

جامعة بـاتـة 1
كلية الحقوق والعلوم السياسية
قسم الحقوق

الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش

أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق
تخصص: علوم جنائية

إشراف الدكتورة
ميموني فايزة

إعداد الطالب
لهوى رابح

لجنة المناقشة:

اللقب و الإسم	الرتبة العلمية	الجامعة الأصلية	الصفة
د/ بن نصيب عبد الرحمان	أستاذ محاضر (أ)	جامعة باتنة 1	رئيساً
د/ ميموني فايزة	أستاذ محاضر (أ)	جامعة باتنة 1	مشرفاً، مقرراً
أ.د/ علواش فريد	أستاذ التعليم العالي	جامعة بسكرة	عضوا مناقشا
د/ بن بوعبد الله وردة	أستاذ محاضر (أ)	جامعة باتنة 1	عضوا مناقشا
د/ بوخالفية فيصل	أستاذ محاضر (أ)	جامعة سطيف 2	عضوا مناقشا
د/ سعدي الربيع	أستاذ محاضر (أ)	جامعة مسيلة	عضوا مناقشا

الله
بسم الله الرحمن الرحيم

شكرو تقدير

الشكر لله سبحانه وتعالى الذي هدانا لهذا و ما كنا لنهتدي لولا أن هدانا الله.
و التقدير كل التقدير لأستاذة الفاضلة المشرفة على الرسالة، الدكتورة ميموني فايذة التي
كانت كريمة معي بعلمها و توجيهاتها بكل صدق و اخلاص، و لا يمكن أن اغفل
عرفانها الذي سيظل دوما أمانة في عنقي، كما لا أستطيع أن أعبر عن مدى فخري و
اعتزازي بتكرم أساتذتي الأجلاء بقبولهم المشاركة في مناقشة الرسالة.
جَزَى اللهُ تَعَالَى الْجَمِيعَ خَيْرَ الْجَزَاءِ وَأَوْفَاهُ.

إلى والديّآ...

مقدمة

التعريف بالموضوع:

اتّسعت في العصر الحديث دائرة استخدام تكنولوجيا الإعلام و الإتصال نتيجة ما حقّفته للإنسانية من اختصار للمسافات و الجهد و الوقت و المال، حيث باتت المعلومات مرتبطة بمختلف مجالات النشاط الإنساني و صارت عمليات تجميعها و تخزينها و معالجتها و إسترجاعها بمثابة مقياس لرقى الأمم و تحضرها، إلاّ أنّه على الجانب المقابل فقد استغلّ المجرمون هذه التّقنية بكلّ ضراوة بجعلها هدفا لغاياتهم الجرمية أو وسيلة لتحقيقها بعيدا عن أعين السلطات العامّة، على نحو بات من الصّعب في الوقت الرّاهن تصور جريمة ليس لها بعد رقمي.

و من الطّبيعي أن يكون لحالة الصراع بين المجتمع و الجريمة في بعدها التّقني إنعكاسات على طرق الإثبات، من منطلق التّوافق الواجب تحقيقه دوما بين طبيعة الدّليل و طبيعة الجريمة التي يتولّد منها، ما أفضى إلى بزوغ وسيلة جديدة من وسائل الإثبات الجنائي إنضمت بجدارة إلى المفاهيم التّقليدية للدليل يطلق عليها "الأدلة المعلوماتية"، من هنا اتّجه البحث القانوني إلى الاعتراف بالحجّة القانونية لملفّات الحاسوب و مستخرجاته ذات المحتوى المعلوماتي، ليست بصورتها الموضوعية ضمن حاوية مادّية و لكن بطبيعتها الرّقمية المحضّة استنادا إلى مبدأ راسخ في النّظام القانوني مبناه حرّية الإثبات الجنائي.

و إذا كان القضاء المقارن قد أسهم بدوره في تكوين معالم الأدلة المعلوماتية بمجرد قبولها لتكوين عقيدته في بناء حكم الإدانة أو البراءة، فإنّ هذا النّوع المستجد من الأدلة الجنائية قد خلّف وجها من أوجه التّعارض بين حق المجتمع في مواجهه الجريمة و حق الفرد في التّمتع بحقوقه و حرياته الشّخصية، بحسبان أنّ جلّ إجراءات استرداد الأدلة المعلوماتية ممثلة في المراقبة الإلكترونيّة و التّسرب الرّقمي و تفتيش نظم المعلومات قد تقيّد بعض الحقوق الأساسيّة للأفراد، و في مقدّماتها الحقّ في الخصوصية المعلوماتية، باعتبار أنّ الحرمة التي يتمتّع بها النّظام المعلوماتي حاليا تجاوزت حرمة المساكن و غرف النّوم.

فإذا دقّقنا النّظر في أخطر هذه الإجراءات الحديثة من حيث تعلّقه بالحريات الشّخصية و من حيث ما يسفر عنه من أدلة تكشف وجه الحقيقة، لوجدنا أنّ أخطرها مساسا بالشرعيّة و أكثرها فاعليّة و أهميّة هو الولوج إلى الأنظمة المعلوماتية تفتيشا عن البيانات المخزّنة،

و من ثمّ كانت "الشّرعيّة الإجرائيّة للأدلة المعلوماتيّة المستمدّة من التّفّتيش" موضوعا لبحثنا.

الإشكالية الرئيسيّة:

إنّ هذه الرّؤية الحديثة للنّواحي الفلسفية التي نثيرها علاقة التّفّتيش بتكنولوجيا الإعلام و الإتصال في إطار استرجاع البيانات المخزّنة كقيمة إثباتية تجلي حقيقة الواقعة الإجرامية بأشخاصها، تقودنا إلى الإعتقاد الجازم بأنّ المبادئ العتيده التي تقوم عليها نظريّة التّفّتيش عن الأدلة الماديّة التي إعترف بها- منذ أمد بعيد- فقه القانون و قضائه ليست سوى عزاء تافه لضحايا هذا الإجراء في البيئّة الرّقميّة، فهي في الحقيقة لا تعدو أن تكون مجرد وهم لحماية الحريّات الفرديّة التي تعصف بها العملية الإثباتية القائمة على الأدلة المعلوماتيّة المستمدّة من التّفّتيش، و يصبح حينئذ من العبث طرح سؤال - جرى الفقه إلى اليوم على تكراره- مبناه مدى إمكانية تطويع القواعد التقليديّة للتّفّتيش عن الأدلة المعلوماتيّة.

إستلهاما من هذه الرّؤية التي أبدينا ملامحها في متسهل هذا البحث، و التي لا تعكس ذاتية الأحكام الإجرائيّة للأدلة المعلوماتيّة المستمدّة من التّفّتيش، بقدر ما تتّرجم تلك العلاقة الجدليّة غير المستقرّة القائمة بين مبدئين أساسيين يحكمان نظريّة الإثبات الجنائي، "مبدأ حرية الإثبات" و "مبدأ شرعيّة الإثبات"، و التي تتدرج في إطار حقين متناقضين، حق المجتمع في مواجهة الظّاهرة الإجرامية في بعدها التّقني، و حق الفرد في التمتع بحقوقه الرّقمية، و إن كُنّا نسلم مبدئيا بضرورة التقليل من جمود مبدأ الشرعيّة الإجرائيّة و جعله أكثر مرونة في ظل المتطلّبات التي تفرضها فعالية التّفّتيش على هذا النوع من الأدلة، فإنّ المنطق يفرض في المقابل بيان نطاق التّضييق الواجب لهذا المبدأ، تحقيقا للتوازن بين هذه الحقوق المتعارضة، و من هنا تبرز الإشكالية واضحة تبحت عن الحل:

إلى أي مدى تشكل ضوابط الشرعيّة الإجرائيّة قيّدا على حرية القاضي الجنائي في قبول الأدلة المعلوماتيّة المستمدّة من التّفّتيش في بناء حكم الإدانة او تعزيز قرينة البراءة؟

تساؤلات البحث:

- مدى إمكانية تجاوز الأحكام الإجرائية للتفتيش عن الأدلة المادية مع البيئة الرقمية دون تجاوز الضوابط التي يفرضها مبدأ الشرعية الإجرائية؟
- ما المقصود بـ "مستهدف التفتيش المعلوماتي"؟
- كيفية تحديد أجهزة التخزين الرقمية التي يحوزها المتهم كمستهدف للتفتيش المادي و تخصيص تلك التي تحتوي على الدليل دون غيرها؟
- ما هي حدود سلطة التحقيق في مرحلة التفتيش المادي و مرحلة التفتيش المعلوماتي و مرحلة ما بعد التفتيش؟
- ما هي شروط قبول هذا النوع من الادلة و ما مدى حرية القاضي في تقدير حجيتها؟

منهج البحث:

لقد إعترفنا منذ البداية بأنّ الأحكام الإجرائية للأدلة المعلوماتية المستمدة من التفتيش تبدو في كثير من المسائل منقطعة الصلة بأحكام التفتيش عن الأدلة المادية، و مع ذلك فهي تلقي الضوء على بعض أصل هذه الضمانات و الضوابط، فضلا عن قيمتها في البحث المنهجي ذاته، خاصة و أنّ "التفتيش المادي" يعتبر مقدمة ضرورية للتفتيش عن الأدلة المعلوماتية لا غنى عنها في معظم الأحوال.

من هذا المنطلق حرصنا من خلال تأصيل موضوع دراستنا على معالجة مختلف جوانبه بالتحليل المصغر في كل جزئياته و أصوله العامة بالمقارنة مع مختلف الأنظمة القانونية، و لأنّ التفاعل القانوني مع الأدلة المعلوماتية المستمدة من التفتيش يقف عند حدّ معين لم يتجاوزه، فقد كان التركيز على الإجتهد القضائي المقارن، و الذي لا يزال في إعتقاد متسمر أنّه في موضع قصور عن إرساء نظرية متكاملة لموضوع البحث رغم الأشواط الطويلة التي قطعها، لذا كان المفترض أن نعتمد على المنهج التحليلي و الوصفي.

اسباب اختيار الموضوع:

لا ريب أن موضوع البحث يعتبر من المواضيع الهامة الحديثة اذ اصبح يكتسي أهمية متزايدة في ضوء التطورات التقنية والسعي المحموم من قبل المجرمين لتوظيف التقنية بدلالاتها الواسعة في تحقيق جرائمهم و التخفي من وجه العدالة، مما جعل مواجهة هذا النوع

من الجرائم يستدعي الاستناد الى نوع جديد من الأدلة ممثلا في نبضات غير مرئية يقتضي استردادها مساسا ببعض الحقوق و الحريات الفردية.

انطلاقا من طبيعة هذا الدليل، يطرح موضوع البحث اشكاليات لا تزال محل استفهام إلى غاية اليوم حول مفهوم محل التفتيش و محله و نطاق امتداده داخل الوطن و خارجه و اثر ذلك على حقوق المتهم و غيره، و حق الفرد في حذف البيانات الي لا علاقة لها بالواقعة كل ذلك في ظل عدم تعرض المشرع إلى هذه المسائل بالتنظيم، في وقت خطى فيه القضاء المقارن خطوات طويلة سعيا لايجاد ضمانات تقيم توازنا بين حق المجتمع في محاربة الجريمة و حق الفرد في التمتع بحقوقه و البحث عن هذه الضوابط هو الذي دفعنا إلى اختبار موضوع البحث.

أهمية البحث:

إذا كنا قد تعرّضنا في هذه المقدمة إلى جزء يسير من الإشكاليات الهامة التي يطرحها موضوع البحث، فإننا لسنا بعد ذلك في حاجة إلى تأكيد أهمية هذا الموضوع، إذ يبدو واضحا ما لهذه الدراسة من أهمية ترجع في حقيقتها لتلك الأهمية التي تحضى بها قاعدة الشرعية الإجرائية للدليل الجنائي باعتبارها وسيلة فعّالة لحماية حقوق الإنسان و حرّياته، لا سيما في الوقت الراهن الذي يشهد تزايدا في الجرائم التي تعد البيئة الرقمية مسرحا لها، بحكم استغلال المجرمين للمعلوماتية بدلالاتها الواسعة في تحقيق مآربهم الجرمية بعيدا أعين العدالة، ممّا وفر للقائمين على محاربة هذا النوع من الجرائم ذريعة للمساس بحريّات الأفراد و حقوقهم، و من هذا المنطلق فإنّ أهمية البحث تتجلى من خلال ثلاثة نواحي:

فمن ناحية أولى، يقع موضوع البحث في أكثر مناطق الإجراءات الجزائية دقّة و حساسيّة تثير معها إشكالية الموازنة بين الثلاثية "الفعالية" و "الشرعية" في الوصول إلى "الحقيقة"، إذ لا فارق بين أن تنتهك حرّيات الأفراد و حرمة حياتهم الخاصة بمعرفة أشخاص يعملون تحت ستار القانون أو بمعرفة مجرمين يرتكبون آثامهم بمنأى عن سطوة القانون، خصوصا في الوقت الراهن الذي بات فيه النظام المعلوماتي أقرب إلى المسكن من حيث نطاق و كمية المعلومات الخاصة التي يخزنها، فاستقر في ضمير الجماعة تمتعه بقدر من الخصوصية يتجاوز المفهوم الراسخ لخصوصية غرف النوم، فالتعامل مع الخصوصية الرقمية وفق منطق الخصوصية المكانية أو الجسدية هو بمثابة افتتات على الحرّيات الشّخصيّة،

و مثل هذا الأمر ترتب عليه أزمة في الشرعية الإجرائية لعدم وجود ضمانات رقمية تراعي هذه الرؤية الجديدة للحقوق الفردية، و لا ريب أنّ التّعرض لهذه الجدلية يفرز العديد من الإجهادات القيّمة.

و من ناحية ثانية، تجرّنا أزمة الشرعية الإجرائية في التفتيش عن الأدلة المعلوماتية إلى إحياء الدور الخلاق للقاضي الجنائي، وقد اضطررنا سعياً لذلك إلى عقد الأهمية للقضاء المقارن الذي و إن كان منقطع الصلة بنظامنا القضائي، إلاّ أنّه ينفرد في إطار تجاوبه مع المعلوماتية بأحكام متميزة بعد أن خاض معركة كفاح تجاوزت العقدين من الزمن لأجل تطوير القواعد القانونية لكي تتفاعل مع الرقمية وفق نظرة فلسفية مضمونها الالتزام بالشرعية الإجرائية بمفهومها الواسع حال التفتيش عن الأدلة و إلاّ فقدت هذه الأخيرة أهميّة وجودها قانوناً، و استقرت في المنطق الافتراضي كواقعة رقمية مجردة من أيّ قيمة إثباتية، و من شأن رصد بعض هذه السوابق القضائية زيادة المعرفة و فتح الجديد من الأفاق على نظام لا شك في أهميته، خاصّة و أنّ الإجراءات الجزائية المعلوماتية بشكل عام تتجه نحو تجاوز الحدود الإقليمية بمفهوما المادي لتقترب أكثر من العولمة.

و من ناحية ثالثة، يرتبط موضوع الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش بمواضيع وثيقة الصلة به لا تقل عنه أهميّة، أهمها نظرية الإثبات العلمي سواء في بعدها القانوني أو طابعها العلمي، أين نلمس مؤشرات خطيرة في تراجع دور القاضي حال إعمال سلطانه في تقييم مدى موثوقية هذه الأدلة و تقدير قيمتها الإثباتية و الإكتفاء بالإنصياح لتوجيهات الخبير التقني، خاصة في ما يتعلق بمسألة أصالة و سلامة الدليل المعلوماتي من التعديل، و نعتقد أنّ دراسة جادة لهذا الموضوع سوف ترصد في ثناياها معايير موضوعية بعيدة عن الطابع العلمي يُهتَدَى بها لإعادة إرساء "مبدأ القاضي خبير الخبراء"، و سوف يلاحظ القارئ أنّ هذه المسألة الهامة شكلت هاجساً للقضاء و الفقه المقارن على مدى عقدين من الزمن لأنّه يتوقّف عليها مصائر المتهمين، و من ثم تزداد أهميّة البحث لتصبح ضرورة ملحة، سيما و أنّ بؤادر هذا الموضوع بدأت تظهر في المحاكم العربية.

أهداف البحث:

ليست الغاية من الدراسة إضافة مؤلف إلى المؤلفات الكثيرة التي تناولت موضوع الأدلة الجنائية المعلوماتية بشكل عام، و إنما الإحساس العميق بأن أي من هذه الدراسات لم تصل إلى حد تأصيل نظرية عامة تمكنت من وضع أسس عملية لحل التساؤلات الشائكة التي تثيرها الاجراءات الجزائية في البيئة الرقمية، فالدراسات العربية على كثرتها لا تزال تنتظر إلى التفتيش المعلوماتي و اثاره بشكل لا ينعق من المفهوم و التكيف و الضمانات التقليدية رغم أنّ الفارق بليغ بينهما على نحو ما سيستيقن منه القارىء

و إن كانت الدراسات الأجنبية قد تطرقت إلى موضوع البحث، فإن هذه الأبحاث على ندرتها متناثرة و مبعثرة بطريقة يصعب الرجوع إليها، و من هنا كانت الحاجة ماسة إلى الالمام بهذه الاتجاهات الفقهية المقارنة، و البحث عن نقاط الخلاف بينهما و بين التشريع الجزائري و العربي عموما و تنظير هذه الشتات، و هذا ما استهدفته من البحث، بمحاولة تحديد الآثار القانونية لمبدأ الشرعية على التفتيش المعلوماتي كإجراء ينطوي على مساس بالحقوق الرقمية و على الأدلة المستمدة منه، و كذا بيان الجزاء المترتب على الاخلال بهذا المبدأ.

الدراسات السابقة:

في حدود البحث الذي أجريناه فقد اطلعنا على العديد من الدراسات ذات العلاقة المباشرة بموضوع دراستنا الراهنة، و من بين أهمها بحث بعنوان **الإثبات الجنائي للجرائم المعلوماتية**، و هو عبارة عن أطروحة دكتوراه من اعداد الباحث بن فريدة محمد، كلية الحقوق و العلوم السياسية، جامعة الجزائر 1، 2015، و ايضا بحث بعنوان **الدليل الإلكتروني و دوره في الإثبات الجنائي دراسة مقارنة**، و هو عبارة عن أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تيزي وزو، 2019، اذ استفدنا مما جاء في كلا البحثين من استفاضة في موضوع ماهية هذا النوع من الأدلة و أثر هذه الذاتية على اجراءات استخلاصه، و كذا بيان مدى حرية للقاضي الجنائي في الاقتناع بهذا النوع المستحدث من الادلة. و يعتبر البحث الذي اعده الباحث محمود عبد الغاني فريد جاد المولى بعنوان **دور الدليل الإلكتروني و دوره في المجال الجنائي**، و هو عبارة عن رسالة دكتوراه، كلية الحقوق جامعة بنها، مصر، 2016، من بين اهم الدراسات التي استفدنا منها كثيرا لانها لاتعنى

من موضوع دراستنا و زيادة على ثراء هذه الدراسة لأنها تناولت موضوع حجية الأدلة المعلوماتية في التشريعات المقارنة من بينها الشريعة المصري و الفرنسي و الأمريكي، و مازاد من اهميتها ايضا لجوء الباحث الى الاستشهاد بعدد معتبر من الاحكام القضائية في كل اشكالية من الاشكاليات الهامة التي يثيرها الموضوع.

صعوبات البحث:

لعل ابزر عائق واجه الباحث هو صعوبة الامام بالمصطلحات التقنية المتنوعة التي لا عهد للقانون الجنائي بها، و الاحاطة بهذه المصطلحات يعتبر امر بالغ الأهمية حتى يدرك الباحث بعدها القانوني، انطلاقا من أول اشكالية يثيرها الموضوع حول المقصود بالتفتيش المعلوماتي و متى يقع بالضبط إلى غاية آخر اشكالية يطرحها و المتعلقة بشروط قبول هذا الدليل.

و تكمن الصعوبات ايضا في قلة المراجع العربية التي تناولت هذا الموضوع، اما المراجع الاجنبية فهي تتميز بصعوبة ترجمتها لعدم وجود توحيد المصطلحات عند ترجمتها للغة العربية و ايضا ارتباط المسائل القانونية بالتقنية في عومهما- عند معالجتها- مما يجعل الاستناد الى المراجع الاجنبية امرا بالغ الصعوبة، فضلا على قلة الاعتماد على هذا النوع من الادلة الجزائية من الناحية العملية في الدول العربية و من بينها الجزائر مما افضى إلى قلة القرارات القضائية المتعلقة بالموضوع.

خطة البحث:

إنطلاقا مما سلف بيانه، فقد شرعنا في دراسة موضوعنا وفقا لخطة لتحقيق الفائدة التي استهدفناها، و تقوم هذه الخطة على محاولة وضع تلك الجزئيات المنبثقة من التساؤلات الفرعية في نسق علمي متكامل، و هكذا تكون خطتنا لمعالجة الموضوع على النحو التالي:

الفصل التمهيدي: ماهية الأدلة المعلوماتية المستمدة من التفتيش.

الباب الأول: الأحكام الإجرائية للأدلة المعلوماتية المستمدة من التفتيش.

الفصل الأول: تاصيل التفتيش عن الأدلة المعلوماتية المستمدة من التفتيش

المبحث الأول: مدلول فكرة التفتيش عن الأدلة المعلوماتية.

المبحث الثاني: مقدمات التفتيش عن الأدلة المعلوماتية.

الفصل الثاني: ضوابط التفتيش عن الأدلة المعلوماتية.

المبحث الأول: الضوابط الموضوعية للفتيش عن الأدلة المعلوماتية.

المبحث الثاني: الضوابط الشكلية للفتيش عن الأدلة المعلوماتية.

الباب الثاني: حجية الأدلة المعلوماتية المستمدة من التفتيش.

الفصل الأول: القيمة الإثباتية للأدلة المعلوماتية المستمدة من تفتيش مشروع.

المبحث الأول: حرية القاضي الجنائي في قبول الدليل المعلوماتي المستمد من التفتيش المشروع.

المبحث الثاني: حرية القاضي الجنائي في تقدير الدليل المعلوماتي المستمد من التفتيش المشروع.

الفصل الثاني: القيمة القانونية للأدلة المعلوماتية المستمدة من تفتيش مشروع.

المبحث الأول: جزاء التفتيش غير المشروع عن الأدلة المعلوماتية.

المبحث الثاني: الجزاءات التي توقع على مرتكب التفتيش غير المشروع عن الأدلة المعلوماتية.

على أن تكون خاتمة البحث موجز نتعرض فيه لأهم النتائج و التوصيات المقترحة التي تم التوصل إليها من خلال الدراسة.

الفصل التمهيدي

ماهية الأدلة المعلوماتية

المستمدة من التفتيش

من البديهي أن تنعكس طبيعة الجريمة أو وسيلة إرتكابها على الدليل المتولّد منها، و تثير هذه الحقيقة في معرض دراستنا تساؤلات مشروعة تتعلّق أساسا بمفهوم هذا الدليل الجنائي الذي يستهدفه التفتيش؟ و ما هو المصطلح الدقيق للدلالة عليه؟ هل هناك فارق بين مصطلح الدليل المعلوماتي و الدليل الرقمي و الدليل الإلكتروني؟ ما الذي يختصّ به هذا الدليل على غيره من الأدلة الجنائية التقليدية؟ ما موقعه بين التقسيمات المعروفة للأدلة التقليدية؟

الواقع من الأمر أنّ هناك تساؤلات قانونية بالغة الأهمية تعدّ الإجابة عنها بمثابة المدخل الطبيعي لدراسة فكرة الشرعية الإجرائية للأدلة المعلوماتية المستمدة من هذا الإجراء، بحكم الارتباط الوثيق القائم بين طبيعة هذا الدليل و إجراءات استخلاصه، و ذلك من خلال التّطرق إلى تحديد مدلول الدليل المعلوماتي (مبحث أول)، و تقسيماته (مبحث ثاني).

المبحث الأول

مدلول الأدلة المعلوماتية المستمدة من التفتيش

ما المقصود بالدليل المعلوماتي المستمد من التفتيش؟ الحقيقة أنّ هذا السؤال يحدّد بدقّة طبيعة الدّراسة و غايتها، فإن كانت تسمية هذا الدليل تبدو كاشفة للوهلة الأولى عن مدلوله، إلا أنّ ذلك يعتبر بمثابة تبسيط محل لإشكالية لا تزال محل جدال خصب، تعدّ الإجابة عنها مقدّمة ضرورية لدراصة مشروعية هذا الدليل، كما أنّ الهيئات المتنوعة التي يوجد عليها هذا الدليل من حيث تكوينه تدفعنا للبحث عن تصنيف له بين الأدلة الجنائية التقليديّة حتّى يمكن الإستناد إليه في بناء الإدانة أو البراءة، لذا كان من المقتضى الطّبيعي أن يعالج مستهل هذه الدّراسة مفهوم الدليل المعلوماتي (مطلب أول) و تقسيماته (مطلب ثاني).

المطلب الأول: مفهوم الدليل المعلوماتي المستمد من التفتيش

إنّ البحث في نطاق مفهوم الدليل المعلوماتي الجنائي المستمد من التفتيش يجعل الباحث - و بحق - عرضة لخضم عدد هائل من الآراء في تعريفها لهذا الدليل، حتّى إنّ من الصّعوبة بمكان رصد موقف تشريعي أو فقهي يعرّفه تعريفا جامعا مانعا (فرع أول)، أو يُقدّم و لو جزئيا منطقا قانونيا يمكن من خلاله تحديد المصطلح الدقيق للدلالة عليه (فرع ثاني).

الفرع الأول : تعريف الدليل المعلوماتي المستمد من التفتيش

يفرض البعد التقني للدليل المعلوماتي المستمد من التفتيش أن يتّسم مفهومه بالمرونة و الوضوح بُغية وضع تعريف دقيق له، خشية حصره في نطاق ضيق لا يتواءم مع التطور المتسارع الذي تشهده تقنية المعلومات، و إن أغفلت الإتفاقيات الدولية رصد تعريف له (أولا)، و تردّدت معظم التّشريعات في بيان مدلوله (ثانيا)، إلا أنّ ذلك لم يمنع الفقه من المساهمة في رسم ملامح واضحة لمدلوله (ثالثا).

أولا: تعريف الاتفاقيات للدليل المعلوماتي المستمد من التفتيش

إنّ المتأمل للاتفاقيات الدولية، يلحظ في مستهلها إدراج مادة لتعريف المصطلحات و المفردات المستخدمة في متن الإتفاقية، توضّح فيها المعاني المقصودة بتلك المصطلحات، و الغرض من ذلك هو تحري الدقّة في استخدام المصطلح و إخراج ما لا يقصده الأطراف، و هو المسلك الذي سلّته الإتفاقيات الدولية التي تُعنى بمحاربة الإجرام المعلوماتي، بأن

تعرّضت إلى بيان مفهوم عديد من المصطلحات الهامة المرتبطة بالإثبات الجنائي المعلوماتي، إلا أنها أغفلت إيراد تعريف للدليل المعلوماتي⁽¹⁾.

و أهمية تحديد مدلول الدليل المعلوماتي في الإتفاقيات الدولية يفرضها البعد الدولي لهذا الدليل، لذا استشرع المشرع الأوروبي الحاجة إليه عند محاولة إبرام إتفاق دولي يحدّد من خلاله آليات جمع الأدلة المعلوماتية و تبادلها بين دول الإتحاد الأوروبي، أين أثّرت إشكالية تحديد المفهوم الدقيق لمصطلح "الدليل المعلوماتي"، و ذلك مفترض طبيعي نتيجة إنعكاس مفهومه على إجراءات الوصول إليه و استرداده، و ما يترتّب على ذلك من مساس خطير بالحقوق و الحرّيات الفرديّة، خاصة تلك الإجراءات التي تجرى في سرّيّة عن بعد و عابرة للحدود الدوليّة بالمفهوم التقليدي.

نتيجة لذلك إستدرك المشرع الأوروبي هذا القصور ضمن مشروع الإتفاقية الأوروبية لتبادل المعلومات و الأدلة الرقمية المسماة "Evidence"⁽²⁾، بمقتضاها عُرّف الدليل المعلوماتي بأنه يمثل "أيّ معلومات (تشمل مخرجات الأجهزة التناظرية أو البيانات في شكل رقمي) ذات قيمة إثباتية محتملة تتمّ معالجتها أو توليدها أو تخزينها أو نقلها بواسطة أيّ جهاز إلكتروني"⁽³⁾.

(1) و هذا المسلك واضح من خلال المادة الأولى لأهمّ الاتفاقيات الدولية المتعلقة بمكافحة الجرائم المعلوماتية و هي:

- الإتفاقية الأوروبية لمكافحة الجرائم المعلوماتية و المسماة "بإتفاقية بودابست" التي تمّ إعتماها و تقريرها التفسيري من لدن لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة (8 نوفمبر 2001) و فتح باب التوقيع على الإتفاقية في بودابست المجرية في 23 نوفمبر 2001 بمناسبة المؤتمر الدولي حول الجريمة الإلكترونية.

- إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني و حماية البيانات ذات الطابع الشّخصي، التي تمّ اعتمادها في الدورة العادية الثالثة و العشرون لقمة رؤساء و حكومات الإتحاد الإفريقي المنعقدة في ملابو، غينيا الإستوائية، بتاريخ 27 يونيو 2014.

- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تمّ اعتمادها من قبل مجلس وزراء العرب و الداخلية بتاريخ 21-12-2010 و تمّ المصادقة عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 252/14 المؤرخ في 08 سبتمبر 2014، الصّادر بالجريدة الرّسمية عدد 57، بتاريخ 28 سبتمبر 2014.

(2) "European Informatics Data Exchange Framework for Courts and Evidence".

