, p 772.*

[27] - *Orin S. Kerr, Ex Ante Regulation of Computer Search and Seizure, Virginia Law Review, Vol 96, Issue 6 2010, p 1261.*

[28] - *United States v. Schesso 9th Cir. 2013.*

للإطلاع على هذا الحكم وعديدا من التطبيقات القضائية الصادرة في هذا الشأن راجع:

Adam M. Gershowitz, op, cit, p 619.

[29] - *Paul Ohm, Massive Hard Drives, General Warrants, and the Power of Magistrate Judges, Virginia Law Review,Vol 97,2011,p 5.*

[30] - *H. Marshall Jarrett, et al, p 79.*

[31] - *United States v. Burgess, 576 F.3d 1078, 1093 10th Cir. 2009[Available online]. Retrieved August 20, 2019, from: https://www.courtlistener.com/opinion/172511/united-states-v-burgess/.*

[32] - *United States v. in the Matter of the Search Associated With Rwgann, Criminal No. 2014-0228 D.D.C. 2014 [Available online]. Retrieved August 20, 2019, from: https://www.courtlistener.com/opinion/2679245/united-states-v-in-the-matter-of-the-search-associated-with-rwgann/.*

[33] - *United States v. Apple iPhone, IMEI 013888003738427, Criminal No. 2014-0278 D.D.C. 2014 [Available online]. Retrieved August 20, 2019, from: https://www.courtlistener.com/opinion/2658339/united-states-v-apple-iphone-imei-013888003738427/.*

[34] - *United States v. Gray, 78 F. Supp. 2d 524, 529 E.D. Va. 1999.*

مذكور لدى: *H. Marshall Jarrett, et al, p 76*

[35] - *Derek Haynes , op, cit, p 774.*

[36] - *Paul Ohm,op cit , p 12.*

[37] – **الجدير بالذكر أنّه في بعض الحالات أظهر القضاة براعة فائقة في هذا المجال، ففي إحدى القضايا تقدمت الحكومة بطلب الموافقة على إذن بتفتيش نظم المعلومات يستهدف أجهزة تخزين رقمية، أين رفض قاضي التحقيق الطلب لعدم تقديم بروتوكول يرسم نطاق التفتيش، وحدد بذات الوقت أجلا لاستدراك هذا القصور وأثناء جلسة مناقشة الجوانب الفنية للبروتوكول المقترح لاحظت المحكمة أن عدم رد الحكومة في أحد الجوانب كان مثيرا للدهشة، فعندما أثارت المحكمة إمكانية قصر التفتيش على فترات زمنية معينة، ذكر أحد ممثلي الحكومة أنّ هذا القيد لن يكون مفيدا لأن دليل الملفات لا يبين إلا تاريخ آخر مرة تم فيها حفظ الوثيقة. ثم سألت المحكمة الخبير التقني الحكومي عما إذا كان من الممكن التغلب على هذه المشكلة بدراسة "البيانات الوصفية" التي لا تكشف فقط عن التاريخ الذي تم فيه حفظ الوثيقة، بل تظهر أيضا كيف ومتى تم استلامها، أو إنشائها، أو الوصول إليها، أو تعديلها، ولم يقدم الخبير التقني الحكومي أي رد، تاركا للمحكمة انطباعا راسخا بأنه لم يكن على دراية بمصطلح يتوقع أن يعرفه خبير في مجال الحاسوب.انظر:**

Christina M. Schuck, op, cit, p 777.

[38] - *Kerr,Orin S ,Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data , op cit , p 4.*

[39] - *Ibid , p 6.*

[40] - *Ibid , p 11.*

[41] - *Ibid ,pp 13-14.*

[42] - *Ibid , pp 25-27.*

[43] - *State v. Mansor, 421 P.3d 323 Ore. 2018.[Available online].Retrieved* June 3,2019*, from https://www.leagle.com/decision/inorco20180628715.*

[44] - *United States v. Ganias, 755 F. 3d 125, 134 2d Cir. 2014. [Available online]. Retrieved march 1, 2019, from https://casetext.com/case/united-states-v-ganias.*