(3) Electronic evidence is " any information (comprising the output of analogue devices or data in digital format) of potential probative value that is manipulated, generated through, stored on or

و الملاحظ على هذا التعريف أنه ورد دقيق الصياغة من الناحية اللغوية و القانونية، إذ بقدر ما كان التعريف موسعا شاملا لجميع أنواع المعلومات، أيًا كان نوعها، و وضعها، خشية توصل التقنية إلى معلومات حديثة تجعل التعريف لا يتجاوب مع التطورات الحاصلة في مجال تقنية المعلومات و الاتصالات، فقد كان قاصرا على معلومات محدّدة و هو ما يتجلّى من عبارة "ذات قيمة إثباتية محتملة" (Of Potential Probative Value).

و كلمة "محتملة" في نظرنا تترتب عليها مسائل قانونية هامة، فمن جهة أولى تفضي إلى تفادي تضيق دائرة الأدلة المعلوماتية بحصرها في تلك التي تتمتع بالقوة الإثباتية دون غيرها أو تلك التي يرجح أن تكون كذلك، في وقت تحول دون التعميم المجرد للمعلومات، إذ ليست كلّ المعلومات التي قد توجد بحوزة المتهم - بالمفهوم التقليدي للحيازة- مما له إرتباط بالواقعة الجرمية أو يفيد في إظهار الحقيقة، خاصة بالنظر إلى ظاهرة التخزين الرقمي التي تشهد تنظورا يفوق قدرة العقل البشري على الإستيعاب، و هو ما يحسب للمشرع الأوروبي في هذا الصدد⁽¹⁾.

communicated by any electronic device", The European Evidence project, "European Informatics Data Exchange Framework for Courts and Evidence" (Grant Agreement Number 608185),p 7.[Available online].Retrieved April 3, 2019, from file:///C:/Users/toshiba/Downloads/evidence-ga-608185-d3-1-411.pdf.

(1) قد تظهر بساطة المعنى الظاهري للنص، إلا أنّ المتأمل لصياغته يجده يعني الكثير بمنطق بسيط جدا، فهو يمتاز بدقّة متناهية، و يميل إلى تأمين حماية فاعلة، بالنتفات المشرّع إلى روح تلك المعاني الشمولية المترابطة و غاياتها، فقصر نطاق عناصر الدليل على "المعلومات" التي يُحتمل أن تكون لها قيمة إثباتية، و تلك عبارة تفيد بمفهوم المخالفة إستبعاد المعلومات التي يرجح عدم إنتمائها إلى عناصر للدليل الجنائي من نطاق الإجراءات الجنائية - التي يشكل التفتيش عنها و استردادها قيّدا على الحرّية الفردية- كقاعدة عامة، و كأنّ المشرّع أراد بذلك أن يرصد نطاق العلاقة بين الحقوق الرقمية و إجراءات إستخلاص الدليل من منطلق مبدأ عتيد في الإجراءات الجنائية التقليدية و هو "مبدأ العلاقة الكاشفة" Principle of Relevance و هو أحد مقومات النهج الفلسفي القائم على الإلتزام بصون الحرّيات الفردية في تحصيل الدليل المعلوماتي المعروف "بالشّرعية الإجرائية المعلوماتية" و ذلك هو مبنى الخلاف لعدم وجود إستقرار قانوني أو قضائي يضمن التفاعل بين الإجراء الجنائي و البيئة المعلوماتية دون الاخلال بضوابط الشرعية في معناها الواسع و هي الإشكالية التي يتحور حولها البحث.

ثانيا: التعريف التشريعي للدليل المعلوماتي المستمد من التفتيش

تجنّب التشريع الجزائري شأنه شأن معظم التشريعات المقارنة الخوض في تعريف الدليل الجنائي المعلوماتي⁽¹⁾، و السبب في اعتقادنا يرجع إلى كون التطور المتسارع الذي تشهده تقنية المعلومات في الوقت الراهن قد يتجاوز أيّ تعريف يمكن صياغته، لذا ترك أمره للإجتهادات الفقهية.

على نقيض ذلك، تطرّق المشرّع العربي إلى تعريف هذا النوع المستحدث من الأدلة و يأتي التشريع السوري في مقدّمة هاته التشريعات، و ذلك بموجب المرسوم التشريعي رقم 17 لعام 2012 المتضمّن قانون تنظيم التّواصل على الشّبكة و مكافحة الجرائم المعلوماتية و بالتّحديد بمقتضى المادة الأولى منه و التي جاء فيها "الدليل الرّقمي: البيانات الرّقمية المخزّنة في الأجهزة الحاسوبية أو المنظومات المعلوماتية أو المنقولة بواسطتها و التي يمكن استخدامها في إثبات أو نفي جريمة معلوماتية"⁽²⁾.

يُعبّأ على هذا التعريف أنّه اتخذ من منطق تكوين الدليل المتمثّل في "البيانات" أساسا لتعريفه، فتجاهل "المعلومات" التي تشكّل عناصر الدليل المعلوماتي و التي بدونها يفقد هذا الدليل معناه و قيمته⁽³⁾، فالبيانات تعبّر عن الأرقام و الكلمات و الرموز أو الحقائق أو

(1) واقع الأمر أنّه يجب على المشرّع تجنّب إيراد التعريفات إلّا للضرورة القصوى، إذ ليس من وظيفة المشرّع إيراد تعريفات إلّا في حالتين هما: أن يكون غرض التعريف حسم خلاف فقهي قائم، أو أن يكون هذا التعريف مغايرا لمعنى مستقر، ذلك لأنّ للتعريف أضرار في بعض الأحيان لأنّه يقيد القاضي و يسلب منه حرية الحركة في التقدير، و مع ذلك فإذا كان التشريع حديثا و يتناول في أحكامه مجموعة من المصطلحات الجديدة و الفنيّة فقد يكون إيراد التعريف أمرا مقبولا.

يراجع بهذا الخصوص: عصمت عبد المجيد بكر، مشكلات التشريع دراسة نظرية و تطبيقية مقارنة، دار الكتب العلمية، بيروت، لبنان، 2013، ص 196.

(2) المرسوم التشريعي السوري رقم 17 لسنة 2012 المتعلّق بتطبيق أحكام قانون التّواصل على الشّبكة و مكافحة الجريمة المعلوماتية الصادر بالجريدة الرّسمية (بدون رقم العدد) بتاريخ 15 فيفيري 2012.

(3) هناك فارق بليغ بين "البيانات" و "المعلومات"، فوفقا للمادة الأولى من القانون الجزائري رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 أوت 2009 المتضمّن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها و الذي دخل حيّز النّفاذ بموجب الجريدة الرّسمية عدد 47، الصادرة بتاريخ 16 أوت 2009 تُعرّف المعلومات بأنّها "أيّ عملية عرض للوقائع و المعلومات و المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها"، أمّا

الإحصائيات الخام التي لا علاقة بين بعضها البعض، و لم تخضع بعد للتفسير أو للتجهيز للإستخدام أي هي تخلو من المعنى الظاهري في أغلب الأحيان، أمّا "المعلومات" فهي المعنى الذي يستخلص من هذه البيانات "فالمعلومات نتيجة تحليل للبيانات"⁽¹⁾.

لذا كان الأحرى بالمشرع السوري ربط التعريف بفكرة المعلومات لأنها تمثل الوسيلة الفعلية التي يستعين بها القاضي للوصول إلى حقيقة الواقعة الإجرامية، و تظهر عدم دقة صياغة التعريف من الناحية القانونية من جهة أخرى في قصر نطاق العمل بالدليل المعلوماتي على الجريمة المعلوماتية فقط، في حين فإنّ دور الدليل المعلوماتي في إثبات الجريمة التقليدية لا يقلّ عن دوره في إثبات الجرائم المعلوماتية، لأنّه "من الصّعب في الوقت الزّاهن تصور جريمة ليس لها بعد رقمي"⁽²⁾.

و تطرّق حديثاً التشريع المصري إلى تعريف الدليل المعلوماتي بموجب المادة الأولى من القانون 175 رقم لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات معتبرا إياه يشمل "أيّ معلومات إلكترونية لها قوّة أو قيمة ثبوتية مخزّنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية و ما في حكمها، و يمكن تجميعها و تحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة"⁽³⁾.

مصطلح "البيانات" فينصرف بصفة عامة إلى الحقائق أو الأرقام أو الحروف أو الرموز التي تشير أو تصف موضوعا ما أو فكرة أو حالة أو أية عوامل أخرى. ومعنى ذلك أنّ البيانات تكون عبارة عن تمثيل أو تصوير للحقائق أو المفاهيم أو التعلّيمات في شكل معياري يناسب عملية اللاتصال أو الإنتقال أو الترجمة أو المعالجة بواسطة الحاسب، أمّا المعلومات فهي النتائج النهائية لهذه العمليات، فإذا كانت البيانات بمثابة المدخلات للحاسب فإنّ المعلومات بمثابة المخرجات، و إذا كانت البيانات هي المادة الخام التي تنقل أو تعالج بوسائل أوتوماتيكية فإنّ المعلومات هي النتائج التي يمكن الحصول عليها من هذه البيانات.

لمزيد من التفصيل راجع: هلاي عبد الله أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري و البحريني على ضوء إتفاقية بودابست، الطبعة الثّانية، دار النهضة العربية، مصر، 2014، ص ص 45 - 46.

(¹) طارق إبراهيم الدسوقي، الأمن القانوني النظام القانوني لحماية البيانات، بدون رقم الطبعة، دار الجامعة الجديدة، مصر، 2015، ص 42.

(²) Eoghan Casey, Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet, Academic Press, London, 2000, p 3.

(³) القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات الصّادر بالجريدة الرّسمية عدد 32 مكرر (ج) بتاريخ 14 أوت 2018.

الحقيقة أنّ هذا التعريف يفتقر إلى الدقة في الصياغة إذ ورد التعريف عاما و ليس قاصرا على الدليل المعلوماتي في مجال الإثبات الجنائي، كما يعاب عليه إشتراط "قوة إثباتية" للمعلومات لخلع صفة الدليل عليها، و لا خلاف على عدم صحة ذلك، إذ أنّ مسألة حجية الدليل أو قوته الإقناعية هي أمر يخضع لتقدير القاضي و ليس لتصور المشرع.

أما المشرع اللبناني فقد رصد تعريفا للدليل المعلوماتي تحت مسمى "الأثار المعلوماتية" و ذلك بمقتضى المادة 121 من القانون رقم 81 لسنة 2018 المتعلق بالمعاملات الإلكترونية و البيانات ذات الطابع الشّخصي كما يلي: "الأثار المعلوماتية، و التي هي من قبيل الأدلة الرقمية أو المعلوماتية، هي البيانات التي يرتكبها الأشخاص بصورة إرادية أو لا إرادية على الأنظمة و قواعد البيانات و الخدمات المعلوماتية و الشبكات المعلوماتية، تتضمن الأدلة المعلوماتية التجهيزات المعلوماتية و البرامج و البيانات و التطبيقات و الأثار المعلوماتية و ما يماثلها"⁽¹⁾.

و يؤخذ على هذا التشريع عدم إعتداد مصطلح واحد للدلالة على الدليل المعلوماتي، و وضع مصطلحين مترادفين و هما "الأثار" و "الأدلة"، و كان الأحرى تبني لفظ "الأدلة" بإعتباره المصطلح المعتمد في قانون الإجراءات الجزائية، كما أنّ المشرع اللبناني وضع مصطلح الرقمية بشكل مقابل لمصطلح المعلوماتية و بذلك يكون قد جانب الصواب، لأنّ المعلومات (Informations) تستوعب الأرقام (Numbers)⁽²⁾.

كما يعاب عليه أيضا الخلط بين التجهيزات المادية و الدليل المعلوماتي عند التّطرق لمضمون هذا الدليل، فالأدلة المعلوماتية مثل أيّ واقعة تحدث من خلال النظام الثنائي الرقمي و هي تستقل بوجودها عن الحاسوب مشكلا في قطعه الصلبة حتّى مع الإعتراف المسبق باستحالة فصله عن وسيط التخزين الذي يحتويه⁽³⁾.

(1) القانون اللبناني رقم 81 لسنة 2018 و المتعلق بالمعاملات الإلكترونية و البيانات ذات الطابع الشّخصي، الصّادر بالجريدة الرّسمية عدد 45، بتاريخ 18 أكتوبر 2018.

(2) ترتيب تركي الدرويش، القواعد الإجرائية الخاصة بالدليل المعلوماتي في لبنان، مجلة الحقوق و العلوم السياسية، الجامعة اللبنانية، لبنان، المجلد 03، العدد 23، 2019، ص 122.

(3) يلاحظ أيضا أنّ صياغة التعريف غير دقيقة من حيث الألفاظ المستعملة، إذ جاء تعريف الأدلة المعلوماتية في عبارة هي "البيانات التي يرتكبها الأشخاص بصورة إرادية أو لا إرادية على الأنظمة و قواعد البيانات و الخدمات

ثالثاً: التعريف الفقهي للدليل المعلوماتي المستمد من التفتيش

لم يتفق الفقه الجنائي إلى غاية اليوم حول تعريف موحد للدليل الجنائي المعلوماتي، وعلّة ذلك هو التطور المتسارع الذي يطرأ باستمرار على طبيعة تكوين هذا النوع من الأدلة و البيئة التي يحيا فيها، سيما و أنّ العالم الافتراضي لا يزال في بداياته و لم يصل بعد إلى منتهاه، و لن يكون من اليسر إحتوائه، مما قد يجعل كلّ تعريف تتم صياغته لا يتجاوب مع التطور المتلاحق للتقنية، و عموماً يمكن تصوّر موقفين بشأن مواقف الفقه في هذا الصدد، إمّا تعريف الدليل بناء على طبيعة تكوينه (أ)، و إمّا ربط التعريف بفكرة المعلومة (ب).

(أ) - ربط تعريف الدليل المعلوماتي بحسب اداة تكوينه.

حيث يذهب الإتجاه الأول إلى أنّ منطق تكوين الدليل الرقمي هو الأساس الذي يجب أن تُبنى عليه معادلة تعريفه، بحيث يُعترف فقط بالبيانات التي تعدّ من طبيعة مغناطيسية و إلكترونية، و بناء عليه فالدليل المعلوماتي هو "الدليل الذي يجد له أساساً في العالم الافتراضي و يقود إلى الجريمة"، فهو ذلك الجزء المؤسس على الإستعانة بتقنية المعالجة التقنية للمعلومات و الذي يؤدي إلى إقتناع قاضي الموضوع بثبوت ارتكاب شخص ما للجريمة، فكّما كان هناك مزج في موضوع الدليل (الفكرة أو المعلومة كبيانات Data) بالمعالجة الآلية للمعلومات فإنّه يعدّ هنا دليلاً رقمياً⁽¹⁾.

و هذا التوجه يجد له أنصاراً في الفقه المقارن، إذ على هدى من تلك الفكرة يعرف الفقيه **Eoghan Casey** الدليل المعلوماتي بأنّه "جميع الأشياء التي تثبت وقوع ارتكاب الجريمة، أو

المعلوماتية و الشبكات المعلوماتية"، فالمعنى الظاهري للنص يوحي إلى المخاطب به إنصراف نية المشرع إلى تعريف الجريمة المعلوماتية و هو ما يفهم من لفظ "يرتكبها"، لأنّ الدليل الجنائي واقعة مادية أو رقمية تكشف صلة الجريمة بمقتربها و هي بذلك تشكّل أثراً لواقعة أخرى نشأت من خلالها ممثلة في الواقعة الجرمية، "فالدليل أثر يترك" و " ليس فعلاً يُرتكب"، ما يجعل مدلول اللفظ يخالف أصلاً قصد المشرع منه، لذا يحسن بالمشرع مراجعة الصياغة منعا من الوقوع في الخلط بين الدليل المعلوماتي و الجريمة المعلوماتية، و إن سعى المشرع إلى التفريق بين الأدلة المعلوماتية حسب المصدر المنشئ لها (النظام المعلوماتي أو التّدخل البشري)، فإنّه لا جدوى من هذا التقسيم من الناحية العملية كما سرنى لاحقاً عند معالجة أقسام الأدلة المعلوماتية المستمدة من التفتيش و المعيار المعتمد في ذلك.

(1) عمرو محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، مصر، 2004، ص969.

توجد علاقة بين الجريمة و مقترفها أو تُوجد علاقة بين الجريمة و المتضرر منها و تتضمن تلك البيانات خليطاً من الأرقام التي تمثل مختلف أنواع المعلومات بما في ذلك النصوص، الرموز، الصور و الأصوات⁽¹⁾، أو هو ذلك الدليل الذي يمثل "أية بيانات مخزنة أو منقولة باستخدام جهاز الحاسوب و التي تؤكد أو تنفي كيفية وقوع الجريمة أو تتناول عنصراً من عناصرها الأساسية"⁽²⁾.

و قد أثر هذا الفقيه استعمال لفظ "البيانات" Data بدلاً من "المعلومات" Informations ، لأنّ "البيانات" في نظره أكثر تجريداً من "المعلومات" بما يسمح بقدر أكبر من التعميم⁽³⁾، إلّا أنّنا نرى خلاف ذلك، فمصطلح "المعلومات" أدقّ و قد اشار التشريع الأردني إلى أنّ "المعلومات هي البيانات التي تمت معالجتها و أصبح لها دلالة"⁽⁴⁾، بحيث لا يعقل أن تقدم البيانات في طابعها الخام كثنائي رقمي قوامه الواحد و الصفر (0-1) كدليل جنائي لبناء هيئة الإدانة أو البراءة على أساسه، بل في شكل معلومات لها فائدة في إظهار الحقيقة.

كما عرّفته المنظمة الدولية لأدلة الحاسوب (IOCE) بأنه يمثل "المعلومات المخزنة أو المتقلّبة في شكل ثنائي، و يمكن أن يُعتمد عليها في المحكمة"⁽⁵⁾، و هو يقترب من التعريف الذي جاء به الفريق الأمريكي العلمي المعني بالأدلة الرقمية (SWGID) الذي يرى بأنّ الأدلة

(1) The definition given by E. Casey, refers to digital evidence as: "Physical objects that can establish that a crime has been committed, can provide a link between a crime and its victim, or can provide a link between a crime and its perpetrator." . Eoghan Casey, op cit, p 260.

(2) Eoghan Casey, Susan W. Brenner, Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet, 3rd Edition, Academic Press, London, 2011, p 7.

(3) Shahzad Saleem, Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics, philosophy doctoral thesis, Stockholm University ,Sweden, 2015, p 22.

(4) المادة الأولى من القانون الأردني رقم 27 لسنة 2015 و المتعلق بالجرائم الإلكترونية، الصادر بالجريدة الرسمية عدد 5343، بتاريخ 04 ماي 2015.

(5) The definition proposed by the International Organization of Computer Evidence (IOCE) states: "Digital evidence is information stored or transmitted in binary form that may be relied on in court." Mattia Epifani, Pasquale Stirparo, Learning iOS Forensics, First published, Packt Publishing, England, 2015, p 9.

المعلوماتية هي "المعلومات المخزنة أو المتقلّلة في شكل ثنائي، ذات قيمة إثباتية"⁽¹⁾، فالدليل المعلوماتي إذن وفق هذا المنظور هو "بيانات يمكن إعدادها و تراسلها و تخزينها رقمياً بحيث تمكن الحاسوب من تأدية مهمة ما"⁽²⁾.

و قد تعرّضت هذه التعريفات إلى النقد على أساس تركيزها على القيمة الإثباتية للدليل و إهمالها للعديد من أنواع البيانات التي أفرزتها الثورة المعلوماتية⁽³⁾.

واقع الأمر أنّ الفقه الأمريكي يميل إلى ترجيح تعريف الفقيه **Carrier Brian** الذي توسّع في تعريف الدليل المعلوماتي متّخذاً من الخلفية العلمية للتحقيق الجنائي الرقمي أساساً تبنى عليه عملية التعريف فيرى بأنّه "بيانات رقمية تدعم أو تدحض فرضية ما حول الأحداث الرقمية أو حالة البيانات الرقمية"، تأسيساً على أنّ التحقيق الجنائي الرقمي يقوم على صياغة و اختبار الفرضيات للإجابة على الأسئلة المثارة حول الأحداث الرقمية السابقة أو حالة البيانات الرقمية، و لا يمكن للمحققين بصفة عامة مراقبة البيانات الرقمية مباشرة⁽⁴⁾.

و بدلاً من ذلك، يمكنهم فقط مراقبة البيانات المعروضة على جهاز العرض أو جهاز الإخراج، أي أنّ مشاهدة البيانات تتم بطريقة غير مباشرة، بحيث يجب صياغة فرضية مفادها أنّ البيانات الفعلية تعادل البيانات الملاحظة، ثم يتمّ البحث عن بيانات تدعم هذه الفرضية أو تدحضها، و بذلك يكون موضوع الدليل المعلوماتي غير قاصر على البيانات المقدّمة في

(1) Standard Working Group on Digital Evidence (SWGDE), stating that: "Digital evidence is any information of probative value that is either stored or transmitted in a digital form ". Mattia Epifani, Pasquale Stirparo, op cit, p 10.

(2) و هو التعريف الذي أخذ به التقرير الأمريكي المقدم ضمن ندوة الأنتربول حول الدليل المعلوماتي المنعقدة سنة 2001 بمدينة ليون بفرنسا ورد فيه :

"Digital Evidence: Information of probative values stored or transmitted in digital form.". Report on Digital Evidence - Prepared by: Mark M. Pollitt, BS, Unit Chief Computer Analysis Response Team - FBI Laboratory, Washington, DC, USA, 13th INTERPOL Forensic Science Symposium, Lyon, France, October 16-19 2001.p 5.

(3) Mattia Epifani, Pasquale Stirparo ,op cit, p 10.

(4) Digital evidence is: "Digital data that supports or refutes a hypothesis about digital events or the state of digital data".Carrier Brian, A hypothesis-based approach to digital forensic Investigations, philosophy doctoral thesis, Purdue University, United States of America, 2006, pp 11-12.

مرحلة المحاكمة فقط، بل هناك بيانات ذات قيمة في التّحقيق تستغل من النّاحية العلمية أثناء عملية التّحليل الحاسوبي الشّرعي و لو لم تقدّم الى القضاء⁽¹⁾.

و إن كان هذا التّعريف أكثر توسّعا عن غيره من التّعريفات السّابقة، إلّا أنّه لا يركّز على تعريف الدّليل المعلوماتي بمفهومه القانوني، بقدر تركيزه على تحديد هذا المفهوم بمنطق علم التّحليل الحاسوبي الشّرعي، كما أنّه يفتقر إلى قصر نطاق هذا المفهوم على موضوع الإثبات في المسائل الجنائية، إذ "الواقعة الرّقمية" أو كما يسمّيها "وضعية أو حالة البيانات الرّقمية" « digital event » or the « state of digital data » ليست بالضرورة مرتبطة بالواقعة الجرمية أو تشكّل ظرفا من ظروفها، فليس "الدليل الإلكتروني في جوهره مجرد واقعة يتمّ حفظها في ذاكرة الحاسوب"⁽²⁾، فذلك بمثابة توسّع مبالغ فيه.

و في هذا الصّدّد يرى الفقيه Stephen Mason أنّ التّعريف الجامع للدليل المعلوماتي يجب أن تنطوي تحته كافة البيانات بمختلف صورها سواء التّنظرية أو الرّقمية، مخزّنة كانت أو منقولة، و أيّا كان الجهاز الذي يخزّنها أو ينقلها، على أن تكون تلك البيانات ذات صلة بالواقعة التي يتنازع حولها الأطراف⁽³⁾.

أمّا في الفقه العربي فتعدّدت التّعريفات بين الإيجاز⁽⁴⁾ و التّفصيل⁽⁵⁾، و التّضييق⁽¹⁾ و التّوسّع⁽²⁾، حيث تم تعريفه بأنّه "الدّليل المأخوذ من أجهزة الكمبيوتر، و يكون في شكل

(1) Carrier Brian, op cit, p 13.

(2) Mark Krotoski, Effectively Using Electronic Evidence Before and At Trial, United States Attorneys Bulletin, Vol. 59, N 6, 2011, p53.

(3) Stephen Mason , Daniel Seng, Electronic Evidence , Fourth edition published by the Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017, p 21.

(4) فعرفه البعض بإيجاز بأنّه "الدليل الذي يحتاج إلى معالج رقمي لقراءته و فهم محتواه".

راجع: حازم محمد حنفي عثمان، الدليل الإلكتروني و دوره في المجال الجنائي، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 2016، ص 11.

(5) و عرفه البعض الآخر بشيء من التّفصيل بأنّه يشمل "أيّ معلومات أو بيانات مخزّنة أو منقولة في المجال الرّقمي تكون دالة على ارتكاب فعل مجرم أو مرتكب ذلك الفعل أو شريك له أو تحوي دليل براءة على فعل ما، و

نبضات مغناطيسية أو كهربائية يمكن تجميعها و تحليلها، باستخدام برامج و تطبيقات و تكنولوجيا خاصة، و هو مكوّن رقمي لتقديم معلومات في أشكال متنوّعة، مثل النّصوص المكتوبة أو الصّور أو الأصوات و الأشكال و الرّسوم، و ذلك من أجل اعتماده أمام أجهزة إنفاذ القانون و تطبيقه⁽³⁾.

حقيقة الأمر أنّ هذا التّوجه في تعريف الدّليل المعلوماتي و إن حاول إستيعاب جانب مهمّ من جوانب هذا النّوع المستحدث من الأدلّة من حيث طبيعته و كفيّة استخلاصه من البيئة الرّقمية، إلّا أنّه يخلط بين مفهوم الدّليل المعلوماتي و المصدر الذي يستمدّ منه، فالقول بأنّ الدّليل المعلوماتي لا تثبت له هذه الصّفة إلّا إذا تمّ استخلاصه من مصدره يؤدّي إلى إستبعاد العديد من الأدلّة المعلوماتية من دائرة الإثبات ما لم يتم نقلها خارج الوسط الرّقمي الذي نشأت فيه، و مثل هذا القول غير صحيح على الإطلاق، لأنّ التّطور المتسارع للتّقنية

يمكن العثور على تلك المعلومات أو البيانات بجهاز الحاسوب الشّخصي أو المكتبي أو الهاتف المحمول، أو آلات التصوير الرّقمية أو أيّ جهاز رقمي آخر تمّ ربطه بوحدة الإتصال المختلفة أو شبكات الإتصال المعلوماتي".

راجع: خليفة محمد صالح جاد المولي، الدّليل الرّقمي و حجبيته في إثبات جرائم المعلومات، رسالة دكتوراه، كلية الحقوق جامعة طنطا، مصر، 2018، ص 36.

(1) فقيل بأنّ الدّليل المعلوماتي هو "الدّليل المشتق من أو بواسطة النّظم البرمجية المعلوماتية الحاسوبية، و أجهزة و معدّات و أدوات الحاسب الآلي، أو شبكات الإتصال من خلال إجراءات قانونية و فنية، لتقديمها للقضاء بعد تحليلها علمياً أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور و أشكال و أصوات لإثبات وقوع الجريمة لتقرير البراءة أو الإدانة فيها".

راجع: محمود عبد الحميد عبد المطلب، البحث و التّحقيق الجنائي الرّقمي في جرائم الحاسب الآلي و الأنترنت، دار الكتب الجامعية، مصر، 2006، ص 24.

(2) و عرّف بكونه "مجموعة الوسائل الإلكترونية المتعدّدة و المتكاملة غير المحسوسة القابلة للتّحليل ذات الدّلالة و البرهان الجنائي الذي يصل إلى حد اليقين أو غلبة الظنّ اللازم لكشف الحقيقة في القضايا الجنائية الإلكترونية". أنظر: أحمد بن عبد الله الرّشودي، حجية الوسائل الإلكترونية في الإثبات الجنائي دراسة تأصيلية مقارنة، رسالة دكتوراه، كلية الدّراسات العليا جامعة نايف العربية للعلوم الأمنية، المملكة العربية السّعودية، 2008، ص 251.

(3) عبد الناصر محمد محمود فرغلي، عبيد سيف سعيد المسماري، "الإثبات الجنائي بالأدلّة الرّقمية من النّاحيتين القانونية و الفنية دراسة تطبيقية مقارنة" ورقة بحث مقدّمة للمؤتمر العربي الأوّل لعلوم الأدلّة الجنائية و الطّب الشرعي، جامعة نايف العربية للعلوم الأمنية، المنعقد بالرياض، في الفترة 2-4/11/2007، ص 13.

تجاوز مسألة المخرجات الحاسوبية في شكلها المطبوع كدليل للإثبات الجنائي⁽¹⁾، و أصبح التعامل في الوقت الراهن يتم عن طريق النسخ الرقمي للبيانات المجرّمة التي تتشكّل موضوعاً للدليل الجنائي، فهذا التعريف ليس دقيقاً بما فيه الكفاية من الناحية التقنية و ينطوي على تضيق كبير لدائرة الأدلة المعلوماتية.

(ب) - ربط تعريف الدليل المعلوماتي بفكرة المعلومة

على ضوء هذه الإنتقادات ذهب إتجاه آخر إلى تعريف الدليل المعلوماتي بما يتعدى منطق تكوينه و طريقة استخلاصه، إلى ربط التعريف بفكرة المعلومة، فعُرف بكونه "معلومات يقبلها المنطق و العقل و يعتمدها العلم، يتم الحصول عليها بإجراءات قانونية و علمية بترجمة البيانات الحاسوبية المخزّنة في أجهزة الحاسب الآلي و ملحقاتها و شبكات الاتصال، و يمكن استخدامها في أيّ مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بالجريمة أو جان أو مجني عليه"⁽²⁾.

و يؤخذ على هذا التعريف قصر مفهوم الدليل الجنائي المعلوماتي على الدليل المشروع المستمدّ وفق إجراءات قانونية، و مثل هذا الأمر يقودنا إلى القول بأنّ الدليل الجنائي المحصل بطرق غير مشروعة لا يدخل في دائرة الأدلة الجنائية، و الحقيقة خلاف ذلك.

(¹) تشير مقدّمات التعامل مع الدليل المعلوماتي بكونه يعبر عن تجاوب متكامل يتطوّر بسرعة كبيرة جداً، فبعد أن كان الدليل الصّامت يشير إلى ما يمكن الحصول على نسخة منه بطريق الطباعة، وهو ما يسمّى بمخرجات الحاسوب مثل الوثائق و الصور، فإنّ التطور إقتضى أن يكون له منطق آخر الآن يُعبر عنه التطور ذاته الذي تنتجه تقنية المعلومات، و هو المظهر التقني المعلوماتي المتّسم بالحركية و الذكاء، و من ثمّ فإنّ موضوع إمكان اعتبار الدليل المعلوماتي بالمفهوم التقليدي بطريق الطباعة و عداد هذه المخرجات أدلة تأخذ بها المحاكم في القانون المقارن، يبدو أنّه قد أضحى تاريخاً إذا علمنا أنّ التطور قد فرض نوعيّة أخرى ذكية و حركية تدرج في الدليل الرقمي و تُعدّ أحد أشكاله الجديدة مثلما هو الحال في نوعيّة الملفات التي تحتوي في موضوعها ما هو غير معدّ للطباعة، كذلك التي يتمّ إعدادها في الحاسوب للقيام بالربط بين الحواسيب، و تلك التي تتولى الربط بين الخوادم عبر الشبكات الخاصة. فالיום لم يعد الأمر مرتبطاً بفكرة الحاسوب الشّخصي PC بل تطوّرت التقنية لتضع لنا فضلاً عن تطوير الحاسوب الشّخصي ذاته، بإضافة إمكانيات ضخمة إليه، نظّم الشبكات Networks و المعالج التوزيعي processing Distributed و الأنترنت.

أنظر تفصيلاً: عمرو محمد أبو بكر بن يونس، المرجع السابق، ص 969.

(²) محمد الأمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 234.

و في سياق مقارب عُرّف هذا الدليل بكونه يمثل "المعلومات التي تمّ الحصول عليها من الحيز الافتراضي (نظام تخزين- نظام تراسل)، و تكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يتمّ معالجتها بتقنيات خاصة لتنتج عنها هيئات معينة يتمّ ربطها بين الجريمة و الجاني و المجني عليه بطريقة لا تتعارض مع القانون"⁽¹⁾.

واقع الأمر، أنّ الأدلة المعلوماتية تشمل أيّ بيانات مولدة أو مخزّنة في شكل رقمي كما استخدم الحاسوب، و هي تشمل المعلومات التي يدخلها أيّ فرد يدويّاً في جهاز إلكتروني أو المعلومات المولدة في معاملة حاسوبية أو إستجابة لطلب، حيث يولّد جهاز إلكتروني معلومات كما لو كان إنساناً آلياً أو معلومات منبّجة و مخزّنة حيثما يعالج جهاز ما معلومات ضمن مصفوفته. و من ثمّ، فإنّ الأدلة الإلكترونية هي "أيّ معلومات مدرّجة أو مولدة أو محفوظة في قواعد بيانات أو نظم تشغيلية أو برامج تطبيقات أو نماذج مولدة حاسوبياً تستتبط بالاستقراء نتائج و رسائل بريد إلكتروني و صوتي بل و حتّى تعليمات محتفظاً بها في صورة خامدة ضمن مصرف ذاكرة حاسوبية"⁽²⁾. فالأدلة المعلوماتية هي "كلّ المواد الإثباتية التي توجد بشكل إلكتروني أو رقمي، و التي تكون مخزّنة أو عابرة، و قد تتخذ شكل ملفات حاسوبية أو مواد منقولة أو سجلات أو بيانات فوقية أو بيانات شبكية"⁽³⁾.

(1) و ترى الباحثة (رشيدة بوكر) أن أهمية تعريفها تبدو من وجهين: الأول التمييز بين الأثر الفيزيائي و الأثر الإلكتروني للمعلومات في نظام المعالجة الآلية، فالآثار الفيزيائية تكون موجودة على القرص الصلب على شكل كهرومغناطيسي أو موجودة بشكل مؤقت في ترانزستورات الذاكرة المؤقتة أو موجودة في الأطياف الكهرومغناطيسية في الكوابل أمّا الآثار الإلكترونية فهي تفسير لهذه الآثار بواسطة أدوات و برمجيات خاصة. و الثاني أنّ نطاق الدليل المعلوماتي لا يقتصر على الجرائم المعلوماتية أو الإلكترونية و إنّما يمتدّ ليشمل طائفة الجرائم التقليدية التي يتمّ تنفيذها بمساعدة النظم المعلوماتية. لمزيد من التفصيل راجع: رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، رسالة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة الجبلاني اليابس سيدي بلعباس، الجزائر، 2017، ص 396.

(2) الفريق العامل المعني بالتعاون الدولي "جمع و تبادل الأدلة الإثباتية الإلكترونية"، مؤتمر الأطراف في إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المنعقد ببينا، في الفترة: 27 و 28 أكتوبر 2015، رقم الوثيقة CTOC/COP/WG.3/2015/2، ص 1.

(3) مكتب الأمم المتحدة المعني بالمخدرات و الجريمة، دراسة شاملة عن مشكلة الجريمة السيبرانية و التدابير التي تتخذها الدول الأعضاء و المجتمع الدولي و القطاع الخاص للتصدّي لها، تقرير فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية و التدابير التي تتخذها الدول الأعضاء و المجتمع الدولي و القطاع الخاص للتصدّي

في تقديرنا فإنّ مرجع قصور هذه التعريفات هو الخلط بين البيانات و المعلومات، و الخطأ في تعريف الدليل الجنائي بشكل عام لربط تعريفه بقيمته الإثباتية و مشروعية تحصيله، لأنّ جوهر الدليل (عناصره سواء الإيجابية أو السلبية) تختلف عن القيمة الإثباتية التي يستخلصها القضاء في ضوء تقديره، و التسليم بخلاف ذلك يؤدي بنا إلى إنكار صفة الدليل عن المعلومات التي تمّ استبعادها لشك في الموثوقية أو لعيب في المشروعية، و ذلك منحي خاطئ و مظلّل⁽¹⁾.

لذا نرى أنّ التعريف الجامع المانع لهذا الدليل يستوجب أن يبيّن جوهره و يوضّح هدفه و يستجلي خصائصه⁽²⁾، فلمّا كانت المعلومات هي قوام هذا الدليل، فإنّه في هذا المنحي يجد متّسعا له بخصوص عناصره (البيانات)، التي يحتويها وعاؤه (الحاسوب)⁽³⁾، في الوقت الذي ينبغي قصر هذا المعطى على البيانات المرتبطة بالواقعة الإجرامية و هو ما يطلق عليها

لها"، مكتب الأمم المتحدة المعني بالمخدرات و الجريمة، منظمة الأمم المتحدة، فيينا، بتاريخ 25-28 فيفيري 2013، وثيقة رقم UNODC/CCPCJ/EG.4/2013/2، ص 12.

(1) راجع لاحقا نطاق مبدأ مشروعية الدليل الجنائي المعلوماتي المستمد من التفتيش في بناء حكم البراءة من خلال المطلب الثاني من المبحث الاول من الفصل الاول ضمن الباب الثاني.

(2) يقصد بجوهر الدليل الجنائي لبّه و مضمونه الأساسي فهو من الوجهة المجردة يحتوي على عناصر إيجابية أو سلبية يتزايد قدر إحداها على الأخرى حسب طبيعة الدليل و تنوّعه باعتباره دليلا للإثبات أو النفي، فالعناصر الإيجابية تميّز أساسا دليل الإثبات و تتزايد فيه على تلك العناصر السلبية، و ذلك بسب ما يهدف إليه ذلك الدليل من التّوصل إلى خلق حالة اليقين المطلوب توافرها كأساس للحكم، بينما ترجّح العناصر السلبية في دليل النفي أو البراءة نزولا على ما تقتضيه طبيعة هدفه من مجرد التشكيك في ثبوت التّهمة، و من ثمّ استمرار صيانة الأصل الإثباتي القائم على افتراض البراءة و هذه العناصر التي ترتبط بمحل الإثبات، و الذي يقصد به بصورة عامة تلك الواقعة الإجرامية المراد إثبات وقوعها و كذلك صحة إسنادها إلى شخص المتّهم.

راجع: أحمد ضياء الدّين محمد خليل، مشروعية الدليل في المواد الجنائية، أطروحة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 1984، ص ص 379-380.

(3) و في هذا الصّدّد نجد أنّ مصطلح الحاسوب يتّسع لأبعد من مفهوم الحاسوب الشّخصي أو المنزلي ليشمل أي جهاز له قابلية استقبال البيانات و معالجتها إلى المعلومات ذات قيمة يخزنها في وسائط تخزين مختلفة، و في الغالب يكون قادراً على تبادل هذه النّتائج و المعلومات مع أجهزة أخرى كالهواتف المحمولة و الأجهزة اللّوحية بالإضافة إلى الملقّات و الخوادم و غيرها مما قد نتيجته التقنيّة مستقبلا، و تقاديا من قصر وعاء هذا الدليل في نطاق ضيق من الأجهزة نجد أنّ التّشريعات تعتمد مصطلح النّظام المعلوماتي بدلا من مصطلح الحاسوب.

بالمعلومات، لذا نرى أنّ الدليل المعلوماتي يشمل "أية معلومات إلكترونية تكشف حقيقة الواقعة الإجرامية بأشخاصها".

الفرع الثاني: تحديد المصطلح الدقيق للدلالة على الدليل المعلوماتي المستمد من التفتيش

بعد أن فرغنا من تحديد المفهوم الدقيق للدليل المعلوماتي، وجب البحث عن "دال" لهذا المفهوم أو تسمية دقيقة له، خاصة و أنّ النماذج المعروضة لتعريفات الدليل المعلوماتي سواء التشريعية أو الفقهية تكشف عن تعدد المصطلحات المستخدمة للدلالة عليه، فهذا الدليل يوسم بـ "الدليل الرقمي"، و "الدليل الإلكتروني"، و "الدليل المعلوماتي" ⁽¹⁾، أو الدليل السيبرنتيكي "La Preuve Cybernétique" ⁽²⁾. و يثور التساؤل في ضوء ذلك عمّا إذا كان هناك فارق بين هذه المصطلحات أم هي مترادفة المعنى؟ و أيّ المصطلحات أدق في الدلالة عليه؟ كلّ ذلك نجيب عنه في ضوء الفقه المقارن (أولاً)، و الفقه العربي (ثانياً).

أولاً: موقف الفقه المقارن

في إجابته على هذا التساؤل يرى الفقه المقارن أنّ هناك فارق بليغ بين "الدليل الرقمي" و "الدليل الإلكتروني"، فالدليل الرقمي هو الدليل الذي ينشأ في الأصل "مؤد رقمية" بواسطة الحاسوب أو أيّ جهاز آخر مماثل، أمّا الدليل الإلكتروني فله مدلول أوسع من ذلك، لأنّه لا يشمل الأدلة الرقمية فقط، بل يمتد ليشمل أيضاً الأدلة المادية أو الأدلة التقليدية (غير الإلكترونية) التي تخضع للرقمنة فيما بعد، كسلاح القتل أو بدم الضحية و التي يمكن رقميتها عن طريق التقاط صورة لها، فالدليل الإلكتروني يشمل "الأدلة المؤلدة رقمياً" "Born Digital" و كذلك "الأدلة غير المؤلدة رقمياً" "Not Born Digital" و تمت رقميتها لاحقاً ⁽³⁾.

(1) و يقابل هذه الألفاظ في اللغة الإنجليزية:

Computer Evidence, Digital Evidence, Electronic Evidence.

و يقابل هذه الألفاظ في اللغة الفرنسية :

la Preuve Numérique, La Preuve Electronique, la Preuve Informatique

(2) Giudicelli-Delage, Geneviève. « Les transformations de l'administration de la preuve pénale. Perspectives comparées : Allemagne, Belgique, Canada, Espagne, Etats-Unis, France, Italie, Portugal, Royaume-Uni », Archives de politique criminelle, vol. 26, no. 1, 2004, p149.

(3) Sveva Avveduto, Sara Conti, Daniela Luzi, and Lucio Pisacane ,The Conceptual Representation of the "Electronic Evidence" Domain, Handling and Exchanging Electronic Evidence Across Europe, Springer International Publishing, 2018,p163.

ثانياً: موقف الفقه العربي

هناك جانب من الفقه العربي يميّز بين الدليل الإلكتروني و الدليل الرقمي على سند من القول بأنّ الدليل الإلكتروني يمثل "جميع الأجهزة التي يمكن أن تخزن أو تعالج أو ترسل أو تستقبل معلومات رقمية"، أمّا الدليل الرقمي فيشمل "جميع المعلومات المخزّنة في الأجهزة الإلكترونية و يشمل ذلك جميع أنواع الوثائق و الصّور و الملفات الصّوتية و المرئية و البرامج التي يتمّ العثور عليها في الحاسب الآلي أو وسائط التخزين أو أيّ أجهزة إلكترونية أخرى و التي تم ضبطها في مسرح الجريمة"، بحيث يلزم لوجود دليل رقمي وجود دليل إلكتروني، على اعتبار و أنّ الدليل الإلكتروني يعدّ بمثابة حاوية للدليل الرقمي، و الفرق بينهما أنّ حيازة الدليل الإلكتروني قد تكوّن جريمة بحدّ ذاتها أو دليلاً على إرتكاب الجريمة، كأجهزة التّشفير فهي دليل على التّخفي أثناء ولوج شبكة المعلوماتية، كما أنّ الدليل الرقمي يكون داخل الدليل الإلكتروني مثل وجود معلومات محظورة داخل جهاز الحاسب الآلي كالصّور الدّاعرة للأطفال القصر أو البرامج المنسوخة، ففي العديد من القضايا تتظافر الأدلّة الرقمية مع الأدلّة الإلكترونية لإثبات التّهمة أو نفيها⁽¹⁾.

بدون تردّد فإننا نرى أنّ أساس التّمييز في الفقه العربي بين الدليل الإلكتروني و الدليل الرقمي يتجاهل الفارق بين القطع الصّلبة و المعلومات، "فالقطع الصّلبة مجرد حاوية لتخزين الدليل المعلوماتي و ليست دليلاً بحدّ ذاتها" (**The hardware is merely a storage container for evidence, not evidence itself**)⁽²⁾.

فالدليل المستهدف بالتفتيش و التّحقيق هو الملف الإلكتروني الذي يشكّل موضوعاً للدليل الجنائي، و إن كان هذا الدليل لا ينفصل بحكم طبيعته الرقمية عن وسيلة تخزينه، فإنّ ذلك لا يعجل وسيط التخزين الرقمي دليلاً معلوماتياً و لا يخرج من دائرة الأدلّة التّقليدية

(¹) سليمان غازي بخيت المقيطي العتيبي، دور البحث الجنائي في الكشف على الجرائم المعلوماتية، رسالة دكتوراه، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السّعودية، 2016، ص 79.

(²) Kerr, Orin S., Digital Evidence and the New Criminal Procedure, Columbia Law Review, Vol 105, Issue 1, 2005, p 299.

(المادية)، و مثال ذلك البصمة الموجودة على لوحة المفاتيح تبقى ضمن طائفة الأدلة التقليدية مهما كانت درجة ارتباطها بالدليل المعلوماتي⁽¹⁾.

و حجّتنا في ذلك أنّ نسخ المعلومات على جهاز مادي آخر لا يقلل من حجّيتها، بل و يمكن في الكثير من الأحوال استرداد الأدلة المعلوماتية من خلال إجراءات "التفتيش عن بعد" في الحالة التي تكون فيها هذه البيانات مخزّنة في الحوسبة السحابية، و الاستغناء تماما عن الجهاز المادي المستعمل في الجريمة، و مثال ذلك الأدلة المستمدة من تطبيقات التّواصل الاجتماعي، بحيث يكون الجهاز المادي في هذه الفروض مجرد نافذة للوصول إليها و لا يستتبع فقدانه إستحالة إسترجاع الدليل المعلوماتي.

من هذا المنطلق نجد أنّ المشرّع الأوروبي درج على استعمال لفظ "الدليل الإلكتروني" في التّوصية رقم 95 في البند رقم 13 التي تمّ إعدادها من قبل لجنة وزراء أوروبا في الحادي عشر من شهر سبتمبر 1995 المتعلقة بضرورة تعديل الإجراءات الجنائية بما يتواءم مع التّكنولوجيا الحاسوبية⁽²⁾، و كذلك تمّ استعماله ضمن المادة 14 من الإتفاقية الأوروبية لمكافحة الجرائم المعلوماتية. كما حافظ على ذات المصطلح ضمن مقترح البرلمان الأوروبي رقم 2018/0108 المتعلّق بأوامر تسليم و حفظ الأدلة الجنائية الإلكترونية بين دول الإتحاد

(1) اعتمادا على طبيعة الجريمة التي يجري التّحقيق فيها، فإنّ أجهزة الحاسوب قد تكون بحدّ ذاتها مجرّمة أو أداة لجريمة فعلى سبيل المثال، يعتبر الحاسوب بحدّ ذاته مجرما متى استُغل في تخزين مواد إباحية متعلّقة بالأطفال، و يمكن اعتباره أداة للجريمة في الأحوال التي يُستعمل فيها لإرتكاب جريمة قرصنة أو إرسال تهديدات، أو نشر و توزيع مواد فاحشة، على الرّغم من أنّه يمكن القول بأنّ أيّ جهاز حاسوب يستخدم لتخزين أدلة الجريمة هو أداة بنفس الوقت، فإنّ القضاء الأمريكي إنتهى إلى القول بأنّه لكي يعتبر جهاز الحاسوب أداة للجريمة و يجب أن يكون استخدامه أمر ضروري في ارتكاب الجريمة و قد أشارت الدائرة العاشرة إلى معيار التّمييز بينها إلى أنّ "أجهزة الحاسوب كانت أكثر من مجرد" حاوية " للملفات، بل كانت أداة للجريمة".

لمزيد من التّفصيل 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, pp 71et ss.

(2) Conseil de l'Europe, Problèmes de procédure pénale liés à la technologie de l'information (Recommandation no R (95) 13 et exposé des motifs), Editions du Conseil de l'Europe, Strasbourg, 1996, note 14.

الأوروبي⁽¹⁾، و نفس المصطلح تبناه المرشد الفيدرالي الأمريكي لتفتيش و ضبط الحواسيب وصولاً للدليل الإلكتروني في التحقيقات الجنائية⁽²⁾. على العكس من ذلك، هناك إتجاه آخر يؤيد خلع صفة الرقمية على الدليل المعلوماتي بحجة أنّ التفوق اليومي للرقمية⁽³⁾، و هي ذات الحجة التي تستند إليها كل من المنظمة الدولية للمعايير (ISO) و اللجنة الكهروتقنية الدولية (IEC) في تفضيلهما لهذا المصطلح الذي يشير وفق تصورهما إلى البيانات الموجودة بالفعل في شكل رقمي باستثناء البيانات الأخرى التي تمّ تحويلها فيما بعد إلى بيانات رقمية⁽⁴⁾، و ينفرد التشريع السوري و المصري من بين التشريعات العربية بتبنيهما لهذا المصطلح صراحة ضمن القوانين المتعلقة بمكافحة الجرائم المعلوماتية⁽⁵⁾.

(¹) عمر محمد بن يونس، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي المرشد الفيدرالي الأمريكي لتفتيش و ضبط الحواسيب توصلاً إلى الدليل الإلكتروني في التحقيقات الجنائية - ترجمة و دراسة و تحقيق - الطبعة الثانية، دار النهضة العربية، مصر، 2006، ص 31.

(²) H. Marshall Jarrett, et al, op cit , p 7.

و للأمانة العلمية فقد تمّ الإعتماد في ترجمة هذا المؤلف على كتاب عمر محمد بن يونس، المرجع السابق، لما يتميز به من دقة في الترجمة رغم أن الطبعة المترجمة ترجع إلى 2004 في حين اعتمدنا طبعة 2009 من هذا المرشد، و قد كان مرجعنا الوحيد في الترجمة خاصة في الشطر المتعلق بترجمة الأحكام التي تضمنها.

(³) حيث تمّ اعتماد مصطلح "الدليل الإلكتروني" ضمن هذا المقترح و على الأخص ضمن الفقرة 06 من المادة 02 من هذا المقترح و التي جاء فيها أنّ مفهوم الدليل الإلكتروني ينصرف إلى "الأدلة المخزّنة في شكل إلكتروني من قبل مزود الخدمة أو من في حكمه وقت إصدار أمر بإنتاج بيانات معلوماتية أو حفظها، و التي تتألف من بيانات المشتركين و بيانات الولوج و كذا بيانات المعاملات و بيانات المحتوى".

Article 2 alinéa 6 de la Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale COM/2018/225 final - 2018/0108 (COD) stipule: "preuve électronique , preuve stockée sous forme électronique par un fournisseur de services ou en son nom au moment de la réception d'un certificat d'injonction de production ou de conservation, consistant en données stockées relatives aux abonnés, à l'accès, aux transactions et au contenu ".

(⁴) Sveva Avveduto, et al , op cit , p173.

(⁵) حيث تكرّر هذا المصطلح في مادة التعريفات و كذا المادة التي عالجت حجية هذا الدليل في كل من التشريعين، حيث تنص المادة 24 من المرسوم التشريعي السوري رقم 17 لسنة 2012 المتعلق بتطبيق أحكام قانون التواصل على الشبكة و مكافحة الجريمة المعلوماتية على ما يلي: "حجية الدليل الرقمي:

(أ) يعود للمحكمة تقدير قيمة الدليل الرقمي شريطة تحقّق مايلي: 1- أن تكون الأجهزة الحاسوبية أو المنظومات المعلوماتية المستمدّة منها هذا الدليل تعمل على نحو سليم. 2- ألاّ يطرأ على الدليل المقدم إلى المحكمة أيّ تغيير خلال مدّة حفظه.

بالنسبة إلى القضاء فإنّ حادثة اللّجوء إلى هذا الدليل جعلته يتردّد في استعمال مصطلح معيّن، على الرّغم من قبوله إياه و الإعتداد به لتكوين الإدانة و البراءة، و نجد أنّ القضاء في المملكة العربية السّعودية يميل نحو إستعمال لفظ الدليل الرّقمي و هو ما تجسّد بقرار حديث صادر عن الهيئة العامة للمحكمة العليا بالسّعودية بتاريخ 12 جانفي 2018 تحت رقم 34 جاء فيه "إنّ الدليل الرّقمي حجة معتبرة في الإثبات متى سلم من العوارض و يختلف قوة و ضعفاً حسب الواقعة و ملابساتها و ما يحتف بها من قرائن"⁽¹⁾، و في حدود البحث الذي أجريناه فإنّه لا يوجد لهذا المصطلح أو غيره موقعا له في قضاء المحكمة العليا الجزائرية⁽²⁾.

مع أنّ لكلّ تسمية من هذه، يمكن أن يجد لها مستخدمها ما يسوّغ إطلاقها، إلا أنّ كليها محل نظر في تقديرينا، فكلّ من الرّأي الأوّل و الثّاني يستمدّ مقوماته من منطق الرّقمية، مهملا ما يجب أن يكون عليه مدلول المصطلح من جمع بين البعدين التّقني و القانوني، باستخدام مصطلح ترقى دقته و وضوحه لما هو مطلوب في القانون الجنائي الإجرائي، فسواء كان الدليل رقميا "مؤلد رقميا"، أو إلكترونيا "غير مؤلدة رقميا" و تمّت رقمته لاحقا، ففي الأخير يصبح كليها من طبيعة رقمية، تلك الطّبيعة التي تعبّر عن حالة البيانات في وضعها الخام كتعداد غير محدّد لأرقام ثنائية لا يفهما سوى الحاسوب، و يتمّ إستردادها كمخرجات في

(ب) يعدّ الدليل الرّقمي المقدم إلى المحكمة مستجمعا للشّروطين الواردين في الفقرة (أ) من هذه المادة مالم يثبت العكس".

و بذات السّياق تقرّيبا وردت المادة 11 من القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات و التي جاء في متنها: "في الأدلة الرّقمية: يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدّات أو الوسائط أو الدعامات الإلكترونية، أو النّظام المعلوماتي أو من برامج الحاسب، أو من أيّ وسيلة لتقنية المعلومات نفس قيمة و حجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشّروط الفنية الواردة باللائحة التنفيذية".

(1) القرار الصّادر عن الهيئة العامة للمحكمة العليا بالسّعودية بتاريخ 12 جانفي 2018 رقم 34 منشور على الانترنت عبر الرابط <https://juwatha.net/250388.html> و تمّ تصفح الموقع في 20 جانفي 2018 .

(2) إعتد القضاء الجزائري في عديد من قراراته على الدليل المعلوماتي في بناء حكم الإدانة دون أن يتمسك بتسمية واضحة لهذا الدليل الجنائي، و مثال ذلك القرار الصّادر عن المحكمة العليا حديثا و الذي جاء في موجزه "تعدّ المكالمات الهاتفية المسجّلة على المستند الإلكتروني المتمثّل في بطاقة ذاكرة الهاتف النقال، من ضمن الوسائل التي يمكن للقاضي الأخذ بها لإثبات جريمة الزّنا"، أنظر القرار الصّادر عن المحكمة العليا غرفة الجنح المخالفات بتاريخ 29 مارس 2016 رقم 1010894، المجلة القضائية للمحكمة العليا، قسم الوثائق و الدّراسات القانونية و القضائية، العدد 01، 2016، ص301.

شكل نصوص و صور ثابتة و متحرّكة و صوت و أرقام و حروف و رموز و إشارات بعد معالجتها، لتصبح في شكل معلومات تنبئ عن حقائق معيّنة لها دلالة مفيدة في كشف الحقيقة، و تلك هي الغاية المرجوة من الدليل الجنائي⁽¹⁾.

و بطبيعة الحال فإنّه لا يمكن تقديم البيانات في وضعيتها الرّقمية كدليل جنائي، بل تُقدّم في شكل معلومات تحمل تسجيلًا مجردًا للواقعة الرّقمية أو الإلكترونيّة و تفسيرا لها، أي تصبح المعلومات -إن جاز القول- بمثابة "حقائق عن الواقعة الرّقمية أو الواقعة المادية"، و في هذه المرحلة تتخذ المعلومات صورة "مرئية" على جهاز العرض منبّنة عن حقيقة الواقعة الجرمية من زوايتين إحداها مادية تتصل بمادية الواقعة أو معلوماتية ترتبط بحالة البيانات الرّقمية، و الأخرى شخصية تتعلّق بشخص الجاني، فالمعلومات أعمّ و أدقّ في دلالتها، لذا نرى الإصرار على دقّة مصطلح "الدليل المعلوماتي" دون غيره من الألفاظ المستعملة في تسميته⁽²⁾.

(¹) إنّ القيمة الفلسفية للبيانات (Data) لا تكمن في حيازتها، بقدر ما ترتبط بإمكانية العمل على استردادها، فالقيمة الإستردادية للبيانات تتمثّل في مدى إمكانية استرداد معلومة محدّدة يكون الباحث في الحاجة إليها، لذلك فإنّ المفارقة بين الإثنين تعدّ قائمة حقا إذا تأملنا دور كل منهما، فالبيانات منطقة فلسفية تأملية لا تحتاج إلى تخزين و لا تحتاج إلى بثّ لها ما لم يكن المرء في حاجة إليها، لذلك فإنّ التخزين هو المقابل الحقيقي لفكرة البيانات في معنى عدم إمكانية الفصل بينهما. أمّا المعلومات (Information) فإنّها تتميز بالتحديد من حيث أنّ الإنسان إذا كان في حاجة إلى معلومات فإنّه لا يستطيع استرداد كافة المعلومات الممكنة، و إنّما يظلم في حاجة إلى تحديد معلومة معيّنة في كلّ مرة يحتاج فيها إلى هذه أو تلك المعلومة و في هذا فإنّ العملية الإستردادية للمعلومات من البيانات المخزّنة في الحاسوب أو في العالم الافتراضي تتشابه مع تلك العملية التي يمارسها العقل حال استرداده لمعلومة مخزّنة في ذاكرته (منطقة التخزين ذات مستهدف إستردادي بالضرورة)، فمنطقة النّجواب بين عبارة البيانات و بين القيمة الإستردادية لها تتمثّل في المعلومات. راجع تفصيلا: عمر محمد بن يونس، المرجع السابق، ص 20.

(²) و لا يُغيّر من موقفنا هذا، قول جانب من الفقه (عمر محمد بن يونس، المرجع السابق، ص 36 و ما بعدها) أنّ ربط الدليل الرّقمي بفكرة المعلومة يجعل موضوع الدليل الرّقمي يؤدي دوره في إطار عملية إسترجاع أو إسترداد المعلومات فقط، بحيث لا يكون دليلا سوى كل ما يمكن إسترجاعه أو إسترداده من معلومات، في حين أنّ منطق التّعامل مع الحاسوب يمكن أن يكون أساسه التّعامل مع بيانات متكاملة قد يكون من المعتاد ظهورها على شاشة الحاسوب لكي يمكن التّعرف عليها، و لكن لا يعدّ ذلك شرطا يلزم وجوده. و في تقديرنا فإنّ هذا النّقد يعبر عن مفهوم خاطئ لمدلول المعلومة، فكلّ بيان يتمّ إسترجاعه يعتبر معلومة و لو تعذر على غير المتخصّص إدراك معناها لما تمتاز به من تعقيد يترجمه الخبراء عن طريق برامج خاصة إلى معلومات تظهر على شاشة العرض، أو وحدة المخرجات و لو سلّمنا جدلا بصحة هذا النّقد بأنّه توجد أحوال تشكّل فيها البيانات دليلا جنائيا يدركه الحاسوب

و قد اعتمد المشرع اللبناني هذا اللفظ ضمن القانون رقم 81 لسنة 2018 و المتعلق بالمعاملات الإلكترونية و البيانات ذات الطابع الشخصي، دون غيره من التشريعات العربية على أنه أشار أيضا إلى مصطلح الدليل الرقمي⁽¹⁾.

المطلب الثاني: خصائص الدليل المعلوماتي المستمد من التفتيش

يتميز الدليل الجنائي المعلوماتي بعدة خصائص تميزه عن غيره من الأدلة التقليدية، تقوم على مدى ارتباطه بالبيئة التي يحيا فيها، و هي البيئة الافتراضية بحيث يقتضي إسترداده اللجوء إلى وسائل علمية (فرع أول)، كما أنّ هذا التكوين الرقمي الثنائي ذو طبيعة تقنية (فرع ثاني) و هو بذات الوقت كثير التنوع و سريع التطور (فرع ثالث).

الفرع الأول : الدليل المعلوماتي دليل علمي

الدليل المعلوماتي عبارة عن آثار رقمية يتركها الجاني في مسرح الجريمة تعكس ظروف ارتكاب الفعل الجرمي و تفسر أساليب اقترافه، و هذه البصمات (digital print) ذات مبنى علمي خالص بحكم منشئها في هذه البيئة، ذلك ما يجعل الدليل المعلوماتي يتعدّد على غير المتخصّص إسترجاعه أو الإطلاع عليه⁽²⁾، إذ يستلزم تحصيله استعمال أساليب علمية بالغة

و لا يعدّ ظهوره على شاشة العرض شرطا لازما لاعتباره كذلك، فما الذي يقدّم إلى القضاء في هذه الحالة كدليل يحقّق حالة اليقين لدى القاضي للحكم بالبراءة أو يبرّح موقف الشكّ لديه فيصون الأصل الإثباتي القائم على افتراض البراءة؟ أو بعبارة أخرى ما هي عناصر الدليل الجنائي في هذه الأحوال إذا اعتبرناه كذلك؟ هل هي الأرقام (0-1) كتمثيل للبيانات داخل ذاكرة وسيط التخزين؟ أم المعلومات؟ حول حقيقة عرض الدليل المعلوماتي في شكل مرئي "visible" في مرحلة الفحص الجنائي الحاسوبي يراجع :

Carrier Brian D, op cit, pp 7 et ss.

(¹) حيث تنص المادة 122 من القانون المشار إليه سابقا: "يعود للمحكمة تقدير الدليل الرقمي أو المعلوماتي و حجبه في الإثبات، و يشترط أن لا يكون قد تعرّض لأيّ تغيير خلال عملية ضبطه أو حفظه أو تحليله".

(²) و هو ما يقودنا إلى القول بالإرتباط بعلوم أخرى، إذ ترتبط الأدلة المعلوماتية بعلوم أخرى تساعد على إستخلاص الدليل و جمعه من مسرح الحادث لتحديد البصمة الرقمية و هذه العلوم يطلق عليها "علوم المعامل الرقمية"، و تشمل هذه العلوم علوم الكمبيوتر التي تقدّم المعلومات التكنولوجية الدقيقة، و هي مطلوبة لفهم المظهر أو الهيئة أو الكينونة الفريدة للدليل المعلوماتي، و لا يمكن إستخلاص هذا الدليل بالشكل الصحيح إلاّ من خلال وجود مختصين في هذه العلوم، كما تشمل علوم الأدلة المعلوماتية، علوم الأدلة الجنائية التي من شأنها أن تقدّم منظورا علميا لتحليل أيّ شكل من أشكال هذا الدليل، و تساهم علوم التحليل السلوكي للأدلة المعلوماتية، في الرّبط المحدّد بين المعارف التكنولوجية و بين الطّرق العلمية لاستخلاص الدليل المعلوماتي، و لفهم أفضل للسلوك الإجرامي التقني، و هذه

التعقيد، تتسارع في تطورها بدرجة تطوّر طرق إرتكاب الجريمة فهو دليل يحتاج إلى قدر من التجاوب مع البيئة التّقنية، وهذا يعني أنّه كدليل يحتاج إلى بيئته التّقنية التي يتكوّن فيها لكونه من طبيعة تقنية المعلومات⁽¹⁾. فهو مستمدّ مما يصنعه أهل علم الحاسوب من أراء و استنتاجات علمية على ضوء ما يتمّ الوصول إليه من برامج و أجهزة تقنية، إذ يعدّ من طائفة ما يعرف بالأدلة المستمدة من الآلة⁽²⁾. و من هنا نخلص - من باب المنطلق و اللزوم - أنّ هذه الخاصية تجعل الدليل المعلوماتي يخضع للقاعدة العامة التي يخضع لها الدليل العلمي و هي لزوم تجاوب الدليل العلمي مع الحقيقة كاملة وفقا للتّوجهات الفقهيّة الحديثة التي ترفض ما استقر تقليديا في الأذهان من كون "القانون مسعاه العدالة أمّا العلم فمسعاه الحقيقة" (Law seeks justice, Science seeks truth)، فلكلّ من القانون و العلم هدف واحد، و هو الوصول إلى الحقيقة و إن اختلفت شروط اعتماد الدليل العلمي من حيث ضرورة موثوقيته و مشروعية تحصيله من الناحية القانونية و دقّة تقنيات و تحاليل إستخلاصه من الناحية العلمية، يبقى التّرابط واضحا بين تقصي الحقائق القانونية و العلمية⁽³⁾.

العلوم مجتمعة تؤدي للكشف عن الدليل المعلوماتي و التّحقق من أصلته و مصدره كدليل يمكن تقديمه لأجهزة إنفاذ القانون، و تحديد خصائصه الفريدة و إصلاحه و إعادة تجميعه من المكوّنات المادية للحاسوب و عمل نسخة أصلية منه للتأكد من عدم وجود معلومات مفقودة أثناء عملية إستخلاص الدليل، كما يمكن جمع "الأثار المعلوماتية الرقمية" التي قد تكون تبدّلت خلال الشبّكة المعلوماتية و التّأكد من أنّ الدليل لم يتم العبث به و تعديله من خلال استخدام خوارزميات محدّدة و عن طريق هذه العلوم يمكن تحريز الدليل المعلوماتي لإثبات أنّه أصيل و موثوق به و يقع ضمن سلسلة الأدلة المقدّمة في الدّعوى و تحديد الخصائص المميّزة لكلّ جزء من الأدلة المعلوماتية مثل المستند الرقمي، البرامج و التّطبيقات و الإتصالات و الصّور و الأصوات و غيرها.

يراجع بهذا الخصوص: ناصر بن محمد البقمي، أهمّية الأدلة الرقمية في الإثبات الجنائي، دراسة وفقا للأنظمة السّعودية، مجلة الفكر الشّرطي، مركز بحوث الشّرطة القيادة العامة لشّرطة الشّارقة، الإمارات العربيّة المتحدّة، مجلد 21، عدد 80، 2012، ص 32-33.

(1) عمرو محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، المرجع السّابق، ص 977.

(2) ميسون خلف حمد الحمداني، مشروعية الأدلة الإلكترونيّة في الإثبات الجنائي، مجلة كلية الحقوق جامعة التّهرين، العراق، المجلد 18، العدد 2، 2016، ص 200.

(3) Howard A. Denmark, Search for Scientific Knowledge in Federal Courts in the Post-Frye Era: Refuting the Assertion that Law Seeks Justice While Science Seeks Truth, High Technology Law Journal, Vol. 8, No. 2 (1993), p 266.

و إذا كان الدليل العلمي له منطقته الذي يجب ألا يخرج عليه من حيث يجب عدم تعارضه مع القواعد العلمية السليمة، فإنّ الدليل المعلوماتي له ذات الطبيعة، إذ يجب ألا يخرج الدليل المعلوماتي عما توصل إليه العلم الرقمي و إلا فقد معناه.

و عدم الخروج عن متطلبات العلم الرقمي لا يعني أنّ هناك قواعد جامدة يرتبط بها هذا الدليل من حيث طبيعته العلمية، و إنّما يجب الأخذ في الاعتبار أنّ العلم الرقمي هو علم متطور جدا، بل إنه يجد ذاته في قدرته الكبيرة على التطور الذاتي المستمر، سيما من حيث كونه لا يستجيب للقاعدة التقليدية، حيث أنّه يمكن أن يكون هناك خبراء في العالم الرقمي لم يتم أيّ منهم منهج دراساته التقليدي المتبع في التدريس، و لا يملك الشهادات و الدرجات العلمية أيضا و مع ذلك برعوا في العلم الرقمي و أصبح كل منهم خبيرا فيه⁽¹⁾.

الفرع الثاني : الدليل المعلوماتي من طبيعة تقنية متطورة

تسمّى هذه الطبيعة بالطبيعة الثنائية للدليل المعلوماتي، و مفاد ذلك أنّ هذا الدليل يتكوّن من تعداد غير محدود لأرقام ثنائية في هيئة الواحد و الصفر (1-0) و التي تتميز بعدم التشابه فيما بينها رغم وحدة الرّم الثنائي الذي تتشكّل منه، فمثلا البيانات المخزّنة في الحاسوب سواء كانت في شكل نصوص أم حروف أم صور ليس لها الوجود المادي الذي عرف في شكل ورقي، و إنّما هي مجموعة من الأرقام ترجع إلى أصل واحد⁽²⁾.

هذا الذي يجعل الدليل المعلوماتي ذو طبيعة تقنية و فنية و كيفية معنوية غير ملموسة، لا يدرك بالحواس الطبيعية و يتطلّب إدراكه الإستعانة بأجهزة و معدّات و أدوات الحاسبة الآلية و استخدام نظم برمجية حاسوبية، و هو على الهيئة المار بيانها عبارة عن مجالات مغناطيسية كهربائية، و من ثمّ فإنّ ترجمة الدليل المعلوماتي و إخراجها في شكل مادي ملموس لا يعني أنّ هذا التجميع هو الدليل، فهي العملية لا تعدو أن تكون مجرد نقل لتلك المجالات من طبيعتها الرقمية إلى الهيئة التي يمكن الإستدلال بها على معلومة معيّنة⁽³⁾.

(1) عمرو محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، المرجع السابق، ص 978.

(2) فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي، رسالة دكتوراه، كلية الحقوق جامعة الجزائر 1 بن يوسف بن خدة، الجزائر، 2017، ص 227.

(3) محمد علي سالم، الإثبات الجنائي عبر الوسائل الإلكترونية دراسة مقارنة، بدون رقم الطبعة، دار المطبوعات الجامعية، مصر، 2020، ص 349.

فالدليل المعلوماتي إذن ليس مثل الدليل التقليدي، إذ لا تنتج التقنية سكيناً يتم به إكتشاف القاتل أو إعترافاً مكتوباً أو مالا في جريمة الرشوة أو بصمة إصبع... إلخ. وإنما ما تنتجه التقنية هو نبضات رقمية تتشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب على أية شاكلة يكون عليها، و من ثمّ فإنّ إطلاق الصفة الرقمية إنّما تعني إنّهُ ينبغي أن يكون هناك توافق بين الدليل المرصود و بين البيئة التي يعيش فيها. و مثل هذا الأمر يجعلنا نقرّر أنّه لا وجود للدليل المعلوماتي خارج بيئته التقنية، و إنّما يجب لكي يكون هناك دليل و جب أن يكون مستوحى أو مستتبطن أو حتّى مستجلب من بيئته التي يعيش فيها و هي البيئة الرقمية⁽¹⁾، فهناك توافق بين هذا النوع من الأدلة و بيئة تقنية المعلومات إذ لا وجود لهذا الدليل خارج بيئة التقنية⁽²⁾.

الفرع الثالث: الدليل المعلوماتي مفهوم يحتوي التنوع و التطور

توصلنا فيما سبق إلى أنّ مصطلح الدليل المعلوماتي يشمل كافة أشكال و أنواع البيانات الرقمية الممكن تداولها رقمياً، بحيث يكون بينها و بين الجريمة رابطة من نوع ما، و تتصل بالضحية على النحو الذي يحقّق هذه الرابطة بينها و بين الجاني، بما يقيم علاقة أساسية بين البيانات الرقمية و بين الدليل المعلوماتي، لكون هذا الأخير إنّما هو القالب الذي يحتوي في داخله مجموعة البيانات الرقمية، فإنّ ذلك يعدّ تعبيراً عن إتساع قاعدة الدليل المعلوماتي، بحيث يمكنه أن يشمل أنواعاً متعدّدة من البيانات الرقمية تصلح منفردة أو مجتمعة لكي تكون دليلاً للإدانة أو للبراءة. إذ يشمل هذا التنوع من البيانات الرقمية مظاهر عدّة، كأن يكون هذا المحتوى معلومات متنوّعة تتضمّن نصوصاً و صوراً و سمعيات و مرئيات⁽³⁾.

و على الرّغم من كون أساس تكوين الدليل المعلوماتي واحد و هو لغة الحاسوب أو الرقمية، إلّا أنّه قد يتخذ أشكالاً مختلفة و متنوّعة فقد يكون واضحاً و مقروءاً و مفهوماً للبشر كما لو كانت وثيقة مكتوبة و معدّة بنظام المعالجة الآلية، بيد أنّه قد يتخذ أشكالاً أخرى مبهمّة

(1) عمرو محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، المرجع السابق، ص 979.

(2) حسن عواد السريحي، دور البحث الجنائي في الكشف عن الجرائم المعلوماتية، رسالة دكتوراه، كلية العدالة الجنائية جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2016، ص 80.

(3) عمرو محمد أبو بكر بن يونس، المرجع نفسه، ص 980.

و غامضة كالأدلة المتمثلة في إشارات رقمية يتم الحصول عليها من خلال المراقبة عبر الشبكات أو من خلال القائمين على تقديم خدمات الإتصال الإلكتروني عن بعد، و هذه الصورة هي التي تعبر عن التطور المستمر للأدلة المعلوماتية بسبب تطوّر علم المعالجة الآلية للبيانات⁽¹⁾.

فقابلية الدليل المعلوماتي للتطور تبقى متواصلة نظرا لإرتباطه الوطيد بالطبيعة المتغيرة و المتجددة التي تتمتع بها تكنولوجيات الإعلام و الإتصال⁽²⁾، و المتأمل لهذه الخاصية يستخلص انعكاساتها فيما تطرحه من تحديات للوصول إلى الدليل، إذ ينعقد الإجماع لدى خبراء التحليل الحاسوبي على ضرورة مواكبة التطور الحاصل في مجال تقنية المعلومات لمواجهة الإجرام المعلوماتي على شبكة الأنترنت من خلال التوصل إلى تقنيات فعّالة للحفاظ على الأدلة على مدى فترات طويلة من الزمن، و تحقق أيضا فعّالية في تحليل البيانات و تطوير نظريات التحليل الحاسوبي الشرعي في المستقبل⁽³⁾.

لذلك يجب العمل على سد الفجوة بين ما هو متاح و بين ما هو ضروري، بغية معالجة هذا التنوع و التطور المتواصل للبيانات الرقمية، ففي الوقت الراهن فإن أدوات المعالجة المختلفة لتفسير البيانات لا تزال محدودة، حيث أنه ليس بإمكانها تفسير جميع أنواع البيانات و هي الحقيقة التي أكدها الفريق العامل المعني بتنسيق و تخزين الأدلة الرقمية المشتركة⁽⁴⁾.

المطلب الثالث: ذاتية الدليل المعلوماتي المستمد من التفتيش

تكشف خصائص الدليل جانبا من ذاتيته، تلك الذاتية بوجهيها السلبي و الإيجابي، مرتبطة جدليا بمفهوم التوازن بين حرية الإثبات و شرعيته فكأما زادت صعوبة التوصل إلى الدليل و جب التساهل في البحث عنه و تلك المقاربة تثير في معرض دراستنا تساؤلا حول الجوانب السلبية للدليل المعلوماتي (فرع أول)، و جوانبه الإيجابية (فرع ثاني).

(1) محمود عبد الغني فريد جاد المولى، دور الدليل الإلكتروني و دوره في المجال الجنائي، رسالة دكتوراه، كلية الحقوق جامعة بنها، مصر، 2016، ص 28.

(2) رشيدة بوكر، المرجع السابق، ص 388.

(3) Eoghan Casey, Susan W. Brenner, op cit, p 206.

(4) Frank Adelstein, Live forensics: diagnosing your system without killing it first, Communications of the ACM, V 49, N 2, 2006, p 63.

الفرع الأول: الجوانب السلبية للدليل المعلوماتي المستمد من التفتيش

يتميز الدليل المعلوماتي بحكم طابع تكوينه و بيئته في بعض مظاهره بطابع خاص كثيرا ما يضيف عليه طابعا سلبيا تجعل أمر اكتشافه و الوصول إليه و استرجاعه آية في التعقيد، فهو دليل هش و غير مستقر (أولا)، يصعب استرداده (ثانيا)، و نسبه إلى مقترف الجريمة (ثالثا).

أولا: الطابع غير المستقر للدليل المعلوماتي المستمد من التفتيش

الأدلة المعلوماتية هشة بطبيعتها، فهي قابلة للتآكل أو الإتلاف أو التدمير من خلال سوء المناولة أو الفحص بطريقة غير سليمة، و لهذا السبب ينبغي إتخاذ احتياطات خاصة من أجل توثيق هذا النوع من الأدلة الإثباتية و جمعه و الحفاظ عليه و فحصه، و قد يؤدي عدم القيام بذلك إلى جعل هذه الأدلة غير صالحة للإستعمال أو يُفسي إلى استنتاجات غير دقيقة⁽¹⁾. بحيث تختلف الأدلة المعلوماتية عن جميع الأدلة الأخرى في أنه يمكن أن تتغير من لحظة إلى أخرى داخل الحاسوب أو النظام المعلوماتي أو أثناء الإرسال، و يمكن بسهولة تغيير الأدلة المعلوماتية بدون أي أثر واضح يسهل إكتشافه، بل يمكن أن يقع التغيير بحسن نية أثناء القيام بجمعها من قبل السلطة الإجرائية المختصة، و هو ما يثير إشكالية التيقن من موثوقيتها، بما يجعل عامل الوقت في الوصول إليها أمر حاسم في هذه المسألة⁽²⁾.

و لأنّ الأدلة المعلوماتية أدلة ظرفية، يجب هنا إحداث مقارنة بين الدليل المعلوماتي و بين الحمض النووي (DNA)، و ذلك لاتحاد كليهما في هذه الخصيصة، حيث يمكن إحداث تعديل في تكوينهما معا، و هذا ما يجعل الدليل المعلوماتي يتميز بطبيعة إحصائية إلى حد ما، و يجعل محاولة إعادة بناء وقائع القضية أمرا صعبا للغاية. و هو ذات الأمر الذي يسري على الشهادة إذا مضت عليها مدة طويلة من الزمن فإنّ مسألة الإستعانة بها تخضع لتحقيق متواصل بحيث يجب التعرف على مدى قدرة الشاهد على التذكر و العوامل المؤثرة في الذاكرة بل و قد تكون الشهادة خاطئة أو مظللة. و في هذا الصدد، فإنّ الإستنتاجات المستخلصة من

(1) U.S. Department of Justice , Forensic Examination of Digital Evidence: A Guide for Law Enforcement, National Institute of Justice , Washington, 2004, p 11.

(2) Eoghan Casey, Susan W. Brenner, op cit, p 165.

الأدلة المعلوماتية تخضع للتدقيق بالطريقة ذاتها التي يتم بها إختبار السكين الموجود في مكان القتل لمعرفة الحمض النووي و بصمات الأصابع للتعرف على المشتبه فيه أي أنها أدلة تعزز أدلة أخرى⁽¹⁾.

و يترتب على هذه الإشكالية مسائل هامة في القانون، أبرزها على الإطلاق مسألة موثوقية الأدلة المعلوماتية التي يتوقف عليها مصير المتهم، فنظرا لما يمكن أن تخضع له طرق الحصول عليها من التعرض للتزييف و التحريف و الأخطاء المتعددة فقد توجس منها كل من القضاء و الفقه خيفة من عدم تعبيرها عن الحقيقة⁽²⁾.

ثانيا: صعوبة الوصول إلى الدليل المعلوماتي

ترجع الصعوبة في الوصول إلى الدليل المعلوماتي إلى طبيعة الوسط الذي يعيش فيه و الذي هو عبارة عن عالم غير محدود من البيانات تختلط فيه البيانات الخرجة عن نطاق الأذن القضائي مع غيرها التي تعدّ موضوعا للدليل الجنائي، و تلك السعة التخزينية التي تتزايد بشكل مذهل كل يوم، استغلها الجناة بكلّ ضراوة لجعل الأدلة مخفية أو مضغوطة أو مفحّخة أو تحمل عناوين مظلمة أو مشفرة أو مدفونة ضمن مساحة التخزين الفارغة، بطرق

(1) Richard boddington, practical digital forensics, first edition , packt publishing , London, 2016, pp 65-66.

(2) و يظهر هذا التردد لدى القضاء الأمريكي بشكل كبير جدا من خلال عديد الأحكام التي أبدى فيها تشددا ملحوظا حيال هذه المسألة و مثال ذلك ما قضت به المحكمة الإبتدائية (منطقة) Nebraska و تحديدا في قضية U.S. v. Jackson التي ترجع وقائعها إلى سنة 2006 أين تظاهر أحد رجال الشرطة السريين بأنه فتاة مراهرة تبلغ من العمر 14 سنة أثناء محادثة بينه و بين المتهم عبر الأنترنت، على إثرها قدّم المتهم للمحاكمة عن جريمة تحريض فتاة قاصر على القيام بممارسات جنسية، رفضت المحكمة قبول الدليل المعلوماتي المستمد من المحادثة التي دارت بين الضابط و المتهم من خلال غرفة المحادثة على شبكة الأنترنت في شكلها المطبوع كبديل عن المحادثة الإلكترونية الأصلية التي جرت بينهما و التي فقدت لسبب من الأسباب، على الرغم من أنّ ضابط الشرطة ادعى أنّه قام بتخزين المحادثة من خلال النقر عليها و سحب كامل النص و نقله على شكل وثيقة مكتوبة، إلا أنّ المحكمة لاحظت وجود طرق أفضل لتخزين الوثيقة و لم يتم استخدامها، يضاف إلى أنّ التناقضات في المحادثة المخزنة تشير إلى أنّ هناك أجزاء منها قد تعرضت للحذف و لا توجد أيّ إشارة في المحرّر الذي يتضمن المحادثة التي أجريت مع المتهم إلى أنّ المتهم يحاول أن يرتب لقاء مع الضحية المزعومة.

راجع الحكم U.S. v. Jackson, 488 F. Supp. 2d 866. مشار إليه لدى: سامي حمدان الرواشدة، الأدلة المتحصلة من مواقع التواصل الاجتماعي و دورها في الإثبات الجنائي دراسة في القانون الإنجليزي و الأمريكي، المجلة الدولية للقانون، كلية الحقوق جامعة قطر، قطر، المجلد 3، 2017، ص 16.

تجعل من المستحيل إكتشافها بسهولة⁽¹⁾، أمّا إذا كانت هذه الأدلة مخزّنة ضمن الحوسبة السحابية فإنّ الأمر بلا ريب يزداد تعقيدا و يستنفذ وقتا طويلا يستغلّه الجاني للعبث بالأدلة بالقدر الذي إستطاع إليه سبيلا.

و حقيقة هذا التعقيد الفتي تفرض تحديًا آخر يكمن في التكاليف الباهظة التي تتطلبها عملية التفتيش عن الدليل المعلوماتي و استرداده، فقد وصلت المصاريف القضائية الخاصة بالخبراء في إحدى القضايا المدنية للقيام بمراجعة البيئة التي يرجح أن يتواجد فيها الدليل المعلوماتي و المتمثلة في فحص و مراجعة ثلاثين مليون صفحة رقمية مخزّنة ضمن حاسوب المدعى عليه إلى خمسين ألف دولار و عادة ما تتعلّق هذه النفقات ببذل إنجاز برامج تكفل القيام بهذه التحاليل الحاسوبية⁽²⁾، و بطبيعة الحال فإنّ هذه التكلفة تتضاعف في مجال التحليل الحاسوبي الشرعي بحكم التعقيد الذي يفرضه الجناة، في الوقت الذي قد لا تقدّم فيه هذه المحاولات شيئا مفيدا في الإثبات على الإطلاق.

كما أنّ الأدلة المعلوماتية تمتاز بسرعة حركتها عبر شبكات الإتصال و تتسم أيضا بسعة إمتدادها عبر الفضاء بدون حدود و لا قيود، و في هذا الصدد يطرح البعد الدولي لجمع هذا النوع من الأدلة تحديات فريدة أمام التعاون الدولي، فنظراً للطابع غير المستقرّ الذي تتميز به يقتضي التعاون الدولي استجابة سريعة و قدرة على طلب إجراءات تحقيق خاصة، بما في ذلك حفظ البيانات و توفيرها.

و تشمل التحديات الشائعة لدى طلب تلك البيانات من ولاية قضائية أخرى حالات التأخير في الإستجابة للطلبات، و عدم الإلتزام و المرونة من جانب السلطة التي تُطلب منها الأدلة المعلوماتية، و الشكّل الذي تُقدّم به هذه الأدلة إلى الدولة الطالبة و ما إذا كان يمكن أن تُستخدم في الإجراءات الجنائية، و في كثير من الأحيان قد تتجاوز هذه المدد الزمنية مدة احتفاظ مقدّم الخدمات للبيانات، أو قد يتمكن مرتكبو الجريمة خلالها من إتلاف الأدلة المعلوماتية الرئيسية تلفاً نهائياً.

(1) H. Marshall Jarrett, et al, op cit, p 76.

(2) Christine Sgarlata Chung and David J. Byer, The Electronic Paper Trail: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence, Journal of Science & Technology Law, V 179, boston university, 1998,p 14.

و مردّ هذه الصّعوبة لا يقف عند حد طبيعة تكوين الدّليل بحدّ ذاتها، بل تعتبر الأساليب الأمنية و تدابير الحماية الفنيّة التي يفرضها الجناة عمدا على عناصر هذا الدّليل من بين أهمّ العراقيل التي تحول دون استرداده أو حتّى الوصول إليه، إذ غالبا ما يضرب هؤلاء سياجا أمنيا على أفعالهم غير المشروعة و ذلك باستخدام كلمات المرور السّريّة و ترميز البيانات المخزّنة إلكترونيا بشكل يستحيل على سلطات التّحقيق تعقّب آثار الجريمة و استخلاص الدّليل المعلوماتي حولها دون الحصول على هذه الرّموز و التّشفير⁽¹⁾، و عادة ما يكون هذا التّشفير مرتبطا بفيروسات حاسوبية تعمل تلقائيا على حذف المحتوى الرّقمي بمجرد محاولة الولوج إلى النّظام المعلوماتي أو عند الخطأ في رمز التّشفير⁽²⁾.

ثالثا: صعوبة نسبة الدّليل المعلوماتي إلى متهم معيّن

و ذلك راجع إلى الطّبيعة الديناميكية للبيانات الرّقمية خاصة تلك الموزّعة عبر الشّبكات بحيث يستعصي جمع الأدلّة المعلوماتية و التّوصل إلى نسبة الجريمة إلى مقترفها، سيما إذا تمّ ارتكاب الجريمة عبر الإتصال بشبكة الأنترنت و ذلك لأنّ المستخدم غير مجبر على الكشف عن هويته الحقيقيّة، إذ يتمّ الإستعارة بأسماء وهمية، و قد أتاحت التّقنية إنتحال شخصيات وهميّة بكفاءة عالية، و يرجع السّبب في ذلك إلى أنّ كثيرا من نظم المعلومات لا تسمح بالتّتبّع العكسي لسير المعلومات أو البيانات. كما أنّه لو أتيح ذلك فإنّ هذا يحتاج إلى مراجعة و فحص كم هائل من البيانات و المعلومات، فما تتيحه النّظم المعلوماتية مجرد

(1) في دراسة أجراها المعهد الوطني للعدالة الأمريكي شملت 126 شخص من أجهزة تنفيذ القانون، يمثلون 114 وكالة حكومية، أفاد 62 بالمائة من مجموع العيّنة أنّه ليس لدى مختبراتهم الجنائية القدرة على فك التّشفير أو أنّ قدرتها ضعيفة بينما أجاب 20 بالمائة أنّه لا يدري، و هذا مؤشّر على خطورة هذا الأسلوب و عدم جاهزية أجهزة العدالة الجنائية على التّعامل معه حتّى الآن.

راجع : تركي بن عبد الرّحمان المشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية و قياس فاعليته، رسالة دكتوراه، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السّعودية، 2012، ص 95.

(2) جدير بالذّكر أنّ عملية كسر التّشفير ليست بالأمر الهين، فقد أورد الفقيه "littman" في معرض سرده لكيفية مطاردة الهاكر الشّهير "كيفن متك"، كيف أنّ هذا الأخير قام بتشفير كامل ملفات الحاسوبية التي تمّ التّحفظ عليها كجزء من أدلّة الإدانة باستخدام المواصفات المعيارية DES و قد استطاع المحقّقون التّوصل إلى التّشفير المستخدم في عملية تمّت بواسطة كومبيوتر عملاق تابع لوزارة الطّاقة الأمريكيّة و قد استغرقت العملية عدّة شهور، و بتكلفة مالية وصلت إلى مئات الآلاف من الدّولارات، مشار إليه لدى: تركي بن عبد الرّحمان المشير، المرجع السّابق، ص 94.

بيانات غير مرئية لا تفصح عن شخصية معينة عادة، مسجلة إلكترونيا بكثافة بالغة و بصورة مرمزة لا يترك التعديل أو التلاعب فيها أي أثر، مما يقطع كل صلة بين المجرم و جريمته⁽¹⁾.

و إذا كانت الإستعانة بالمعلومات و العناوين و المصادر التي يحتويها (IP) يساعد حقيقة على الكشف عن مصدر الجهاز المستخدم في ارتكاب جريمة ما و موقعه و بالتالي الكشف عن المجرم الذي يفترض أن يكون صاحب هذا الجهاز، إلا أن النتيجة ليست دائما صحيحة و موثوقة، لأن ما يتم التوصل إليه من خلال التقنية السابقة هو عنوان رقمي للحاسوب المستخدم فحسب، و هذا لا يكفي وحده لإسناد الفعل الجرمي إلى صاحب الحاسب المذكور، إذ من المحتمل جدا أن لا يكون هذا الأخير هو مرتكب الجريمة⁽²⁾.

و هو ما يثير إشكالية أصالة الدليل خاصة بالنسبة للأدلة المستجلبه من الشبكة بحكم الطابع الديناميكي للبيانات بمجرد إنقراط حركة مرور تبقي النسخ فقط، ولا تتوفر البيانات الأصلية للمقارنة، يمكن توثيق كمية البيانات المفقودة أثناء عملية التجميع، و لكن لا يمكن إسترداد الأدلة المفقودة، و يزداد الأمر تعقيدا فيما لو كان الدليل المعلوماتي مستجلب من قاعدة مجهولة أو خوادم غامضة.

و من الطبيعي أن تفرز إشكالية أصالة الدليل المعلوماتي المستمد من التفتيش مسألة ذات أهمية بالغة في إطار نظرية الإثبات الجنائي، و هي مسألة الدفع بإنكار التأليف (صدر الفعل عن المتهم) خاصة تلك الأدلة المعلوماتية المستخلصة من مواقع التواصل الإجتماعي في ظل سهولة العبث بالملفات التعريفية لأي شخص، ذلك أن قاعدة مواقع التواصل الإجتماعي غير آمنة، فهي بوضع يمكن معه إختراق الموقع من قبل أي شخص آخر، و

(1) هشام محمد فريد رستم، "الجرائم المعلوماتية و أصول التحقيق الجنائي الفني و اقتراح إنشاء آلية عربية موحدة للتدريب التخصصي مقدّم إلى مؤتمر القانون و الكمبيوتر"، المنعقد في الفترة بين 1 و 3 ماي 2000، كلية الشريعة و القانون، جامعة الإمارات العربية المتحدة، الطبعة الثالثة، 2004، ص 424.

(2) و قد أكد القضاء الفرنسي هذه الاحتمالات في قضية شهيرة تدعى (Faurission) حين نشرت رسالة عنصرية ضد الصهيونية تحمل إسم الفرنسي "Robert Faurission" و لما اكتشفت على الموقع (Aaargh) الذي تم إيوائه في الولايات المتحدة الأمريكية، حركت دعوى قضائية ضد هذا الشخص إلا أن المحكمة لم تتمكن من إقامة الدليل على المتهم بأنه هو الناشر الفعلي للرسالة ذات المحتوى المجرم، و بناء عليه قضت بأن وجود إسم المتهم في ذيل الرسالة لا يثبت بأنه مصدرها الحقيقي، و لا يكفي الإعتماد عليه للحكم بالإدانة، طالما أن هذا الإسم يمكن لأي كان أن يكتبه بقصد التمويه و التظليل. مشار إليه لدى: براهيمي جمال، المرجع السابق، ص 203.

بناء عليه يمكن إستخدام الموقع و إرسال رسائل من خلاله لتبدو كأنها صادرة عن صاحب الموقع الحقيقي، و هي الحقيقة التي كرسها القضاء المقارن في كثير من أحكامه⁽¹⁾.

الفرع الثاني: مزايا الدليل المعلوماتي

الواقع أنّ تقنية المعلومات مثلما أضفت مظاهر سلبية على الدليل المعلوماتي فإنّها بذات الوقت أيضا أصبغت عليه طابعا إيجابيا يستبعد إستحالة الوصول إلى هذا النوع من الأدلة، فإن كان سريع التغير فهو سريع النسخ (أولا)، و إن كان سهل المحو من واجهة الجهاز فهو صعب التدمير من ذاكرته (ثانيا)، و إن تعدّرت نسبته إلى مقترف الجريمة بشكل مباشر فإنّ الأدلة المعلوماتية الهامشية قد تهوّن من هذه الصعوبة لوجوده في وسط ذي سعة تخزينية هائلة يؤدي ربطها إلى التوصل للفاعل (ثالثا).

أولا: الدليل المعلوماتي دليل قابل للنسخ

من بين أهمّ مزايا الدليل المعلوماتي أنّه قابل للنسخ بحيث يمكن الحصول على نسخة منه مطابقة للأصل⁽²⁾، و من أمثلة ذلك أنّه يمكن بسهولة نسخ موسوعة كاملة في فترة زمنية وجيزة لا تتعدّى دقيقة واحدة، كما أنّ الدليل المعلوماتي قد يترك عدّة نسخ من نفسه في أماكن عديدة مما قد يسهّل عمل السلطات الإجرائيّة المؤهّلة، فإذا ما قام شخص بإرسال بريد إلكتروني إلى شخص آخر و كان هذا الإرسال ذا محتوى مجرّم، فإنّه بالإمكان الحصول على

(1) راجع العديد من التطبيقات القضائية حول معايير تأكيد موثوقية الأدلة المعلوماتية المستمدة من التفتيش، الصفحة 326 و ما بعدها.

(2) يطلق على النسخة الرقمية لفظ "bitstream" أو "mage copy" هي نسخة نموذجية تختلف عن نوع النسخ التي تستخدم عادة بالنسخ من جهاز حاسوب لآخر، فالنسخ العادية تكرر فقط الملف المحدد، غير أنّ نسخة "bitstream" تكرر كلّ بت bit و بايت byte على محرك الأقراص المستهدف بما في ذلك جميع الملفات و المساحة الفارغة "slack space" و جدول الملفات الرئيسيّة و البيانات الوصفية بالترتيب الذي تظهر به على الأصل، و يتمّ ذلك من خلال استخدام برامج حاسوبية خاصة من قبل خبراء التحليل الحاسوبي و يتمّ حفظها "للقرأة فقط" توخيا من دخول أيّ تعديل على البيانات المخزّنة، على نحو يمكن مصادقتها بسهولة (اثبات أصالة الدليل المعلوماتي) و استخدامها كدليل جنائي، فأيّ تعديل على هذه النسخة مهما كان طفيفا يجعلها عديمة الفائدة كوسيلة للإثبات.

لمزيد من التفاصيل راجع :

Orin S. Kerr, Searches and Seizures in a Digital World, Harvard Law Review, Vol 119, Issue 2, (2005), pp 531et ss.

عدّة نسخ منه و التي تتواجد ضمن أماكن مختلفة كذاكرة جهاز المتهّم، أو من خلال الذاكرة الحاسوبية الموجودة لدى مزوّد الخدمة⁽¹⁾، أو عن طريق مساحة تخزين الموقع الذي تمّ إرسال الرّسالة عبره، و من مساحة تخزين الموقع المرسل إليه، و كذلك يمكن إسترجاعه عن طريق الولوج إلى ذاكرة حاسوب مقدّم الخدمة للمرسل إليه⁽²⁾.

و مثل هذا الأمر لاحظته المشرّع العربي و المقارن أين قام بإدخال تعديلات بمقتضاها يسمح بضبط الأدلّة المعلوماتية من خلال نسخ البيانات المخزّنة في نظم المعالجة الآلية للبيانات بقصد عرضها لاحقا على الجهات القضائية⁽³⁾.

و هذه الخاصية تعتبر من أهمّ وسائل الحفاظ على الدليل المعلوماتي ضدّ الفقد أو التّلف و التّغيير و التّحريف⁽⁴⁾، و في نظرها لا توجد أيّ وسيلة أخرى بديلة عنها للحفاظ على الدليل على حالته الأصلية، خاصة لمواجهة الضّخامة الهائلة لكمّيات البيانات المتعيّن فحصها للوصول إلى الدليل المستهدف ما يستغرق فترة طويلة تعطي للجاني فرصة لتغيير الآثار الرّقمية أو العبث بمصرح الجريمة و البديل العملي هو إجراء "الضّبط الرقمي العرضي الشّامل".

(1) Serge Migayron, Critères d'appréciation technique, vraies et fausses preuves numérique, Colloque du 13/04/2010. La preuve numérique à l'épreuve du litige. Les acteurs du litige à la preuve numérique (l'information numérique fait la preuve), p 19, Disponible à l'adresse: www.cnejita.org/.../CNEJITA-ACTESCOLLOQUE13042010-A5-V5.1-pdf, Consulté le 15 janvier 2018.

(2) محمود عبد الغني فريد جاد المولى، المرجع السابق، ص 47.

(3) و يتجلى ذلك من خلال المادة 06 من القانون الجزائري رقم 09-04 المؤرخ في 5 أوت 2009 المتضمّن القواعد الخاصة للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها K و المادة 124 من القانون اللّبناني رقم 81 لسنة 2018 و المتعلّق بالمعاملات الإلكترونيّة و البيانات ذات الطّابع الشّخصي و المادة 19 من إتفاقية بودابست حول الإجرام المعلوماتي، و المادة 31 من إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني و حماية البيانات ذات الطّابع الشّخصي، و المادة 27 من إتفاقية العربية لمكافحة جرائم تقنية المعلومات.

(4) عبد الناصر محمد محمود فرغلي، عبيد سيف سعيد المسماري، المرجع السابق، ص 15.

ثانياً: الدليل المعلوماتي يصعب التّخلص منه

الدليل المعلوماتي يمكن إسترجاعه بعد محوه، و إصلاحه بعد تلفه، و إظهاره بعد إخفائه⁽¹⁾، و جمع أجزائه بعد تشتيتها⁽²⁾، و هذه أهمّ خصائص الدليل المعلوماتي على الإطلاق، و يقصد بذلك قدرة الدليل المعلوماتي على الإحتفاظ بالمعلومات الموجودة خلال فترة زمنية طويلة بحيث يمكن الرجوع إليه في أيّ وقت، حيث أنّ الوسائط الإلكترونية تضمن الثبات و الإستمرار لما تتضمنه من معلومات⁽³⁾.

فالحاسوب يحتفظ بالملفات و البيانات حتّى بعد أن يعتقد المستخدم أنّه قام بحذفها، فعندما يتمّ حذف الملف فإنّ محتوى الملف يمكن إسترداده، ذلك أنّ المساحة التي كان يشغلها الملف تظلّ متاحة كما كانت قبل الحذف، إذا لم يقم نظام التشغيل بإعادة إستخدام هاتاه المساحة لملف آخر سيظلّ الملف المحدّد للحذف متاحاً لاستعادته، و بهذا يمكن إسترداد

(1) محمد علي سويلم، المرجع السابق، ص 351.

(2) و هو ما يطلق عليه "إعادة بناء المسرح المعلوماتي للجريمة"، فالآثار الرقمية تشمل رؤية لمسرح الجريمة الحقيقي و مسرح الجريمة المعلوماتي نفسه، فإذا كانت هناك جريمة وقعت بالفعل و استخدم الحاسوب بشكل ما في أحد أفعالها فإنّ رجال الشّركة يجب عليهم أن يبحثوا في كلا المسرحين، المسرح الحقيقي و المسرح المعلوماتي، و توجد ثلاثة أنواع من إعادة بناء الأدلة المعلوماتية، و هي الأدلة المعلوماتية التي تمّ العبث فيها أو محوها، و الأدلة المعلوماتية الصحيحة، و هناك نوع ثالث يطلق عليه بالأدلة المعلوماتية الهامشية، و يلاحظ أنّه من الضروري لإعادة بناء الدليل المعلوماتي أن تتمّ الإستعانة بهذه الأنواع الثلاثة، فالأدلة المعلوماتية الصحيحة يتمّ من خلالها إستخلاص المعلومات المتعلقة بالجريمة و المجرم من خلال البحث فيها، كما أنّ الأدلة المعلوماتية التي تمّ محوها أو العبث بها، يتمّ إعادة بنائها باستخدام برامج خاصة معروفة لهذا الأمر، و الأدلة المعلوماتية الهامشية هي أدلة رقمية تلعب دوراً حاسماً في إعادة ترميم الأدلة المحوّة أو التي تمّ العبث فيها، كما أنّها تكمل أوجه النقص في الأدلة المعلوماتية المستخلصة من الأدلة المعلوماتية الصحيحة عن علاقة المجرم بالجريمة المرتكبة، و إعادة بناء الدليل المعلوماتي تعتمد على نوعه و نوع الحاسوب و نظام التشغيل و إعدادات الحاسوب و بإصلاح الأدلة التالفة أو المحوّة و ربطها بالأدلة المعلوماتية الصحيحة و سدّ ثغراتها بالأدلة المعلوماتية الهامشية، و يؤدي ذلك إلى ما يسمى بإعادة بناء مسرح الجريمة الرقمي و ذلك لبيان الأعمال المحيطة بالجريمة و زمن الجريمة و مكانها بشكل يمكن من خلاله تقديم أدلة معلوماتية صحيحة صالحة للأخذ بها أمام أجهزة إنفاذ القانون.

يراجع بهذا الخصوص: مصطفى محمد موسى، التّحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشّركة، القاهرة، 2009، ص 218-219.

(3) عمرو محمد أبو بكر بن يونس، المرجع السابق، ص 977.

كمية كبيرة من البيانات من المساحة الفارغة على القرص الصلب، فالحذف يعني إخفاؤه من مجال الرؤية الخاصة بالمستخدم فقط مع إمكانية إسترداده مجدداً بطرق فنية⁽¹⁾.

و لهذا السبب ففي الغالبية العظمى من الحالات، يمكن إسترداد البيانات التي تم حذفها، و هذا يتوقف على حجم القرص مقارنة بحجم ما تمت كتابته مجدداً على هذا القرص خلال الفترة الزمنية الممتدة بين تاريخ حذف الملف و تاريخ إجراء التحليل الحاسوبي الشرعي⁽²⁾.

بخلاف ذلك، فإن الأدلة التقليدية التي يعرفها القانون تجد قوتها أمام القضاء في مسألة التسريع بالحصول عليها، فبصمات الأصابع مثلا يمكن أن تكون محل شك إذا طالت المدة بين ساعة ارتكاب الجريمة و بين الحصول عليها، و كذلك الشهادة إذا مضى عليها مدة طويلة من الزمن و كذلك يمكن التخلص من الأوراق و الأشرطة المسجلة إذا حملت في ذاتها إقرارات بارتكاب شخص أو أشخاص لجرائم بتمزيقها و حرقها، و كل ذلك بالطبع يجعل عملية التخلص من هذه الأدلة المادية أمرا سهلا، حيث إنها جمعها لن يكون من السهولة - بل و من الإستحالة بمكان - إسترجاعها أو إسترداد الدليل المستمد منها حيث أنه تم تدميرها كلية⁽³⁾.

و إذا كان هذا أمر الأدلة التقليدية، فإن الحال غير ذلك بالنسبة للأدلة المعلوماتية، حيث يمكن إستردادها، فموضوع التخلص من الدليل المعلوماتي باستخدام خاصية الحذف (delete) أو عن طريق تهيئة القرص الصلب (hard disk) أو استخدام الأمر (format) لا يعدّ من العوائق التي تحول دون إسترجاع الملفات المذكورة، إذ تتوفر برمجيات من ذات

(¹) Chan, Gerald. "Life after Vu: Manner of Computer Searches and Search Protocols." The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference 67. (2014), p 438.

(²) Stephen Mason, Daniel Seng, Electronic Evidence, Fourth edition, Humanities Digital Library, School of Advanced Study, University of London, 2017, pp 9-10.

(³) عمرو محمد أبو بكر بن يونس، المرجع السابق، ص 982.

الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التي تمّ إلغاؤها أو إزالتها من الحاسوب⁽¹⁾.

الواقع أنّ هذه الخاصية محل خلاف بين الخبراء و لا تحضى بالإجماع، على أنّ الرأى الرّاجح يعتبر هذا النوع من الأدلة بالغة الهشاشة و يمكن حذفها في زمن متناه القصر و بنقرة زر⁽²⁾، و يصدق هذا بوجه خاص على المعلومات المخزّنة في ذاكرة النّظام RAM و التي تحذف آليا عند قفل النّظام⁽³⁾ أو عند وجود نظام التّشفير فإن لم يتم التمكن من حذفها فإن امكانية التلاعب بها عن طريق التعديل تبقى قائمة و مرجحة، و معنى ما تقدّم أنّ النّشاط الذي يقوم به الجاني للتخلّص من الدليل المعلوماتي بمحوه يعتبر بحد ذاته دليلا، حيث أنّ هذا الفعل يتمّ تسجيله في الحاسوب و يمكن اعتباره دليل إدانة آخر في حدّ ذاته⁽⁴⁾.

(1) ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم، عبد الله عبد العزيز، نموذج مقترح لقواعد إعتقاد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة و القانون، المنعقد في الفترة بين 10 و 12 ماي 2003، كلية الشريعة و القانون، جامعة الإمارات العربية المتحدة، المجلد 5، ص 2240.

(2) من الأمثلة الواقعية على ما تقدم ما حصل في دولة الإمارات العربية المتحدة، حيث قام مشغّل حاسوب بتهديد المؤسسة التي يعمل لديها بتنفيذ مجموعة من مطالبه، و ذلك بعد أن حذف كافة البيانات الموجودة على الجهاز الرئيسي للمؤسسة، و قد رفضت المؤسسة الإستجابة لمطالبه فأقدم على الإنتحار، و وجدت المؤسسة صعوبة في إسترجاع البيانات التي كانت قد حذفت.

أنظر: هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية دراسة مقارنة، بدون رقم الطبعة، مكتبة الآلات الحديثة، مصر، 1994، ص 35.

(3) و هو ما توصل إليه القضاء الأمريكي (الدائرة الفيدرالية الإستئنافية السادسة) في قضية *United States v. Robert Paul Boyd* حيث جاء في القرار الفاصل فيها "إنّ قيام المتّهم بمسح الملفات التي تحتوي على صور داعرة للأطفال أثناء فترة الوضع تحت المراقبة يعدّ ذلك إتلافا منه للدليل أثناء تحقيق قائم، حيث أنّ فترة المراقبة يكون فيها المتّهم عرضة لأية تحقيقات أو تفتيش قد يجري على حاسوبه و بالتالي فإنّ تصرفه هذا يعدّ إتلافا للدليل الجنائي أثناء تحقيق قائم". راجع الحكم: *United States v. Robert Paul Boyd*, 312 F.3d 213 (6th Cir. 2002)، مشار إليه لدى: عمر محمد بن يونس، أشهر المبادئ المتعلقة بالإنترنت في القضاء الأمريكي، الطبعة الأولى، دار النهضة العربية، مصر، 2004، ص 817.

(4) قرّر القضاء الأمريكي (الدائرة الفيدرالية الإستئنافية السادسة) في قضية *United States v. Robert Paul Boyd* " أنّ قيام المتّهم بمسح الملفات التي تحتوي على صور داعرة للأطفال أثناء فترة الوضع تحت المراقبة يعدّ ذلك إتلافا منه للدليل أثناء تحقيق قائم، حيث أنّ فترة المراقبة يكون فيها المتّهم عرضة لأية تحقيقات أو تفتيش قد يجري على حاسوبه و بالتالي فإنّ تصرفه هذا يعدّ إتلافا للدليل الجنائي أثناء تحقيق قائم". راجع الحكم: *United States v.*

و في اعتقادنا فإنّ هذه الجريمة متى ثبت ارتكابها فإنّها تعتبر قرينة يستخلص منها ما يعزّز مصداقية الدليل المعلوماتي المستهدف بالإسترداد، و هو ما يجعل المشرّع الجنائي الجزائري مطالب في هذه النّاحية بتقوية عناصر النّصوص القانونية التي تجرّم التخلص من الأدلة بتشديد العقوبة خاصة و أن جريمة التخلص من الأدلة المعلوماتية قد لا تتم من المتّهم باقتراف الجريمة الأصلية بل بمساعدة أشخاص منعزلين تماما عن مكان تحقق النتيجة الجريمة⁽¹⁾.

ثالثا: الدليل المعلوماتي يحتوي على معلومات أكثر تفصيلا عن الوقائع

أشرنا فيما سبق إلى أنّ منطق عمل الحواسيب و الشبكات يؤخذ مفهومه على أساس علاقات تخزين البيانات فيه و القدرة على إستردادها، فالبيئة الرقمية تعدّ مجالا حيويا ضخما

(2002) 312 F.3d 213 (6th Cir. Robert Paul Boyd ، مشار إليه لدى : عمر محمد بن يونس، المرجع السابق، ص 817.

(¹) تنصّ المادة 43 من قانون الإجراءات الجزائية: "يحظر، في مكان ارتكاب جناية على كل شخص لا صفة له، أن يقوم بإجراء أيّ تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أيّ شيء منها قبل الإجراءات الأولية للتحقيق القضائي، و إلّا عوقب بغرامة 200 إلى 1.000 دج. غير أنّه يستثنى من هذا الحظر حالة ما إذا كانت التّغييرات أو نزع الأشياء للسلامة و الصّحة العمومية أو تستلزمها معاملة المجني عليهم و إذا كان المقصود من طمس الآثار أو نزع الأشياء هو عرقلة سير العدالة عوقب على هذا الفعل بالحبس من ثلاثة أشهر إلى ثلاثة سنوات و بغرامة من 1.000 دج إلى 10.000 دج".

و السّؤال المطروح في هذا الصّدّد مبناه مدى كفاية هذا النّص في العقاب على جريمة إتلاف الدليل المعلوماتي؟ لأنّ النّص الحالي لا يعاقب سوى على جريمة إتلاف الدليل المادي أو العبث بالمسرح المادي للجريمة، فيخرج عن نطاق دائرة التجريم و العقاب فعل محو الدليل المعلوماتي إنطلاقا من مبدأ عدم جواز التّوسّع في تفسير النّص الجنائي و تجريم سلوك لم يجزّمه المشرّع إحتراما للشّريعة الجنائية، و علّة هذا القصور التّشريعي ترجع إلى كون هذا النّص لم يشهد أيّ تعديل منذ سنه بموجب القانون رقم 82-03 المؤرخ في 13 فبراير 1982 المعدّل و المتمم للأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 و المتضمّن قانون الإجراءات الجزائية، الصّادر بالجريدة الرّسمية عدد 7 بتاريخ 16 فبراير 1982، و بديهي أنّ المشرّع الجزائري وقت سن هذا التّعديل التّشريعي لم يتنبأ بما يمكن أن يطرأ من تغيير على نظرية الإثبات الجنائي بالتّحول نحو الإثبات المعلوماتي، لذا فإنّ المشرّع الجزائري مطالب بالتّدخل لأجل تجريم هذا السلوك لكونه فعلا يشكّل إعاقة لسير العدالة مع تشديد العقوبة نظرا لخطورة هذا السلوك من جهة و لكون التّوصل إلى الدليل بعد تعريضه للمحو أو الإتلاف يتقل كاهل الهيئة الإجتماعية من النّاحية المادية بشكل كبير جدا، هذا على فرض التّوصل إليه لأنّ إسترداده يستنفذ الكثير من الجهد و الوقت و المال، في الوقت الذي قد يذهب كل ذلك سدا. فتضيع فرصة إثبات كلتا الجريمتين.

يمكنه تخزين مليارات من البيانات، فالقدرات التخزينية في البيئة الرقمية تستوعب كمًا هائلًا من البيانات بما من شأنه أن يوفر لسلطات التحقيق عددًا كبيرًا من الأدلة عن الجريمة محل التحقيق، و في معظم الأحيان فإنّ هذه المعلومات ينشؤها النظام الحاسوبي بدون علم مقترف الجريمة⁽¹⁾، كما هو الحال بالنسبة للبيانات الوصفية و التي تعدّ معلومات قيّمة في الإثبات الجنائي المعلوماتي⁽²⁾، و قد لاحظت محكمة العدل الأوروبية في معرض فصلها في مدى مشروعية الإحتفاظ بالبيانات الوصفية إلى أن تجميع هذا النوع من البيانات يعطي نظرة عن سلوك الفرد و علاقاته الإجتماعية و أفضلياته الخاصة و هويته تتجاوز حتى تلك التي ينقلها الوصول إلى المحتوى المعلوماتي⁽³⁾.

فالدليل المعلوماتي يرصد المعلومات عن الجريمة و يحلّلها بذات الوقت و بسهولة أكبر، مما يساعد على تسهيل هذه المهمة ضرورة قيام السلطات بالتركيز على الأحداث المهمة أو الوقائع الجوهرية، فتحديد الوقائع الأساسية يعدّ من أهمّ التّحديات التي تواجه سلطات إنفاذ القانون في مجال جمع الأدلة الجنائية المعلوماتية نظرا لما يواجهونه من كم هائل من بيانات

(1) Serge Migayron , op cit, p 20.

(2) تعمل البيانات الوصفية على إعادة بناء أكبر عدد ممكن من الأحداث التي وقعت على النظام لاستخلاص استنتاجات موثوقة بحيث تجيب على الأسئلة الرئيسية التي يطرحها خبراء التحليل الحاسوبي الشرعي مثل: "من المسؤول عن إجراء معين في النظام" و "من ارتكب الجريمة قيد التحقيق"؛ " ما هي الإجراءات التي تمّ تنفيذها فعليًا على النظام"، "متى تمّ تنفيذ هذه الإجراءات"، و "كيف تمّ تنفيذ هذه الإجراءات" أين تمّ الشروع في هذه الإجراءات "أين توجد الأدلة على النظام المعلوماتي"، "ماهية الدوافع الكامنة وراء الإجراءات"، و بالتالي فإنّ البيانات الوصفية المرتبطة بملف أو وثيقة تشير إلى من قام بإنشاء أو تعديل أو الوصول إلى الملف معين و تحدد أيضا عنوان IP، أو الرّمق التسلسلي للكمبيوتر بما يسمح بتحديد مكان الإتصال، و في حالة لجوء المجرّم إلى تغيير الملف بأيّة أداة، فإنّ تاريخ التعديل على مستوى البيانات الوصفية سيكون مختلفًا عن تاريخ الإنشاء و في ذلك قرينة على محاولة إخفاء الأدلة الجنائية.

حول أهمية البيانات الوصفية في التحقيق الجنائي الرقمي يراجع:

Usama Salama, Vijay Varadharajan, and Michael Hitchens, "Metadata Based Forensic, nalysis of Digital Information in the Web", Annual Symposium on Information Assurance & Secure Knowledge Management, 2012, Disponible à l'adresse : <https://pdfs.semanticscholar.org/eaf2/42704b6915e6b359218c1c6725c3245e65f0.pdf>, Consulté le 20 janvier 2018.

(3) Cour européenne de justice, arrêt de la Cour dans les affaires jointes C-293/12 et C-594/12, Digital Rights Irelan et Seitlinger et autres, Disponible à l'adresse : <https://eur-lex.europa.eu/legal content/FR/TXT/PDF/?uri=CELEX:62012CJ0293>, Consulté le 02 Février 2018.

مختلطة في مسرح الجريمة⁽¹⁾، فعلى سبيل المثال لا تعطي الصورة الملتقطة بواسطة كاميرا رقمية معلومات حول مضمون الصورة فحسب (السماء و ما فيها من سحب و الأرض و ما عليها من أشجار و الأشخاص و صفاتهم) و لكنها تعطي أيضا معلومات تفصيلية أخرى حول هذه الصورة تتمثل في نوع الجهاز الذي إستخدم في إلتقاط الصورة و تاريخ و ساعة الإلتقاط و إحدائيات الموقع الذي إلتقطت فيه الصورة⁽²⁾، فما تكشف عنه بيانات المستند الرقمي (المعادل الرقمي للظرف) من معلومات قد يتجاوز أحيانا ما يكشف عنه محتوى المستندات الورقية.

لعلنا نصل من خلال إستعراض شتى مظاهر الذاتية التي تميز الدليل المعلوماتي إلى حقيقة مؤداها أنّ هذه الطبيعة ستكون لها إنعكاساتها الواضحة على مركزه بين مختلف الأدلة الجنائية سواء التقليدية أو الحديثة ممثلة في الأدلة العلمية، و هو ما نفصله بالبيان في المبحث الثاني.

المبحث الثاني

تقسيمات الأدلة المعلوماتية المستمدّة من التفتيش و تصنيفها

ليس للدليل المعلوماتي هيئة واحدة، و إمّا له خصيصة الإلتصاق بمفهوم تكنولوجيا المعلومات من حيث تكوينه، و مثل هذا الأمر له تأثير على دور كلّ نوع من هذه الأنواع في الإثبات و مدى تعارضها مع الحريات الفردية، و اعتراف القانون بهذه الهيئات المتنوّعة التي يكون عليها الدليل المعلوماتي يفيد بالضرورة وجوب البحث عن تصنيف له بين الأدلة الجنائية التقليدية حتّى يمكن الإستناد إليه في بناء الإدانة او البراءة، لذا نستعرض في هذا المبحث تقسيمات هذا الدليل (مطلب أول) و تصنيفه (مطلب ثاني).

المطلب الأول: تقسيمات الأدلة المعلوماتية المستمدّة من التفتيش

جرت محاولات عديدة لتقسيم الأدلة المعلوماتية، فقد ميّزت الإتفاقية الأوروبية لمكافحة الجرائم المعلوماتية بين مختلف فئات الأدلة المعلوماتية على أساس درجة تعارضها مع الحق

(1) محمود عبد الغني فريد جاد المولى، المرجع السابق، ص 50.

(2) مصطفى إبراهيم العربي، دور الدليل الرقمي في الإثبات الجنائي، مجلة البحوث القانونية، كلية القانون جامعة مصراتة، ليبيا، مجلد 4، عدد4، 2016، ص ص77-78.

في الخصوصية (فرع أول)، بينما تبني الفقه معياراً آخر يتمثل في القيمة الإثباتية المنبعثة من مختلف صور هذا الدليل (فرع ثاني)، أمّا القضاء الأمريكي فقد إتخذ من محتوى الدليل أساساً للتقسيم (فرع ثالث).

الفرع الأول: تقسيم الأدلة المعلوماتية على أساس درجة تعارضها مع الحق في الخصوصية

إنّ المتأمل لنصوص الإتفاقية الأوروبية لمكافحة الجريمة المعلوماتية يجدها تخلو من تقسيم صريح لأنواع الأدلة المعلوماتية، و لكنها عدّدت مصادر هذا الدليل إنطلاقاً من درجة تعارضها مع الحق في الخصوصية و هي الأدلة المعلوماتية المستمدة من البيانات المتعلقة بالمرور (أولاً)، و الأدلة المعلوماتية المستمدة من بيانات المحتوى (ثانياً)، و الأدلة المعلوماتية المستمدة من بيانات المشتركين (ثالثاً)، و نطرح ذلك على التفصيل الآتي:

أولاً: الأدلة المعلوماتية المستمدة من البيانات المتعلقة بالمرور

وفقاً للمادة الأولى من الإتفاقية الأوروبية لمكافحة الجرائم المعلوماتية، يقصد بالبيانات المتعلقة بالمرور (**Données Relatives Au Trafic**) مجمل البيانات التي تتعامل مع الإتصال، و التي تمرّ من خلال نظام معلوماتي، أو يتمّ إعدادها بواسطة هذا الأخير و الذي يعدّ عنصراً في سلسلة الإتصال، بالإشارة إلى مصدر الإتصال، مكان الوصول، خط السير، السّاعة و التاريخ، الحجم، مدّة الإتصال، أو نوع الخدمة المؤدّاة⁽¹⁾.

و تشير المذكرة التفسيرية للإتفاقية الأوروبية لمكافحة الجرائم المعلوماتية إلى أنّ بيانات المرور المعرّفة في الفقرة الأولى من المادة الأولى من الإتفاقية تشكّل طائفة من البيانات المعلوماتية الخاضعة لنظام قانوني معيّن، و أنّ هذه البيانات ينتجها نظام معلوماتي في سلسلة من الاتصالات، من أجل توجيه الإتصال من منبعه أو أصله إلى مكان وصوله، و

(1) على خلاف الإتفاقية العربية لمكافحة جرائم تقنية المعلومات التي أغفلت إيراد تعريف لهذا النوع من الأدلة المعلوماتية، نجد أنّ بعض التشريعات العربية قد تناولتها بالتعريف مستلهمة إياه من الإتفاقية الأوروبية لمكافحة الجرائم المعلوماتية (صياغة و فحوى) كالتقنين المصري و اللبناني و هو موقف المشرّع الجزائري الذي تجسده المادة الأولى فقرة هـ من القانون 04-09، أين عرّف المشرّع المعطيات المتعلقة بحركة السير بأنها تشمل "أيّ معطيات متعلّقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءاً في حلقة إتصالات، توضّح مصدر الإتصال، و الوجهة المرسل إليها و الطّريق الذي يسلكه، و وقت و تاريخ و حجم و مدة الإتصال و نوع الخدمة".

على ذلك فهي من ملحقات الإتصال بحد ذاته⁽¹⁾. كما تبين المذكرة التوضيحية أهمية بيانات المرور في حالة وقوع جريمة بقولها أنه في حالة التنقيب بخصوص جريمة إرتكبت في نظام معلوماتي فإن بيانات المرور تكون ضرورية من أجل تحديد مصدر الاتصال، و ذلك نقطة بداية تسمح بتجميع أدلة أخرى أو جزء من دليل الجريمة، و هي تتصف بكونها سريعة الزوال و لذلك يكون من الضروري العمل على حفظها فوراً و بالتالي يكون من الضروري الكشف السريع عنها لمعرفة خط سير الإتصال و تجميع الأدلة قبل أن تمحى أو من أجل تحديد هوية المشتبه فيه⁽²⁾.

ثانياً: الأدلة المعلوماتية المستمدة من البيانات المتعلقة بالمحتوى

و إذ لم تعرّف الإتفاقية بيانات المحتوى (Données Relatives Au Contenu) إلا أنها تشير إلى محتوى الإتصال، أي مضمون الإتصال، أو الرسالة أو المعلومات التي ينقلها الإتصال باستثناء بيانات الحركة⁽³⁾، و قد إستدرك المشرع الأوروبي هذا القصور بموجب مقترح بخصوص توجيه صادر عن البرلمان الأوروبي و مجلس الإتحاد الأوروبي بشأن "أوامر إنتاج و حفظ الأدلة المعلوماتية في المسائل الجنائية" بمقتضى الفقرة العاشرة من المادة الثمانية منه، حيث نصّ بأن بيانات المحتوى تمثل "جميع البيانات المخزّنة في شكل رقمي مثل النصّ و الصوت و الفيديو و الصور و الصوت بخلاف بيانات المشترك، و بيانات الولوج أو البيانات المستمدة من المعاملات"⁽⁴⁾.

(1) و قد أشار التقرير التفسيري لإتفاقية بودابست في البند 30 منه إلى أنّ هذا التعريف قد وضع قائمة مستفيضة لفئات بيانات الحركة التي تخضع معالجتها لنظام خاص و لكن لن تكون جميع هذه الفئات متاحة دائماً من الناحية الفنية أو قد لا يتمكّن مقدّم الخدمة من إنتاجها أو لن تكون ضرورية لإجراء تحقيق و يشير مصطلح "المنشأ" إلى رقم الهاتف أو عنوان بروتوكول الأنترنت أو ما شابه ذلك من هوية هيئة الإتصالات التي يزودها مقدّم الخدمة بخدماته و يقصد بمصطلح "الوجهة" العنوان المماثل لهيئة الإتصالات التي تنقل إليها الإتصالات و تشير عبارة "نوع الخدمة المؤداة" إلى نوع الخدمة التي يتمّ إستخدامها داخل الشبكة مثل نقل الملقّات أو البريد الإلكتروني أو الرسائل الفورية.

(2) Conseil de l'Europe, Rapport explicatif de la Convention du Conseil de l'Europe sur la cybercriminalité . Adoptés par le Comité des Ministres du Conseil de l'Europe à l'occasion de sa 109e Session, le 8 novembre 2001, Clause n°29 .

(3) Rapport explicatif, op cit, Clause n° 209.

(4) Article 02 alinéa 10 de la Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en

في سياق مقارب عرّفها المشرّع البحريني بأنها "بيانات وسيلة تقنية المعلومات، خلافاً لبيانات خط السّير، يتم إرسالها كجزء من إتصال"⁽¹⁾، فهي تمثّل "أيّ بيانات سواء كانت في شكل رقمي أو بصري أو أيّ شكل آخر، بما في ذلك البيانات الوصفية، تنقل المضمون أو المعلومات أو المعنى أو الغرض من الاتصال، سواء كانت هاته البيانات في شكل فردي أو في شكل مجمّع، سواء في شكل معالج أو غير معالج. و تتضمنّ بيانات المحتوى أيّ بيانات تنقل مضمون الرّسالة أو فحوى الإتصال بالإضافة إلى البيانات التي تتمّ معالجتها أو تخزينها أو إرسالها بواسطة برامج الكمبيوتر"⁽²⁾، فهي ببساطة تشمل محتوى النّظام المعلوماتي مخزّناً أو منقولاً أيّما كان شكل ذلك المحتوى نصّاً مكتوباً أو صوتاً أو صورة أو صوتاً و صورة.

ثالثاً: الأدلة المعلوماتية المستمدة من البيانات المتعلقة بالمشاركين

ورد تعريف هذا النوع من الأدلة المعلوماتية **Données Relatives Aux Abonnés** ضمن المادة 18 فقرة 3 من الإتفاقية الأوروبية لمكافحة الجرائم المعلوماتية التي تنصّ على أنّه يقصد بالبيانات المتعلقة بالمشارك "كل معلومات تحتوي على شكل بيانات معلوماتية أو أيّ شكل آخر في حوزة مقدّم الخدمة و ترتبط بالمشاركين و خدماتهم غير بيانات المرور أو المحتوى و التي من خلالها يمكن تحديد: (أ) _ نوع خدمة الإتصال المستخدمة و الأوضاع الفنية المنصوص عليها بالنسبة لفترة الخدمة. (ب) _ الهوية، العنوان البريدي أو الجغرافي، و رقم هاتف المشارك، و رقم الولوج، و البيانات المتعلقة بدفع الفاتورة، و المبلغ المدفوع،

matière pénale stipule: «données relatives au contenu»: toutes les données stockées dans un format numérique tel que du texte, de la voix, des vidéos, des images et du son autres que les données relatives aux abonnés, les données relatives à l'accès ou les données relatives aux transactions.

(1) أنظر المادة الأولى من القانون البحريني رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات الصّادر بالجريدة الرّسمية رقم 3178 المؤرخة في 09 أكتوبر 2014، أمّا باقي التّشريعات العربية بما فيها التّشريع الجزائري فلم تنطرق إلى تعريف بيانات المحتوى.

(2) و قد ورد هذا التّعريف من قبل الإتحاد الدّولي للاتصالات ضمن مشروع تنسيق سياسات تكنولوجيا المعلومات و الاتصالات في منطقة البحر الكاريبي، الصفحة 16، البند السّابع، أنظر:

Union internationale des télécommunications, Preuve électronique, Modèles de lignes directrices politiques et de textes législatifs Harmonisation des politiques, législations et procédures réglementaires en matière de TIC dans les Caraïbes, p 16. Disponible à l'adresse: hipcar.gov.kn/sites/hipcar.gov.kn/files/HIPCAR_1-2

B_Model_Policy_Guidelines_and_Legislative_Texts_Electronic_Evidence.pdf,

Consulté le 08 décembre 2018.

و المتوفرة على أساس عقد أو إتفاق تقديم خدمة. (ج) - أية معلومات أخرى تتعلق بموقع تجهيزات الإتصال، المتوفرة على أساس عقد أو إتفاق تقديم الخدمة".

أوضحت المذكرة التفسيرية إلى أنه في إطار التّحقيق الجنائي فإنّ البيانات المتعلقة بالمشاركين تكون ضرورة في حالتين: أولاً، ثمة حاجة إلى المعلومات عن المشاركين لتحديد نوع الخدمات أو التدابير التقنية ذات الصلة التي إستخدمها أو إستخدمها المشترك، مثل نوع الخدمة الهاتفية المستخدمة كان يكون هاتف محمول مثلاً، و نوع الخدمات الأخرى المرتبطة و المستخدمة مثل إعادة توجيه المكالمات، و البريد الصوتي أو عنوان البريد الإلكتروني. ثانياً، عندما يكون العنوان التقني معروفاً، تكون هنالك حاجة إلى المعلومات عن المشترك من أجل المساعدة في تحديد هوية الشّخص المستهدف. و يمكن أن تكون معلومات أخرى عن المشترك، مثل ذلك المعلومات التجارية المتعلقة بسجلات الفواتير و دفع الإشتراك، يمكن أيضاً أن يتكون مفيدة في التّحقيقات الجنائية، خاصة عندما تتطوي الجريمة قيد التّحقيق على إحتيال أو جرائم إقتصادية أخرى⁽¹⁾.

و الذي يبدو من خلال الإتفاقية الأوروبية لمكافحة الجريمة المعلوماتية أنها لم تعتمد معياراً واضحاً بجلاء في تقسيمها لهذه الأدلة، بل ركزت على دور كلّ دليل من هذه الأدلة في الإثبات الجنائي، إلا أنّ المتأمل للمذكرة التفسيرية يجدها تشير بكل وضوح إلى مدى خطورة كلّ نوع من هذه الأنواع على الحرّيات الفردية أثناء إتخاذ إجراءات تجميعها، و لأن كانت جميع هذه البيانات تتطوي على المساس بمصالح خاصة، إلاّ أنّه بالنسبة لمعظم الدّول فإنّ بيانات المحتوى تعدّ أشدّ خطورة و مساساً بالحقوق في الخصوصية.

و من هذا المنظور يمكن فرض قيود على عملية جمع بيانات المحتوى أشدّ من تلك الخاصة ببيانات المرور، و للمساعدة على إدراك هذا الفارق فإنّ الإتفاقية تشير بشكل معياري في عناوين الماديتين 20، 21 إلى تجميع البيانات المتعلقة بالمرور تحت مسمّى التّجميع في الوقت الفعلي *Collecte en temps réel* و تجميع البيانات المتعلقة بالمحتوى تحت مسمّى الإعتراض في الوقت الفعلي *Interception en temps réel*⁽²⁾.

(1) Rapport explicatif de la Convention du Conseil de l'Europe sur la cybercriminalité, Clause n° 31, 142.

(2) Rapport explicatif, op cit, Clause n° 210.

و الرأى عندنا أنّ هذا التّقسيم لا يخلو من التّقد، فإن كان هذا التّقسيم يجد له ما يبرّره في إطار العلاقة الجدلية غير المستقرّة التي تربط بين مبدأ حرّية الإثبات و مبدأ شرعية الإثبات ، على اعتبار أنّ البيانات المتعلّقة بالمرور و بيانات المشتركين قد لا تستدعي قدرا من الحماية يعادل ما هو مقرّر من حماية لبيانات المحتوى، لأنّها لا تكشف سوى القليل من المعلومات الشّخصية للأفراد، فإنّ تطوّر التّقنية مع مرور الوقت و القدرة على ربط هذه البيانات و تحليلها يتجاوز المعيار الذي على أساسه بُني هذا التّمييز، إذ قد تكشف بيانات المرور عند جمعها أخصّ شؤون الحياة الخاصة للأفراد على نحو يتجاوز بكثير ما يكشفه محتوى الإرسال ذاته.

الفرع الثاني: تقسيمات الأدلة المعلوماتية على أساس قيمتها الإثباتية

هذا المعيار في تقسيم الأدلة المعلوماتية مرجعه الإجتهد الفقهي، الذي يرى أنّ الآثار المعلوماتية التي يحدثها مقترف الجريمة قد تتمّ بصورة لا إرادية أو بصورة إرادية و من هذا المنطلق تمّ تقسيم الأدلة المعلوماتية إلى نوعين أدلة أعدت خصيصا لتكون وسيلة إثبات (أولا) و الأخرى لم تعد لتكون وسيلة لإثبات (ثانيا).

أولا: أدلة معلوماتية أعدت لتكون وسيلة إثبات

و هذا النوع من الأدلة يمكن حصره فيما يأتي:

(أ) - البيانات و السّجلات التي يتمّ إنشاؤها من قبل جهاز الحاسوب بشكل تلقائي بحيث لا يكون لإرادة الإنسان و فعله أية مساهمة في إنشائها بطريقة مباشرة مثل ملفات الدّخول التي يتمّ فيها تسجيل جميع المتغيّرات التي تحدث في قاعدة البيانات و سجلات الهاتف و فواتير السّحب الآلي⁽¹⁾.

(ب) - البيانات التي يتمّ إدخالها بواسطة الإنسان بصورة مكتوبة و لم يتمّ حفظها داخل الجهاز الرّقمي⁽²⁾، و من أمثلتها رسائل البريد الإلكتروني و مواقع التّواصل الإجتماعي و غيرها.

(1) ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، المرجع السّابق، ص 2248

(2) خليفة محمد صالح جاد المولي، المرجع السّابق، ص 81.

(ج) - البيانات التي يتم حفظ جزء منها بالإدخال و يتم إنشاء الجزء الآخر منها بواسطة الجهاز الرقمي، و من أمثلتها العمليات التي تتم على برامج إكسل حيث يتم إدخال كافة البيانات و الأرقام المطلوبة داخل هذا البرنامج لكي يقوم بمعالجتها بأدواته لإجراء العمليات الحسابية.

ثانياً: أدلة معلوماتية لم تُعد لتكون وسيلة إثبات

و هذا النوع من الأدلة المعلوماتية ينشأ دون إرادة الشخص، أي أنها أثر يتركه الجاني دون أن يكون راغباً في وجوده، و يسمى هذا النوع من الأدلة بالبصمة الرقمية، و هي ما يمكن تسميته أيضاً بالآثار المعلوماتية الرقمية، و هي تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسله منه أو التي يستقبلها و كافة الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات العالمية.

الواقع أنّ هذا النوع من الأدلة لم يُعد أساساً للحفظ من قبل من صدر عنه، غير أنّ الوسائل الفنية الخاصة تمكّن من ضبط هذه الأدلة و لو بعد فترة زمنية من نشوئها، فالإتصالات التي تجرى عبر الأنترنت و المراسلات الصادرة عن الشخص أو التي يتلقاها، كلّها يمكن ضبطها بواسطة تقنية خاصة بذلك⁽¹⁾.

و المثال الشئع على هذا النوع من الأدلة ملفّات تعريف الإرتباط و البيانات الوصفية و عنوان بروتوكول الأنترنت IP address، و مثل هذا الأمر و إن كان لا يقود تحديداً إلى الشخص مرتكب الجريمة إستناداً الى الدليل المعلوماتي فقط إلاّ أنّه يمكن أن يساعد حتماً في التّوصل إليه عبر إقامة الدليل التقليدي فيما بعد، و يصلح كقرينة لاعتبار صاحب الجهاز مرتكب الجريمة إلى أن يثبت العكس⁽²⁾.

و هناك بعض الخصائص المميّزة لهذين النوعين من الأدلة المعلوماتية تشكّل حجر الزاوية في التفريق بينهما، فالنوع الأول من الأدلة و المولّدة بواسطة الحاسوب غير مُعدّة للطباعة و تتميز بطابعها غير المستقر بحيث تتطلّب هشاشة هذه الأدلة أدوات خاصة

(1) طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، مجلة الحقوق، جامعة التّهرين، العراق، المجلد 12، العدد 1، 2010، ص 46.

(2) محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، المرجع السابق، ص 398.

لفحصها بشكل سليم للوصول إلى معلومات دقيقة لأنها بيانات تفتقر للمشاركة البشرية. و لابد من إجراء التدقيق لضمان عدم تأثير العنصر البشري على البيانات أثناء عملية جمع الأدلة و فحصها⁽¹⁾.

و هي تتصف بالتعقيد الفني الكبير إذا يتعدّر على غير المتخصّص إدراك فحواها، و على نقيض هذا النوع من الأدلة، فالأدلة المعلوماتية التي يساهم الفرد في نشأتها قابلة للطباعة كالصور الرقمية و ملفات، Word، Excel، إلخ، بحيث يمكن طباعتها على أشكالها الموجودة بها على شاشة العرض، بالإضافة إلى ذلك فهي أقلّ تعقيدا و يمكن للقضاء و الهيئات التشريعية فهمها و التمييز بينها بدون مشقة⁽²⁾.

نحن نرى من جانبنا، أنّ محاولة تقسيم الأدلة المعلوماتية على أساس قيمتها في الإثبات الجنائي مجردة من أنّ قيمة عملية أو تطبيقية، ذلك أنّ ردّ الدليل المعلوماتي إلى تقسيم معيّن غير مفيد و لا يمكن إطلاقا أن يترتب على هذا التقسيم قوة اقناعية محدّدة سلفا، إذ أنّ كافة الأدلة المعلوماتية تتساوى في قيمتها و أهميتها ما دامت تخضع في نهاية الأمر إلى تقدير القاضي، و لعلّ ذلك مرجعه في الحقيقة إلى تميّز الإثبات الجنائي في جملته بخاصتي عدم الحصرية و الإقناعية و هما الخاصيتان اللتان تصبغان نظام حرّية الإثبات الجنائي⁽³⁾.

الفرع الثالث: تقسيمات الأدلة المعلوماتية على أساس المحتوى

هذا المعيار في تقسيم الأدلة المعلوماتية تمّ إعماله من قبل وزارة العدل الأمريكية في دليلها الصادر سنة 2002 ثمّ تبناه القضاء الأمريكي، و إستنادا إلى هذا المعيار تقسّم الأدلة المعلوماتية إلى ثلاث مجموعات و هي "الأدلة المعلوماتية المستمدة من سجلات الحاسوب المتوالدة" (أولا)، و "الأدلة المعلوماتية المستمدة من سجلات الحاسوب المخزّنة" (ثانيا)، والأدلة المستمدة من السجلات المتوالدة و المخزّنة بذات الوقت (ثالثا).

(¹) Khaled Ali Aljneibi, The Regulation of Electronic Evidence in the United Arab Emirates: Current Limitations and Proposals for Reform, philosophy doctoral thesis, Bangor University, Royaume-Uni, 2014, p 73.

(²) Khaled Ali Aljneibi, op cit, p 74.

(³) حول عدم جدوى تقسيم الأدلة الجنائية بشكل عامل يراجع: أحمد ضياء الدين محمد خليل، المرجع السابق، ص 377-379.

أولاً: الأدلة المعلوماتية المستمدة من سجلات الحاسوب المتوالدة

يطلق على هذا النوع من الأدلة بمخرجات حركة البرامج **The Output Of Computer Programs** و هي الأدلة التي يقوم بتكوينها الحاسوب **Computer Generated Evidence** و التي تتخذ الطبيعة الرياضية الجبرية (لغة الحاسوب)، ففي إطار مخرجات البرامج فإن الذي يسيطر عليها تحديدا ليس مستخدم الحاسوب أو مرتكب الجريمة بقدر ما يكون المسيطر هنا هو الحاسوب ذاته حين إستقباله للبرمجيات التي تعمل على تشغيله و تفاعله، و في هذا الصدد فإن كل ما تقوم به التقنية في إطار تكوين الدليل المعلوماتي أنها تجعل إمكانية قيامه ليست بالمستحيلة، و يبقى الأمر بعد ذلك متعلقاً بمدى إمكانية قبول الدليل في القانون أو أمام القضاء حسب الأحوال، فمثلا تعدّ من قبيل مخرجات حركة البرامج كمحتوى إلكتروني التعلّيمات التي تظهر أثناء فتح البريد الإلكتروني (تعليمات فتح صندوق البريد مثلا التي تأتي في صيغة مراسلة يقوم بإعدادها الخادم المخصّص للبريد الإلكتروني و ليس الفرد)⁽¹⁾.

ثانياً: الأدلة المعلوماتية المستمدة من سجلات الحاسوب المخزّنة

و يقصد بها التخزين الإلكتروني **Computer Stored-Records** و هو تعبير يحمل على مفهوم تدخّل الفرد في تكوين الملف الملفات التي يتمّ تخزينها بالضرورة في الحاسوب لكونه يشكّل بيئتها، ذلك أنّ تخزين البيانات في الحاسوب يأخذ أحد الشكلين إمّا بيانات يتمّ استخدامها و في هذه الحالة تظهر القوّة الإستردادية للبيانات في شكل معلومات محدّدة، و إمّا بيانات يتمّ تخزينها دون أن تستخدم و في هذه الحالة لا تكون بصدد مساحة مادية في القرص الصلب و إنّما فقط مجموعة من الأرقام، و المعيار المميّز لهذه الأدلة عن مخرجات حركة البرامج هو التّدخل الإنساني في تكوينها بشكل مباشر إذ يجب أن تتضمّن حضوراً للإنسان كما لو كان هناك أقوالاً ضمن ملف محتوى البريد الإلكتروني الذي يكتبه الفرد بقصد الإرسال. فالفرق بين سجلات الحاسوب المتوالدة و سجلات الحاسوب المخزّنة يتوقّف على ما إذا كانت الآلة أو الفرد هو الذي أنشأ محتويات السجلات (مصدر السجلات)⁽²⁾.

(1) عمر محمد بن يونس، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي المرشد الفديريالي الأمريكي لتفتيش و ضبط الحواسيب توصّلاً إلى الدليل الإلكتروني في التّحقيقات الجنائية، المرجع السابق، ص ص 421-422.

(2) المرجع نفسه، ص 420.

ثالثاً: الأدلة المعلوماتية المستمدة من سجلات الحاسوب المتوالدة و المخزنة

إنّ التّقسيم الثنائي السالف الذكر ليس مطلقاً، و إنّما مقيد بعدم وجود تزواج بين منطق عمل مخرجات حركة البرامج و بين التخزين الرقمي، فإذا حدث و وجد هذا التزواج فإنّ الأمر لا يعدو سوى مزجا ظاهريا من حيث تكوين الدليل المعلوماتي، فمثلا من يعطي أمرا للبريد الإلكتروني باستمرار بث رسالة معينة تتضمن تشهيرا بواقعة ما تتطوي على مساس باعتبار أحد الأفراد، فإنّه في هذه الحالة نكون بصدد بث تخزين قائم مسبقا بطريق نظام مخرجات حركة البرامج إلاّ أنّه يجب ألاّ ننسى أنّ مضمون الرسالة قد كتبها الفرد، و هذا النوع الثالث من سجلات الحاسوب تعدّ سجلات حاسوب متوالدة و أيضا تعدّ سجلات حاسوب مخزّنة، فهي تجمع بين التّدخل الإنساني و معالجة الحاسوب⁽¹⁾.

و بطبيعة الحال فإنّ هذا التّقسيم بات عتيقا و تجاوزته التّقنية بشكل كبير جدا، فهناك أنواع كثيرة من البيانات كالتطبيقات المعلوماتية و بروتوكولات الإتصالات التي تعتبر من أهمّ البيانات التي لا يمكن الإستغناء عنها في أيّ تحقيق جنائي يستهدف التّوصل إلى استرداد دليل معلوماتي و لا يستغرقها هذا التّقسيم، و ليست هناك أيّ فائدة ترجى من هذا التّقسيم من حيث القيمة الإثباتية، زيادة على أنّه تجاهل معيارا مهم تقوم عليه نظرية الإثبات الجنائي و هو مبدأ الشّرعية ممثلا في مدى تعارض الأدلة مع الحرّيات الفردية، و إن كنا نؤيّد المعيار الذي اعتمده الإتفاقية الأوروبية في تقسيم الأدلة المعلوماتية من حيث المبدأ إلاّ أنّنا لا نؤيّد في التّقسيم لأنّه أصلا معارض للمعيار الذي تبنته⁽²⁾.

(1) أميرة محمود بدوي الفقي، الإثبات الجنائي للجرائم المرتكبة عبر الأنترنت، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، مصر، 2014، ص 157.

(2) انسيقا وراء كلّ هذه الإعتبارات فإنّنا نرى أنّ أيّ تقسيم للأدلة المعلوماتية يجب أن يكون من الشّمول ما يستغرق كافة أنواع البيانات أيّا كان المصدر المنشئ لها (النظام المعلوماتي أو التّدخل البشري)، و أيّا كان نوعها (بيانات المرور أو بيانات المحتوى أو بيانات المشترك) و أيّا كان وضعها (مخزّنة أو متنقّلة) و أيّا كان شكلها (نصا أو صورة أو رمزا أو رقما.. إلخ)، و أن يتخذ من مبدأ الشّرعية أساسا يبنى عليه التّقسيم أي بحسب درجة مساس الدليل بالحرّية الشخصية و التي على ضوئها تقنّ ضمانات التّوصل إليه تشددا أو تساهلا و يحدّد الموقف بين هذا و ذاك الفلسفة السائدة بشأن مدى التّوازن بين الفعالية البحثية من ناحية و احترام الحقوق و الحرّيات من ناحية أخرى، أمّا مسألة القيمة التّبوتية فمرجعها إلى القاضي بقدر إحداث درجة اليقين لديه، و تلك هي الغاية الأسمى التي يجب أن يُبنى عليها التّقسيم.

و لعلّ مثار الصّعوبة في رصد معيار ثابت لتقسيم الأدلّة المعلوماتية يكمن في عدم إستقرار التّقنية على أنواع معيّنة من البيانات، و في هذا ما يجعل مناطق الخلاف قائمة بين هذا الدليل و بين الدليل في صورته التّقليدية، تلك الحقيقة التي تدفعنا إلى التساؤل حول موقع هذا الدليل من بين الأدلّة المعروفة في فكر الإثبات التّقليدي؟

المطلب الثاني: تصنيف الأدلّة المعلوماتية المستمدّ من التّفتيش

إنّ اختلاف الأدلّة من حيث نوعها أدى لدفع كثير من الفقهاء لوضع تصنيفات متدرّجة، و لقد تتعدّدت هذه الدّرجات بحسب المعيار المعتمد في التّصنيف⁽¹⁾، و ما يهمنا في هذا الصّد هو تحديد تصنيف الدليل من حيث علاقته بالواقعة المراد إثباتها (فرع أول)، و من حيث مصدره (فرع ثاني).

الفرع الأول: تصنيف الدليل المعلوماتي من حيث علاقته بالواقعة الإجرامية

يقسّم الفقه الأدلّة الجنائية من حيث علاقتها بالواقعة الإجرامية المراد إثباتها إلى أدلّة مباشرة و أدلّة غير مباشرة، و تعدّ الأدلّة مباشرة إذا ما انصبّت مباشرة على الواقعة محل الإثبات، فهي توصل الحقيقة التي تدلّ عليها إلى القاضي متى تأكّد من مشروعيتها و صدقها دون حاجة إلى فاصل ذهني في التأمّل و الإستنتاج⁽²⁾، و مثال ذلك المعاينة و التّفتيش.

(1) هناك تقسيمات عديدة قال بها الفقه يتخذ كلّ منها معياراً معيّناً كأساس للتّقسيم الذي يراه، فالبعض يجعل من مصدر الدليل أساساً للتّقسيم، و بناء عليه فهناك الأدلّة المادية و الأدلّة القولية و أخيراً الأدلّة الفتيّة، كما يتخذ آخرون من علاقة الدليل بالواقعة المراد إثباتها معياراً لتقسيم الأدلّة و من ثمّ تقسّم الأدلّة أدلّة مباشرة و أدلّة غير مباشرة و يقسّمها فريق ثالث بالنظر إلى وظيفة الدليل أو الغاية التي يرمي إليها و على هذا الأساس تستم الأدلّة إلى أدلّة على الإتهام و أخرى لاستبعاد المسؤولية الجنائية عن المتهّم أو تخفيفها، أي أدلّة الثبوت و أدلّة النفي، و هناك من الفقه من يقسّمها إلى أدلّة عامة و أدلّة خاصة على أساس التّمييز بين مضمون الدليل المتمثّل في الواقعة التي علم بها القاضي و بين وسيلة الإثبات التي أولت تلك الواقعة إلى علم القاضي كالمعاينة التي تنقل مضمون الدليل إلى علم القاضي مباشرة عن طريق إدراكه الشّخصي بينما شهادة الشّهود تنقل الواقعة إلى علمه عن طريق شخص ما. و عموماً فإنّ هذه التّقسيمات جميعاً مثار جدل كبير بين الفقهاء، و تلك مسألة تفيض عن حدود دراستنا، و لا يتسع المقام للإستفاضة في معالجتها. يراجع بخصوص تلك الإشكاليات: مفيدة سعد سويدان، نظرية الإقتناع الدّاتي للقاضي الجزائي دراسة مقارنة، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 1985، ص 121 و ما بعدها.

(2) أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، الطبعة الثامنة، دار النهضة العربية، مصر، 2012، ص 402.

و هذا بخلاف الأدلة غير المباشرة فهي لا تدلّ بذاتها على هذه الواقعة و إنّما تحتاج إلى عملية ذهنية يؤديها العقل بواسطة المنطق، و مثالها القرائن و الدلائل باعتبار أنّ الدليل هنا يستفاد من وجود واقعة أخرى ليست هي المراد إثباتها و إنّما تفيد في استخلاص نتيجة معينة تتعلق بالواقعة موضوع الإثبات، و قد اختلف الفقه بصدد تصنيفه للدليل المعلوماتي من حيث علاقته بالواقعة الإجرامية إلى إتجاهين:

الإتجاه الأول: الدليل المعلوماتي دليل غير مباشر

يميل غالبية الفقه المقارن إلى اعتبار الأدلة المعلوماتية أدلة غير مباشرة بطبيعتها بحيث تكون دائما في حاجة إلى أدلة أخرى تعضدها و تعزز موثوقيتها بحيث لا يمكن الإعتماد عليها بمعزل عن أدلة أخرى تدعمها⁽¹⁾، و يرى هذا الإتجاه الفقهي وجود تلازم وثيق بين علاقة الدليل بالواقعة الجرمية و بين موثوقية هذا الدليل، و يتجلى ذلك بشكل واضح في حالة الأدلة المعلوماتية المستمدة بشكل أساسي من رسائل البريد الإلكتروني أو الرسائل المحادثة الفورية، إذ لا يمكن الإعتماد عليها بسبب عدم كشفها عن الهوية الحقيقية للمرسل بالرغم من إمكانية تتبع مسار الرسالة و تحديد مكان الإرسال (الجهاز)⁽²⁾.

(1) Richard boddington, op cit , p 65.

(2) يتنازع إمكانية تحديد مسار الأنترنت من عدمه رأيان، فيذهب رأي إلى أنه لا يمكن تحديد مسار إرتكاب الجريمة، و تكمن وجهة هذا الرأي في أنّ الأنترنت مرنة الطبيعة بحيث أنه حتى و إن أمكن تحديد مسار الأنترنت فإنّ ما يتم الحصول عليه في هذا الإطار إنّما هو دليل رقمي يحتاج إلى تكملته بأدلة إثبات أخرى، فيما لو إقتصر الأمر على هذا الدليل فإنّ الأمر يظلّ في حومة الشك، ذلك أنّ ما يتمّ التوصل إليه في الحقيقة من خلال الدليل الرقمي إنّما هو عنوان رقمي فقط IP address و هو لا يكفي في نسبة العمل الإجرامي إلى مالك الحاسوب أو عنوان الإسم المذكور، إذ من الممكن ألا يكون هو مرتكب الجريمة حقا، كما لو كان حاسوبه مسروقا أو مؤجرا أو أن يكون عنوانه الرقمي مسروقا أو أن يكون أحد يستخدمه إحتيالا، و كذلك لن يكون له أيّ تأثير في الإدانة إذا تبين أنّ المتهم لا يعرف عن الأنترنت أو حتى الحاسوب أيّ شيء . فمثل هذه الأمور تجعل من الصعوبة بمكان إمكانية الإعتماد على مسار حركة الأنترنت للتوصل إلى المتهم ، و إنّما يحتاج الأمر هنا إلى دليل مادي و مثابرة من جهات التحقيق لكي يتوافر لها دليل مادي كاعتراف أو شهادة أو خبرة أو قرائن .. إلخ. بل إنه حتى في إطار الأدلة المادية ينبغي ألاّ تتجاوز إلى تقرير المستحيل و بما لا يتفق و طبيعة الأنترنت، و على محكمة الموضوع عدم الخروج على الطبيعة التي عليها تقنية الأنترنت و بما يتجاوزها فتقرّر أحكاما لا تتفق ما طبيعة الأشياء، بل يجب أن يكون القاضي مدركا لها و محيطا بطبيعتها و عالما بحركتها وإمكاناتها الهائلة. و يمكن التأكيد على أنه حتى في الحالات التي تمت فيها إدانة أشخاص أمام القضاء المقارن كان هناك دائما دليل مادي يتمّ الإستناد إليه إلى جوار الدليل الرقمي في هذا الشأن. في حين يذهب رأي آخر تزعمته محكمة باريس في حكم حديث لها إلى إمكانية تتبع مسار الأنترنت، و

إلا أنه نادراً ما يتم نسبة الجريمة إلى شخص معين على وجه الجزم و اليقين ما لم يكن هناك اعتراف صريح بذلك، فهناك دائماً احتمال بشأن المرسل الفعلي، إذ يمكن لأي شخص لديه كلمة المرور الصحيحة الوصول إلى حساب البريد الإلكتروني لشخص آخر و إرسال رسالة متظاهراً بكونه صاحب الحساب⁽¹⁾، ففي بعض الحالات قد يتشارك الأفراد ليس فقط في استخدام الحاسوب بل حتى في استخدام الكلمات السرية أو التشفير للولوج إلى الأنظمة المعلوماتية المشتركة⁽²⁾.

و هناك من الفقه من يعتبر الدليل المباشر في المثال السابق هو الجهاز المادي الذي تمّ من خلاله إرسال المحتوى المجرّم أو الحساب الإلكتروني الذي تمّ من خلاله الإرسال، بينما تعتبر نسبة الفعل إلى صاحب الحساب دليلاً غير مباشر يحتاج إلى إثبات إضافي، و الحقيقة أنّ هذا الرأى غير صحيح و ينطوي على فهم خاطئ لمدلول الدليل الجنائي المباشر و غير المباشر هذا من جهة⁽³⁾، و من جهة أخرى فليس معنى الدليل المباشر هو الدليل

بالتالي يمكن التوصل من خلال هذا التتبع إلى تحديد مسار العمل الإجرامي. و لقد قامت محكمة باريس الابتدائية بتبني هذا الرأى بناء على اعتماد تقرير خبرة في هذا الإطار. يراجع بهذا الخصوص: عمرو محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، المرجع السابق، ص 1003-1004.

(¹) Stephen Mason , Daniel Seng, op cit, p 219.

(²) Eoghan Casey, Susan W. Brenner, op cit, p 26.

(3) يتجه جانب من الفقه يقوده الفقيه رمسيس بهنام هذا التقسيم إلى إنتقاد هذا التصنيف القائم على تقسيم الدليل إلى مباشر و غير مباشر و يقرّر بأنّه لا وجه له إطلاقاً لأنّ الدليل على الجريمة و مقترفيها بينه و بين هذين صلة على الدوام مباشرة، و من ثمّ فإنّ الكلام على دليل إدانة غير مباشرة من شأنه أن يوجد لبساً و يؤدي إلى الخطأ في التقييم، فطالما أنّ الدليل هو أساس الحسم بوقوع الجريمة من المتهم أي أنّ له صلة، فالعلاقة إذن بينه و بين الجريمة و المجرم علاقة مباشرة فما يمكن أن تكون العلاقة بينه و بين الدليل علاقة غير مباشرة هو القاضي و ليس الجاني مرتكب الجريمة، ذلك أنّ القاضي تكون العلاقة بينه و بين وعاء الدليل الجنائي مباشرة في مجال الأدلة المادية إذ يعاينها بنفسه مستخدماً في ذلك محض ملكاته الذاتية و النفسية بينما تكون العلاقة بينه و بين وعاء الدليل غير مباشرة في مجال الأدلة النفسية إذ تتوسّط بين نفسية القاضي و بينها، نفسية الغير الذي تمثّل وعاء الدليل في ملكاته بما فيها من عيوب و وعي و إكراه و انصياع لمؤثرات مختلفة على هذا المعنى وحده و في العلاقة بين القاضي و الدليل يمكن الحديث على دليل مباشر و غير مباشر أمّا العلاقة بين الدليل و بين الجريمة و الجاني الذين ينصرف إليهما الدليل فإنّ هذه العلاقة لا يمكن إلاّ أن تكون على الدوام مباشرة . مشار إليه لدى: أحمد ضياء الدين محمد خليل، المرجع السابق، ص 376.

الكامل الذي يحقق اليقين القضائي و الدليل غير المباشر هو الدليل الناقص الذي يحتاج إلى دليل يكمله⁽¹⁾.

الإتجاه الثاني: الدليل المعلوماتي دليل مباشر و غير مباشر

يرى جانب آخر من الفقه أنّ الدليل المعلوماتي يمكن تصنيفه كدليل مباشر في أحوال معينة و دليل غير مباشر في أحوال أخرى، بحسب طبيعة الدليل المعلوماتي و الحقائق المراد إثباتها. على سبيل المثال، يكون الدليل المعلوماتي دليلا مباشرا حال وجوده في هيئة صورة رقمية تثبت حيازة محتوى مجرم، و هو "دليل غير مباشر" عندما يستخدم لإعادة بناء تسلسل الأحداث في مسرح الجريمة، مثل ملفات الإرتباط و تواريخ النفاذ إلى المواقع و غيرها⁽²⁾.

على أنّ هناك إتجاه آخر يعتمد في تصنيفه الأدلة المعلوماتية على نوع الجريمة المراد إثباتها فيكون دليلا مباشرا حين ينصبّ على واقعة تمثّل جريمة من الجرائم المستحدثة المرتكبة بواسطة النظم المعلوماتية أو عبر الأنترنت و يكون دليلا غير مباشر إذا ما تعلّق بواقعة تمثّل جريمة تقليدية⁽³⁾، إلا أنّنا نخالف هذا الرأي فتقسيم الدليل المعلوماتي إلى دليل مباشر و غير مباشر لا يتمّ على أساس طبيعة الواقعة الجرمية المراد إثباتها بل بمدى إتصاله بها.

في حين سلك إتجاه فقهي مسلكا مغايرا، فيرى أنّه لا يمكن رصد معيار عام بحسبه يصنّف الدليل المعلوماتي إلى دليل مباشر أو غير مباشر، بل بحسب الوقائع الجرمية و ظروفها، فعلى سبيل المثال يعدّ تسجيل الدخول إلى جهاز الحاسوب دليلا مباشرا على إستخدام حساب معين للنفاذ إلى نظام معلوماتي ما في وقت محدّد، و لكنه بذات الوقت دليل غير مباشر على أنّ صاحب الحساب هو الشخص الفعلي الذي قام باستعمال الحساب، فقد

(1) و في هذا الصدد تقتضي الإشارة إلى وجود توجه يعود للفقهاء بيكاريا و الذي قسّم الأدلة الجنائية إلى الأدلة التامة مثل الإعتراف و شهادة شاهدين و الأدلة الناقصة مثل شهادة شاهد واحد و اعتراف غير قضائي، و هذا ما كان له دور كبير في ظل نظام الإقتناع المقيد حيث كان يشترط توافر أدلة كاملة للحكم بعقوبة معينة، كما قد وضع البعض تفرقة بين الأدلة البسيطة و هي الكافية بمفردها للإقتناع القاضي و الأدلة المركّبة و هي التي تحتاج إلى أكثر من دليل لتكوين القاضي لقناعته. راجع بهذا الخصوص: مفيدة سعد سويدان المرجع السابق، ص 227.

(2) Shahzad Saleem, op cit , p 22.

(3) خالد حازم إبراهيم، المرجع السابق، ص 105.

يكون استخدامه تمّ من طرف غيره، بما يقيم الحاجة إلى أدلة أخرى لإثبات أنّ مالك الحساب هو من قام بتسجيل الدخول الفعلي إلى النظام، و قد يكون من الكافي إثبات أنه لا يمكن لغيره الوصول إلى جهاز الحاسوب لاشتراط رمز الدخول مثلا فيتخلف تصنيف الدليل⁽¹⁾.

و يتجه الرأى لدينا إلى أنّ الدليل المعلوماتي يمكن أن يكون بمثابة دليل مباشر عن طريق "إثبات حقيقة" فيكسب القاضي العلم مباشرة بالواقعة الواجب إثباتها و بذات الوقت يمكن أن يكون في أحوال أخرى دليلا غير مباشر يؤدي "إستنتاج حقيقة" معيّنة، و الأساس الذي يجب أن يُعتمد في هذا التّصنيف هو التّمييز بين طبيعة الأدلة المعلوماتية و فحواها، فالأدلة المعلوماتية المستمدة من بيانات المحتوى تشكّل دليلا جنائيا في غالب الأحيان يكون دليلا مباشرا يقدّم عناصر موضوعية تسقط تحت التّصور المباشر للقاضي و مثال ذلك في حالة ما إذا كان محتوى الإرسال المجرم تمّ عبر موقع معيّن من مواقع التّواصل الإجتماعي و كانت طبيعة الإرسال عبارة عن ملف مرئي و صوتي خاص بالمتهم يقوم من خلاله بتهديد الضّحية أو إبتدراها بألفاظ بذيئة فالدليل في هذه الحالة منصب مباشرة على الواقعة الجرمية.

في حين تعتبر بيانات المرور أدلة غير مباشرة و من طائفة تلك البيانات، البيانات الوصفية التي تعتبر المثال الأكثر شيوعا على الأدلة المعلوماتية غير مباشرة، فتحديد موقع المتهم في وقت معيّن يثبت وجوده بمسرح الجريمة، لا يعتبر دليلا منصبا على الواقعة الإجرامية بل دليل يفيد في استخلاص نتيجة معيّنة تتعلّق بالواقعة المراد إثباتها بما يتطلّب البحث عن سبب وجوده و علاقته بهذا المكان لحظة ارتكاب الجريمة و علاقته بالضّحية.

و نودّ أن نوضّح هنا أنّ الصّفة المباشرة أو غير المباشرة للدليل الجنائي بشكل عام سواء بالنسبة للأدلة النّقليدية أو الأدلة المعلوماتية ترتبط في حقيقتها بما يمكن للقاضي أن يستخلصه للإقتناع بثبوت الجريمة في حدّ ذاتها و أنّ المتهم هو المرتكب لها، أي وقوع الجريمة بشكل عام و نسبتها إلى المتهم بشكل خاص و ذلك بغض النّظر عن النّشاط الذي قام به القاضي في الوصول إلى القيمة الإثباتية للدليل المعلوماتي المستمد من التّفتيش⁽²⁾.

(1) Eoghan Casey, Susan W. Brenner, op cit, p 72.

(2) و قد أوضحت محكمة النقض المصرية ذلك بموجب قرارها الصّادر في الطّعن رقم 866 لسنة 10 جلسة 1940/04/22 قائلة "أنّ مدار الإثبات في المواد الجنائية ليس إلّا إطمئنان المحكمة إلى ثبوت أو نفي الوقائع المطروحة عليها. فمتى إستقرت عقيدتها على رأي فلا يهمّ أن يكون ما استندت إليه في ذلك دليلاً مباشراً مؤدياً بذاته

الفرع الثاني: تصنيف الدليل المعلوماتي من حيث مصدره

تتقسم الأدلة الجنائية من حيث مصدرها إلى ثلاثة أقسام: مادية و قولية و قانونية⁽¹⁾، و الأدلة المادية هي الأدلة التي تتبع منها عناصر مادية ناطقة بنفسها⁽²⁾، فقد يترك الجناة في مكان الحادث بعض الأدوات التي إستخدمت في ارتكاب الجريمة أو بصمات الأصابع أو الأقدام أو غير ذلك من المظاهر المادية التي تفيد القاضي في الإثبات، و يتم التوصل إلى الأدلة المادية عن طريق المعاينة أو الضبط أو التفتيش أو الخبرة⁽³⁾، فالدليل المادي هو الدليل الذي له بعد مادي يدلّ على وجوده الحسيّ فيستخلص من الأثر الذي يخلفه الفعل الجرمي و ينشئ رابطة بينه و بين مقترفه⁽⁴⁾.

أمّا الأدلة القولية فهي التي تنتج من أقوال صادرة عن الغير، يتشكّل منها إقتناع القاضي بحقيقة واقعة ما و يتوقف هذا الإقتناع على مدى صدق هذا الغير فيما ينقله إلى القاضي، و تنحصر هذه الأدلة في المجال الجنائي في الشهادة و الإقرار⁽⁵⁾.

إلى النتيجة التي إنتهت إليها، أو غير مباشر لا يوصل إلى هذه النتيجة إلا بعملية منطقية. و لذلك فإن محكمة الموضوع متى قالت بثبوت واقعة، و أوردت الأدلة التي إعتمدت عليها، و كانت هذه الأدلة من شأنها أن تؤدي عقلاً إلى ما قالت به فلا تصحّ مجادلتها في ذلك لدى محكمة النقض، إذ المجادلة في هذه الصورة لا يكون لها من معنى إلا إثارته البحث في عدم كفاية الأدلة بذاتها للثبوت، و هذا مما لا يجوز التّعيب على محكمة الموضوع فيه". مشار إليه لدى: إيهاب عبد المطلب، الإثبات في جرائم المخدرات، الطبعة الأولى، المركز القومي للإصدارات القانونية، مصر، 2015، ص 185.

(1) و هناك من يضيف نوعاً رابعاً إلى هذا التصنيف و هي الأدلة الفنية، و في رأينا فإنّ الخبرة ليست دليلاً بل أداة للتّقيب عن الدليل، يسترشد بها القاضي لإيضاح مسألة تعذر عليه فهمها، لذا فهي تستبعد من هذا التصنيف.

(2) أحمد فتحي سرور، المرجع السابق، ص 414.

(3) هلالى عبد الله أحمد، النظرية العامة للإثبات الجنائي دراسة مقارنة بين النظم الإجرائية اللاتينية و الإنجلوساكسونية و الشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1984، ص 385.

(4) محمد حسن شريف، النظرية العامة للإثبات الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 2002، ص 137.

(5) يسمّى الفقيه "بنتام" هذا النوع من الأدلة بأنّها الأدلة الحقيقية و هي تلك التي تستطيع إثبات مادية الفعل كبصمات الأصابع و بقع الدّم و الأدوات التي إستخدمها الجاني في ارتكاب جريمته و يقابل الأدلة المادية الأدلة الشخصية التي قسّمها إلى نوعين أولهما "أدلة شخصية غير مباشرة" و مثالها الإنفعالات التي تطرأ على الإنسان من جراء الخجل أو الإضطرابات التي تعتريه في حالة الخوف و الغضب و هذا النوع من الأدلة غير قاطع الدلالة أمّا

و تعرف الأدلة القانونية بأنها الأدلة التي حددها المشرع و عين قوة كل منها بحيث لا يمكن الإثبات بغيرها كما لا يمكن للقاضي أن يعطي أي دليل منها قوة أكثر مما أعطاه المشرع⁽¹⁾. فأين تقع الأدلة المعلوماتية من بين هذه الأنواع؟ واقع الأمر أنّ الجواب حول هذا التساؤل لم يكن محل إجماع بين الفقهاء و يمكن إجمال هذا الإختلاف في ثلاثة إتجاهات نذكرها تفصيلا فيما يلي:

الاتجاه الأول: الدليل المعلوماتي دليل مادي

يرى أنصار هذا الإتجاه أنّ الأدلة المعلوماتية ما هي إلا مرحلة متقدمة من الأدلة المادية التي يمكن إدراكها بالحواس الطبيعية للإنسان من خلال الإستعانة بجميع ما يبتكره العلم من أجهزة مخبرية و وسائل التقنية العالية و منها الحاسوب محور الأدلة المعلوماتية، فالأدلة الجنائية المعلوماتية في منظور أنصار هذا الإتجاه لا تختلف عن آثار الأسلحة و البصمات أو البصمة الوراثية ADN فهي إما أن تكون مخرجات ورقية يتم إنتاجها عن طريق الطابعات أو الرّاسم و إما أن تكون إلكترونية كالأشرطة و الأقراص الممغنطة و أسطوانات الفيديو و غيرها من الأشكال الإلكترونية غير التقليدية⁽²⁾. و إما أن تتمثل في عرض مخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به أو وحدة العرض المرئي⁽³⁾ و هذه الحالة التي تتواجد عليها الأدلة المعلوماتية يمكن تلمسها باعتبار أنّ لها مظهرا خارجيا سواء كانت عبارة عن أدلة ورقية أو إلكترونية في شكل دعامات بأنواعها المختلفة⁽⁴⁾.

النوع الثاني فهي "أدلة شخصية إختيارية"، و مثالها الإقرار الصادر عن إرادة أو الشهادة المقدمة عن رضا و هذا النوع من الأدلة قاطع الدلالة. مشار إليه لدى: أحمد أبو القاسم، الدليل المادي و دوره في الإثبات في الفقه الجنائي الإسلامي، دار النشر بالمركز العربي للأمنية و التدريب، الرياض، 1994، ص 158.

(1) هلاي عبد الله أحمد، النظرية العامة للإثبات الجنائي، بدون رقم الطبعة، دار النهضة العربية، مصر، 2011، ص 378.

(2) Eoghan Casey, op cit , p 5.

(3) هلاي عبد الله أحمد، حجية المخرجات الكمبيوترية في الإثبات الجنائي، الطبعة الأولى، دار النهضة العربية، مصر، 1998، ص 14

(4) سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب و حجيتها في الإثبات الجنائي، بدون رقم الطبعة، دار الكتب القانونية، مصر، 2011، ص ص 65-66.

و من هنا فإنَّ الطَّبيعة الَّتِي عليها الدَّلِيل المعلوماتي تجعل من البيئَة الَّتِي يحيا فيها أمرا لازما فبدون تلك البيئَة لا يُمكن التَّعويل عليه في الإثبات فلا يمكن الحكم إستنادا إلى تقرير يؤكِّد وجود قرص متحفَّظ عليه يحتوي على ملفات محل الجريمة فلا بد من فتح القرص أمام القضاء و الإطلاع عليه و من ثمَّ تقدير هذا الدَّلِيل و تحديد قيمته⁽¹⁾، فليس لازما لمس الدَّلِيل باليد لإضفاء الطَّابع المادي عليه بل يكفي إدراكه بالنَّظر أو السَّمع عن طريق شاشة الجهاز، كملفات الكتابة (Word) و المقاطع المرئية (Vedeo) لا اعتبار الدَّلِيل المعلوماتي من الأدلَّة المادية⁽²⁾.

و هناك من ينظر إلى مادية الدَّلِيل المعلوماتي من منظور علمي بحت، فالدَّلِيل المعلوماتي رغم كونه مجموعة من النَّبضات الكهربائِيَّة و المغناطيسية إلاَّ أنَّه له كيانا ماديا و يمكن تحريزه و حساب حجمه و مقدار المساحة الَّتِي يشغلها و ذلك بوحدَة البايٲ byte و كل ما في الأمر أنَّ الكيان المادي لهذا الدَّلِيل لا يمكن إدراكه بالعين المجردة و إنَّما يمكن إدراكه بالوسائل و الأساليب الإلِكترونية⁽³⁾، على أنَّ ذلك لا ينفي حقيقة التَّواجد المادي الفعلي للبيانات على وسائط التَّخزين المادية كحقيقة تكنولوجية و ليس تصوِّرا أو إفتراضا⁽⁴⁾.

(1) حازم محمد حنفي عثمان، المرجع السَّابق، ص 28.

(2) للإطلاع على الإشكاليات الهامة الَّتِي يثيرها المفهوم المادي للدَّلِيل المعلوماتي في إطار الشَّرعية الإِجرائية للتفتيش عنه و استرداده و مبلغ أثره على الحقوق الفردية في مقدَّمتها الحق في الخصوصية، أنظر المنظور الممزوج لمحل التفتيش المعلوماتي ص 158 و مابعدهما.

(3) محمود عبد الغني فريد جاد المولى، المرجع السَّابق، ص 21.

(4) و في سياق مقارب يرى بعض الفقه الأمريكي أنَّ الدَّلِيل المعلوماتي دليل مادي و أنَّ هذه الصِّفة مستمَّدة من وسائط التَّخزين المادية بحيث لا تعتبر الملفات بمثابة "أشياء" على الإطلاق فهي لا تعدو أن تكون مجرد مجموعات من البيانات، مرتبطة بشكل يجعلها لا تنفصل عن وسيلة التَّخزين، و هي بهذا المعنى ليست "مكانا" بل "شيئ". و من هذا المنطلق يرى أنَّ وسيط التَّخزين لا يمثَّل حاوية للدَّلِيل المعلوماتي بل هو شيء واحد (القطع الصَّلبة و البيانات) فالبيانات الموجودة على القرص الصَّلب غير موجودة في "العالم الإفتراضي" كما يُتصوَّر لدى البعض بل موجودة فعلا على وسيط التَّخزين بقدر وجود البيانات المطبوعة في "عالم الورق"، إذ لا تتمتع البيانات الحاسوبية بوجود مادي مستقل، بل هي عبارة عن تغيُّر فعلي يتمَّ إجراؤه على وسيط التَّخزين و هي حقيقة تكنولوجية و ليس تصوِّرا، فتخزين البيانات يتمَّ عن طريق التَّعامل مع الأشياء المادية المتمثَّلة في مناطق معيَّنة على القرص المغنط فكل ما يتمَّ حفظه على القرص هو بيانات و جميع البيانات مادية، و هكذا فإنَّ الملفات هي مجموعات من البيانات، يتمَّ تنظيمها بواسطة نظام محدَّد في نظام الملفات، و من هنا فإنَّ وجود البيانات على القرص الصَّلب يفيد أنَّ شخصا ما قام بتعديل وسيط التَّخزين فعليا لتخزين تلك البيانات، بحيث تمثَّل هذه المناطق المادية الَّتِي تعرَّضت للتَّعديل

و على هذا التوجه يردّ المعارضون، بأنّ هناك حالات من الأدلّة لا تعدّ دليلاً مادياً مثل الأدلّة المستمدّة من الوسائل التي تمس سلامة الجسم كجهاز كشف الكذب و التّويم المغناطيسي و التّحليل التّخديري و أمصال الحقيقة و جهاز رسم المخ الكهربائي و كذلك الوسائل السّمعية البصرية التي يترتّب على إستخدامها تعدّ على الحياة الخاصة للإنسان مثل كاميرات المراقبة و أجهزة التّصنّت، و إستبعاد هذه الأدلّة من دائرة الأدلّة المادية يقوم على أساس أنّها لا تعتبر أثراً مادياً ملموساً تصلح للمعالجة الفيزيائية لتحديد أبعادها و هو ما ينطبق تماماً على الدّليل المعلوماتي فهو عبارة عن نبضات غير ملموسة و لا تدرك بالحواس العادية بل يتطلّب ذلك الإستعانة ببرامج خاصة⁽¹⁾.

واقع الأمر أنّ ما يسوقه المؤيّدون لهذا الإتجاه يخالف أصلاً مدلول الدّليل المادي، فالصفة المادية التي تلحق هذا الدّليل توجب وجود الأثر الفيزيائي المحسوس الذي يشكّل عناصره و أبعاده، الأمر الذي يستبعد كل دليل يفنقر إلى هذه الصّفة من طائفة الأدلّة المادية، لذا نحن ننفي هذه الصّفة عن الدّليل المعلوماتي، بسبب طبيعة تكوينه بحدّ ذاتها و التي إنعكست عليه بحكم طبيعة البيئة التي يتواجد بها، إذ هي مجردّ تعداد غير محدود للرّقمين (0-1).

و هي بهذه الصّورة لا تفتقر فقط للبعد المادي المحسوس، بل قد تصل إلى درجة التّخيلية في شكلها و حجمها، أيّا كانت كمّية هذه التّثائية الرّقمية المحدّدة لحجم الملف داخل ذاكرة وسيط التّخزين، بحيث يمكن نقلها في أيّ مكان على كوكب الأرض أو يمكن تقسيمها على أماكن عديدة في مناطق مختلفة أو حتى بلدان مختلفة في زمن منته القصر، بل يمكن

بأياً byte ، و هذه البايات كتلة، و هذه الكتل عبارة عن ملف في نهاية المطاف، غير أنّ أجهزة الحاسوب تجنّب المستخدم كلّ هذه التّفاصيل أثناء التّعامل معها، مثال ذلك عندما يقوم المستخدم بإدخال بيانات في شكل صور و صوتيات فهو لا يطّلع حقّاً على الملفات أو يراها أو يسمعها، فعند فتح الملف الخاص بهذه البيانات يقوم برنامج خاص بترجمة الملف إلى صور يمكن التّعرف عليها بعد عرضها على الشّاشة، أو إلى أصوات عبر مكبر صوت. يراجع بهذا الخصوص:

Josh Goldfoot, The Physical Computer and the Fourth Amendment, Berkeley J. Crim. L. Vol 16, Issue 1, (2011), pp 113 et ss.

(1) عائشة بن قارة مصطفى، حجية الدّليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن، دار الجامعة الجديدة، 2010، ص 69.

أن يتواجد هذا الدليل بنسخ يعجز العقل البشري عن إحصائها بنفس الوقت و ضمن مختلف أصقاع الأرض، و بطبيعة الحال فإنّ الحيز الافتراضي Cyberspatial الذي تتواجد فيه تتعدّم فيه الحدود المادية فيستحيل تحديد موقع الدليل عن طريق رسم الإحداثيات المادية الخاصة به، فالقول بأنّ الآثار المعلوماتية معادلة للآثار المادية ضرب من ضروب الخيال.

الاتجاه الثاني: الدليل المعلوماتي دليل معنوي

يرى أنصار هذا الإتجاه أنّ الأدلة المعلوماتية هي أدلة معنوية غير ملموسة باعتبار أنّ الدليل المعلوماتي عبارة عن مجالات مغناطيسية أو كهربائية، الأمر الذي يترتب عليه أنّ إخراج الدليل المعلوماتي في شكل مادي ملموس لا يدل على أنّ المخرجات هي الدليل و إنّما هي عملية نقل تلك المجالات من طبيعتها التّقنية و الرّقمية إلى هيئة يمكن الإستدلال بها على معلومة معيّنة، ففهم و إدراك مضمون الدليل المعلوماتي يعتمد على إستخدام أجهزة تقنية خاصة لتحليل محتوى الدليل و أنّ ما لا يمكن تحليله و فهم محتواه لا يعتبر ضمن الأدلة المعلوماتية لعدم إمكانية الإستدلال به على معلومة معيّنة مما يلغي قيمته في إثبات الجريمة و معرفة مرتكبيها⁽¹⁾.

و في تقديرنا فإنّ الأدلة المعلوماتية في مجموعها مجرّدة لا تستمدّ من أمور حسيّة و إنّما يتوصّل إليها من أمور معنوية غير مادية و تحتاج إلى إيضاح و جلاء، و مع ذلك فإنّ مناطق الإختلاف قائمة بين هذا الدليل و بين الأدلة المعنوية في صورتها التقليديّة كالشهادة و الإقرار، فإذا تأملنا موضوع الدليل المعلوماتي فإنّه بدون شك لن يكون له تلك الطّبيعة التي عليها الأدلة المعنوية في العالم المادي و ضمّه إلى هذه الطّائفة من الأدلة أمر يجافي المنطق.

الاتجاه الثالث: الدليل المعلوماتي يقع خارج التّصنيف التقليدي

هذا الإتجاه و إن إتفق مناصروه على أنّ الدليل المعلوماتي بما عليه من كينونة يستحقّ تصنيفا خارج التّصنيف التقليدي، غير أنّهم إختلفوا حول الأساس المعتمد في ذلك، فجانبا و جيه من الفقه يميل إلى ترجيح تصنيف خاص للأدلة المعلوماتية إنطلاقا من طبيعة تكوينها

(1) مسعود بن حميد المعمرى، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة الحقوق، كلية الحقوق العالمية، قطر، ملحق خاص، العدد 3، الجزء الثاني، 2018، ص 197.

و خصائصها التي تميّزها عن غيرها من الأدلة الجنائية الأخرى، و بهذه الخاصية فهي تشكّل إضافة جديدة لأنواع الأدلة الجنائية⁽¹⁾.

و هناك رأي آخر يرى أنّ الدليل المعلوماتي هو "ملك الأدلة" و أنّ الأساس الذي يجب أن يعتمد في عملية التصنيف هو "القوة الثبوتية للدليل" ففي ظلّ إنعدام أمارات توحى بأنّ المشرّع ساير التطور الحاصل في بعض عناصر الأدلة التي ترقى إلى رتبة "الدليل الكامل" خاصة بالنظر إلى قوة إقناعها الكبيرة، و يجب إعادة النظر في التصنيف التقليدي لأنّه عند تمعّن الأحكام القانونية لا يضع المشرّع أيّ تصنيف قائم على أساس القوة الإثباتية للأدلة، ذلك أنّ التمييز بين القيم الداخلية و الخارجية لعنصر إثبات ما يستند أساسا إلى التصنيف الخماسي التقليدي للأدلة (الإعتراف، الشّهادة، الدليل الكتابي، القرينة و الخبرة)، غير أنّ التطورات التكنولوجية أظهرت عدم ملاءمة هذا التصنيف و لا يبدو من الوجيه أن نجتمع داخل نفس الفئة الأدلة الإلكترونية ضمن الخبرات و القرائن⁽²⁾.

(1) عائشة بن قارة مصطفى، المرجع السابق ص 69، أنظر ذلك محمد الأمين البشري، التحقيق في الجرائم المستحدثة، أكاديمية نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2004، ص 235، و أنظر كذلك أحمد بن عبد الله الرّشودي، جدية الوسائل الإلكترونية في الإثبات الجنائي، دراسة تأصيلية مقارنة، رسالة دكتوراه، كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2008، ص 254.

(2) و تدعيما لموقفه يرى هذا الجانب من الفقه "أنّ القيمة الثبوتية لطريقة الإثبات بأيّ دليل كان من شأنها أيضا أن تختلف تبعا للسياق الذي ستنشأ فيه أو الشّخص الذي ستصدر عنه، فمثلا فيما يخصّ الشّهادة تشكّل كلّ من صفة و سمعة أو سن الشّاهد عوامل يمكن أن تحدث تغييرا جذريا في القيمة الثبوتية لكلامه، فشهادة شخص مسبوق قضائيا و يحفل بماضي جنائي ثقيل ستنمّ الإعتداد بها بحذر أكثر مقارنة بشهادة شخص بدون سوابق قضائية و نحن ندرك على ضوء هذا المثال أنّ طريقة الإثبات نفسها الشّهادة تملك قوة إقناع مختلفة حسب الشّخص الذي سيكون مصدرا لها و في نفس الوقت يمكن إسقاطه على الإعترافات ذلك ما يسمح بتسليط الضّوء على الهوة الكبيرة بين الأدلة التقليدية و الأدلة الإلكترونية فإنّ الواقع العملي يبيّن بأنّ قوة إثبات الأدلة الإلكترونية لا تخضع لتغيرات متعلّقة بالعناصر التي سيتمّ إستغلالها علميا شريطة أن تحترم بدقّة بعض الكيفيات التّقنية للإستغلال و الحفظ و بناء عليه يمكن القول بأنّ الأدلة الإلكترونية لا "تكذب" و إذا كانت تتميّر بموضوعيتها و علميتها فإنّه علينا أن نضع في اعتبارنا أنّ تقديرها يبقى منوط ببشر تحكمه الدّاتية".

أنظر: يوسف مناصرة، الإثبات الإلكتروني في القانون الجنائي المقارن، رسالة دكتوراه، كلية الحقوق جامعة الجزائر 1 سعيد حمدين، 2017، ص 55 و ما بعدها.

و بالرغم من أن تصنيف الأدلة على أساس قوتها الثبوتية له ما يبزره على الأقل من الناحية النظرية في تقديرنا، إلا أن هناك قدرا من التحفظ نودّ إيضاحه، فالدعوة إلى دمج مفهوم قوة الإثبات كعنصر تقييمي في ترتيب و تدرج الأدلة بموجبه يعتبر الدليل المعلوماتي "سيد الأدلة" فيه الكثير من المبالغة⁽¹⁾، بل و ينطوي على تجاهل واضح للأخطار الجسيمة المتأصلة في فكرة تقنين التّحديد المسبق للقيمة الإثباتية للدلائل الجنائي، فمثل هذا القول في حقيقته يقود إلى "تقنين اليقين القضائي" و الذي يعتبر مسألة واقع لا يملكها المشرع بل ترجع إلى تقدير القاضي تبعا لظروف الواقعة و ملابساتها، و يجب أن تظلّ كذلك و على وجه التّحديد عندما يتعلّق الأمر بالأدلة المعلوماتية التي تمتاز بسرعة تغييرها و تعديلها و التّلاعب بها، ما يجعلها محلا لكثير من الشكّ في قيمتها الإقناعية.

ف "اليقين القانوني" و "اليقين القضائي" و "اليقين العلمي" قد يتطابق ما يتولّد عنها من حقائق و قد تختلف، فالمشرع بما يقننه من حكم عام لا يكون في وضع مباشر مع وقائع جزائية لا تتمتع بالثبات و الإستقرار، و الخبير بما يتوصّل إليه من نتائج فهو لا ينشد سوى ما تمليه عليه الحقيقة العلمية بشكل جامد بعيدا عن الإعتبارات المحيطة بالواقعة، أمّا القاضي فمسعاه الحقيقة الموضوعية المعبرة عن العدالة التي يختلف وضعها باختلاف الجريمة و ملابساتها.

و بدورنا نرى أنّ القول بالطبيعة الدّاتية الخاصة للدليل الجنائي المعلوماتي هو الأولى بالترجيح، فالدليل المعلوماتي دليل فني ذو طبيعة تقنية متميّزة، مضمونه نبضات و ذبذبات إلكترونية غير ملموسة لا تدركها الحواس الطبيعية للإنسان و لا يقوى على فهمها إلاّ الخبير الفني المتخصّص، فلا هي مادية تترك أثرا في الجسم (المادة)، و لا هي مكتوبة و لو كانت

(1) أكثر ما يعاب على هذا التّوجه أنه أغفل مسألة التّنوع الذي عليه الدليل المعلوماتي و ما يثيره من إشكاليات، و مثال ذلك الدليل المعلوماتي المستمدّ من محرّر إلكتروني يتضمّن إقرارا من المتهّم بإرتكابه للواقعة الجرمية، أو أنّ ذات الإقرار واردة ضمن ملف صوتي أو صوتي و مرئي معا، كيف يمكن إعتبره دليلا كاملا و هو دليل لا يزال مثقلا بكثير من أوزار الماضي فقد يأتي نتيجة إكراه مادي أو معنوي؟ و الأمر ذاته ينطبق على دليل معلوماتي ممثلا في ملف صوتي أو محرّر إلكتروني ينسب لشاهد معيّن؟ كيف يمكن تحديد موضعه من السلم الهرمي الخاص بالقوة الإقناعية للأدلة؟ ماذا عن الأدلة المعلوماتية غير المباشرة كالبيانات الوصفية التي لا تنصبّ مباشرة على الواقعة المراد إثباتها و تبقى في دائرة القرائن التي تستنتج منها حقائق أخرى مجهولة؟ ماذا عن باقي الأدلة العلمية التي لا تقلّ موثوقية من الناحية العلمية عن الدليل المعلوماتي؟ هي كلها أسئلة يرفض هذا الإقتراح الفقهي الإجابة عنها.

في هيئة محرّر إلكتروني، و لا هي معنوية و لو وردت ضمن ملف حاسوبي صوتي، بل تعداد رقمي يسبح في حيّز إفتراضي و زمان إفتراضي يخضع إسترجاعها و فهمها للتقنية على وجه التّحديد و هو ما يؤهلها بحق للإستقلال بذاتها لتشكّل إضافة جديدة إلى نظرية الإثبات الجنائي.

و إذا كان الأمر ما سلف، فما هي إذن الأحكام الإجرائيّة الخاصة التي تقيد عملية التفتيش عن هذا المكوّن الرقمي و استرداده، كدليل جنائي يلصح لبناء حكم الإدانة أو البراءة؟ هذا ما سنعالجه في الباب الأول من البحث.

الباب الأول

الأحكام الإجرائية للأدلة

المعلوماتية المستمدة من التفتيش

إذا كان فكر الإثبات التقليدي قد استقر على أن كل إطلاع على مستوع السرّ بحثاً عن الحقيقة يشكل تفتيشاً، أفلا يتحقق هذا الإجراء عند قيام سلطة التفتيش بضبط وسائط التخزين الرقمية و لو لم يتم استعراض محتواها، أليس في عملية الضبط تقييد لخصوصية الفرد على بياناته و لو لم تتضمن هذه الأجهزة مواد محرّجة أو غير قانونية؟ إنّ مثل هذا التساؤل في الحقيقة يضع المشكلة في إطار افتراض التفتيش المسبق عن وسائط التخزين الرقمية قبل تفتيشها؟ فما هو المعيار الفاصل بين "الضبط" و "التفتيش" في البيئة الرقمية طالما أنّ كلا الإجراءين ينطويان على مساس بالحرية الشخصية؟ ما هو أساس مشروعية الضبط الشامل الذي يطال كافة البيانات؟ هل محل التفتيش وفقاً لهذا المنظور هو النظام المعلوماتي ككل أم جزء منه فقط؟ كيف السبيل إلى قصر الاطلاع على مستهدف التفتيش دون تجاوز نطاق الإذن القضائي في ظل ظاهرة اختلاط البيانات و تشابكها؟ ما مصير الأدلة المعلوماتية المكتشفة بشكل عرضي؟

يبدو من الواضح أنّ التجاوب مع هذه الأسئلة يبرز أحكاماً إجرائية خاصة لتفتيش البيانات المخزّنة، و بما أنّ مشروعية الدليل الجنائي ليس سوى إنعكاس لمشروعية الإجراء الذي أستمّد منه، فإنّ ذلك يدفعنا إلى ضرورة التعرّض لفكرة التفتيش عن الأدلة المعلوماتية (فصل أول)، و رصد ضوابط هذا العمل الإجرائي (فصل ثاني).

الفصل الأول

فكرة التفتيش عن الأدلة المعلوماتية

تثير ذاتية الأدلة المعلوماتية كمكون رقمي ثنائي غير محسوس تساؤلا يتضمّن البحث عن تفسير لعبارة "التفتيش عن الدليل المعلوماتي"، و مثل هذا التساؤل ينطلق بالضرورة من الإقرار المسبق بكون وجود الدليل المعلوماتي مرهون بوجود حاوية له، ممثلة في أجهزة التخزين المادية التي تشكل وسية الربط بين البيئة المادية و البيئة الرقمية، فالتفتيش عنها من مستلزمات تفتيشها، و هذه الحقائق تقودنا إلى ضرورة تحديد مدلول التفتيش عن الأدلة المعلوماتية (مبحث أول)، و تحديد مقدمات هذا العمل الإجرائي (مبحث ثاني).

المبحث الأول

مدلول فكرة التفتيش عن الأدلة المعلوماتية

طالما أن المستهدف من البحث هو تحديد مدى مشروعية التفتيش عن الأدلة المعلوماتية، فإنّ إلزام القائمين على تحصيلها بالمشروعية الإجرائية حال قيامهم بتفتيش بيانات المتهم يبدأ عند الشروع في التفتيش، و لتحديد العمل الإجرائي الذي يعدّ منطلقاً للتفتيش المعلوماتي، فإنّه ينبغي أن نستهل هذا المبحث بمناقشة مفهوم هذا الإجراء (مطلب أول)، ثم نردفه بعد تناول مسألة التمييز بينه و بين الضبط في البيئة الرقمية (مطلب ثاني).

المطلب الأول: مفهوم التفتيش عن الأدلة المعلوماتية

الحكم على الشيء فرعٌ عن تصوّره، من هذا المنطلق فإنّ التوصل لتحديد مدى شرعية هذا الإجراء الجزائي الخطير يستوجب مسبقاً تعريفه (فرع أول)، و استجلاء خصائصه (فرع ثاني) و بيان طبيعته (فرع ثالث).

الفرع الأول: تعريف التفتيش عن الأدلة المعلوماتية

من البديهي أن يسبق إجراء التفتيش عن الأدلة المعلوماتية، تفتيش تقليدي بمفهوم مادي يستهدف البحث عن الحاوية المادية للدليل المعلوماتي، و من ثم فإنّه لا مناص من التّطرق إلى تعريف التفتيش المادي (أولاً)، ثم نستتبعه بتعريف تفتيش نظم المعلومات، اتساقاً مع خطوات تنفيذ التفتيش المعلوماتي في الواقع (ثانياً).

أولاً: تعريف التفتيش المادي

من المسلّم به في اطار الفقه التقليدي أنّ التفتيش مرتبط بموضوع مادي "مادية الجريمة"، و محل مادي "مكان التفتيش"، و ذلك بحثاً عن دليل "ذا بعد مادي" محسوس، لذا فضلنا إلحاق الطبيعة المادية على هذا الإجراء القانوني تمييزاً له عن التفتيش المعلوماتي الذي يفتقد لهذه الصّفة من حيث مستهدفه و محله بل و حتى أسلوب تنفيذه.

عموماً لم تتضمّن التشريعات تعريفاً للتفتيش المادي، و لكن الفقه أورد تعريفات متعدّدة له، و إن اختلفت صياغاتها فقد تطابقت مضامينها، فيعرّف جانب من الفقه التفتيش بأنّه "إجراءات من إجراءات التحقيق تقوم به سلطة حدّدها القانون، يستهدف البحث عن الأدلة

المادية لجناية أو جنحة تحقق وقوعها، في محل خاص يتمتع بالحرمة، بغض النظر عن إرادة صاحبه⁽¹⁾.

و هناك من يرى أنّ التنقيش هو إجراء تقوم به السلطة القضائية للإطلاع على محلّ يتمتع بحرمة خاصّة للبحث عن الأدلّة اللّازمة للتحقيق الجنائي⁽²⁾، فهو بحث عن الحقيقة في مستودع السرّ، إذ هو بهذا المعنى إجراء من إجراءات التحقيق الإبتدائي، فلا يكون إستدلالاً بحسب الأصل لما يتضمّنه من اعتداء على حرمة شخص المتهم أو حرمة مسكنه بحسب الأحوال⁽³⁾.

في حين تطرّق الفقه المقارن إلى تعريف هذا الإجراء بتعاريف لا تختلف كثيرا عمّا جاء به الفقه العربي، بسبب تأثر الفقهاء العرب بالفقه اللاتيني، و أيضا لكون التشريعات العربية مستوحاة من هذا النظام، فيعرّف الفقه الفرنسي التنقيش بأنّه " البحث في مكان مغلق عن أدلّة مفيدة في إظهار الحقيقة"⁽⁴⁾، و عرّفه البعض الآخر بشيء من التوسّع بكونه " بحث بوليسي أو قضائي عن عناصر الدليل عن جريمة ما، و يمكن وفقا لقواعد قانونية خاصة أن يُنفذ في المسكن الخاص بأيّ شخص أو في أيّ مكان آخر حيث يمكن أن توجد أشياء يكون إكتشافها مفيدا في إظهار الحقيقة"⁽⁵⁾.

(1) سامي حسني الحسيني، النظرية العامة للتنقيش في القانون المصري و المقارن، الطبعة الأولى، دار النهضة العربية، مصر، 1972، ص 37.

(2) توفيق محمد الشاوي، حرمة الحياة الخاصة و نظرية التنقيش، الطبعة الأولى، منشأة المعارف، مصر، 2006، ص 28.

(3) رؤوف عبيد، نوع بطلان التنقيش في القانون المصري، المجلة الجنائية القومية، العدد الأول مارس 1960، مصر، ص 24.

(4) Mathias Murbach-Vibert, Les pouvoirs d'investigation en droit français, Essai d'une théorie générale, thèse de doctorat, Faculté de droit, Université Jean Moulin - Lyon 3, 2010, p 345.

(5) la perquisition" est une recherche policière ou judiciaire des éléments de preuve d'une infraction. Strictement réglementée, elle peut être réalisé au domicile de toute personne ou en tout autre lieu où pourraient se trouver des objets, documents ou données informatiques, dont la découverte serait utile à la manifestation de la vérité"

Voir : Serge Guinchard, Thierry Debar, Lexique des termes juridiques 2017-2018 - 25e éd, Dalloz, France, 2018, terme « perquisition ».

و قد ساهم القضاء بدروه في تحديد مدلول التفتيش التقليدي، فعرفته محكمة النقض المصرية في أحد أحكامها بقولها "التفتيش كما هو معروف في القانون هو ذلك الإجراء الذي رخص الشارع فيه التعرض لحرمة الشخص بسبب جريمة وقعت أو ترجح وقوعها، و ذلك تغليبا للمصلحة العامة على مصالح الأفراد الخاصة، و احتمال الوصول إلى دليل مادي يكشف الحقيقة"⁽¹⁾.

و في سياق مقارب عرفت محكمة النقض الفرنسية التفتيش بأنه "إجراء يراد به البحث في مكان مغلق عن أدلة ارتكاب الجريمة و نسبتها إلى مرتكبها"⁽²⁾، أمّا المحكمة العليا الفيدرالية الأمريكية فقد تعرضت لمدلول هذا الإجراء في قضية *Smith v. Maryland* ، معتبرة إياه "إجراء ينتهك التوقع المعقول أو المشروع للحق في الخصوصية"⁽³⁾.

عموما يُعرّف التفتيش بأنه السعي للحصول على الأدلة لدى المتهم ذاته أو مسكنه أو حيثما تكون تحركاته، شريطة إتباع إجراءات شكلية يتطلبها القانون، و تكمن الفكرة الأساسية للتفتيش في إباحة انتهاك الحق في الخصوصية طالما أنّ هناك مبرر في القانون لهذا الانتهاك، و من ثم يعدّ التفتيش أحد مظاهر تقييد الحريات الإنسانية التي ساهمت التشريعات الكبرى الأساسية في دعم المحافظة عليها⁽⁴⁾.

بدورنا نرى أنّ التفتيش التقليدي إجراء من إجراءات التحقيق يستهدف البحث عن أدلة مادية لجريمة تحقق وقوعها و ذلك في محل يتمتع بالحرمة، فهو يمثل إطلاع استثنائي على محل له حرمة خاصة ابتغاء كشف حقيقة الواقعة الإجرامية.

(1) نقض 4 يونيو 1973 السنة 24 رقم 148، مشار إليه لدى: محمود محمد محمود جابر، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقّال، بدون رقم الطبعة، المكتب الجامعي الحديث، مصر، 2018، ص 163.

(2) Cass crim. 29 mars 1994, no 39-85.995, Bull. Crim. no 118, et cass crim. 26 fivr 2014, n o 13-87.065, Bull. crim. no 61 " Attendu que toute perquisition implique la recherche, à l'intérieur d'un lieu normalement clos, notamment au domicile d'un particulier, d'indices permettant d'établir l'existence d'une infraction ou d'en déterminer l'auteur "

(3) *Smith v. Maryland*, 442 U.S. 735, 739-40 (1979) " "search" is: government action that violates an individual's "reasonable" or "legitimate" expectation of privacy."

See Orin S. Kerr, *Searches and Seizures in a Digital World*, Harvard Law Review, Vol 119, Issue 2, (2005), p 546.

(4) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، المرجع السابق، ص 852.

ثانياً: تعريف التفتيش المعلوماتي

إنّ التطور المتسارع لتقنية المعلومات جعل المشرّع العربي و المقارن يتفادى الخوض في إيراد تعريف محدّد لهذا الإجراء المستحدث⁽¹⁾، خشية صيرورة التعريف الذي يصاغ قديماً لا يتواءم مع التطور التقني⁽²⁾، و يميل الفقه عموماً إلى اعتبار التفتيش المعلوماتي "ليس سوى تفتيش تقليدي ينصب على الأجهزة المعلوماتية"⁽³⁾، لذا يعرفه جانب من الفقه الغربي بكونه "إطلاع على البيانات المخزّنة في النظام المعلوماتي"⁽⁴⁾، فهو "إجراء ينصب على المعلومات و يسمح بجمع الأدلة المخزّنة أو المسجّلة في شكل إلكتروني"⁽⁵⁾، أي أنّ كل ولوج إلى نظام معلوماتي من قبل السّلطة هو بمثابة تفتيش معلوماتي باستثناء بعض الحالات المنصوص عليها قانوناً⁽⁶⁾.

و إن اختلفت التشريعات في المصطلح المستعمل، فإنّ كلمة "تفتيش" تترجم فكرة ممارسة الدّولة لسُلطة قسرية، و هي نظيرة لمصطلح التفتيش التقليدي الذي يعني البحث، القراءة، التّحصيل، و فحص البيانات المعلوماتية، و إن كان مصطلح "الولوج" أو "النفاذ" هو

(1) يطلق على هذا الإجراء لدى الفقه الأمريكي مطلق "التفتيش الرّقمي" "digital search" و تفتيش الحاسوب "computer search" و التفتيش الإلكتروني "Electronic search"، و سايره في ذلك الفقه الفرنسي الذي استقر على عبارات لها ذات المعنى «perquisition numérique»، «perquisition électronique»، و أضاف هذا الأخير مصطلح التفتيش المعلوماتي "perquisitions informatiques" و هي عبارات تقريبية فقط و ليس ثمة فارق بينها إذ هي لا تعبر سوى عن تفضيل شخصي لصياغة دون أخرى، غير أنّنا فضلنا مصطلح التفتيش المعلوماتي لذات الأسباب التي دفعتنا إلى ترجيح تسمية مستهدف هذا الإجراء بالدليل المعلوماتي.

(2) Lorena Bachmaier Winter, « Section III – Procédure pénale. Societé de l'information et droit pénal. Rapport Général », Revue internationale de droit pénal, vol 85, no1, 2014, p 20.

(3) Olivier Decima, les investigations numériques en procedure pénale francais: du piratage informatique aux requisitions et saisie numeriques ? Revue la faculté de droit, université de galatasaray, no1, 2017, p 3.

(4) Catherine Forget « La collecte de preuves informatiques en matière pénale », Pas de droit sans technologie, Larcier, Bruxelles, 2015, p 253.

(5) Conseil de l'Europe, la criminalité informatique, (Recommandation no R (89) 9 sur la criminalité en relation avec l ordinateur et rapport final du comité européen pour les problèmes criminels, Editions du Conseil de l'Europe, Strasbourg, 1990, p 128.

(6) Catherine Forget, op cit, p 253.

الأدق لأنه أكثر إرتباطاً بالمصطلحات المعلوماتية⁽¹⁾، لذا فإنّ غالبية الفقه العربي يرجّح إنطباق المفهوم التقليدي على هذا الإجراء الجنائي، فعرفه البعض بكونه "تفتيش في وعاء السرّ بقصد ضبط ما يفيد من الأسرار في كشف الحقيقة، فجوهر التفتيش هو كشف نقاب السرية عما تحويه نظم الحاسوب من خفايا و أسرار و نوايا إجرامية، و بالتالي إزاحة ستار الكتمان عنها في معرفة الحقيقة، و هذا المعنى لا يتقيّد بالمكان المادي لوعاء السرّ سواء كان مسكناً أو شخصاً أو جهاز حاسوب أو نظاماً أو برنامجاً، أو أية أجهزة ملحقة بالحاسوب"⁽²⁾.

و عرفه البعض الآخر بأنه "البحث عن أدلة الجريمة في أجهزة الحاسوب التي استخدمت في ارتكاب الجريمة أو من خلال شبكات الاتصال مثل شبكة الأنترنت، و يتمّ تنفيذ هذا التفتيش بقيام السلطات بالدخول إلى النظام الحاسوبي الذي ارتكبت فيه أو من خلاله الجريمة و ذلك لبحث و فحص البيانات الموجودة به"⁽³⁾.

و بهذا المعنى فنحن نرى أنّ التفتيش المعلوماتي هو إطلاع استثنائي لسلطة التحقيق على معلومات مخزّنة تتمتع بالحرمة بهدف ضبط أدلة الجريمة و كل ما يفيد في كشف الحقيقة، على أنّه ينبغي الإشارة إلى مسألة جوهرية، فالقول بأن لكلا الإجرائين - التفتيش التقليدي و التفتيش المعلوماتي - نفس المفهوم و الجوهر فإنّ ذلك لا يفيد اعتبارهما بمثابة

(1) عند محاولة مواءمة القوانين الإجرائية التقليدية مع البيئة التكنولوجية الجديدة، نشأت مسألة المصطلحات المناسبة و شملت الخيارات الإبقاء على اللغة التقليدية " التفتيش " و " الضبط " ، أو استخدام مصطلحات حاسوبية جديدة و أكثر توجهاً من الناحية التكنولوجية " النفاذ " و " النسخ "، بصيغتها المعتمدة في نصوص المنتديات الدولية الأخرى بشأن هذا الموضوع مثل الفريق الفرعي المعني بجرائم التكنولوجيا العالية التابع لمجموعة الثمانية، أو استعمال حل وسط يتمثل في لغة مختلطة التفتيش أو النفاذ بطريقة مماثلة، و " الضبط أو التأمين بطريقة مماثلة"، ولما كانت هناك حاجة إلى تجسيد تطور المفاهيم في البيئة الإجرائية، فضلاً عن تحديد جذورها التقليدية والحفاظ عليها، تم تبني مقارنة مرنة تتيح استخدام المفاهيم التقليدية " التفتيش و الضبط " أو المفاهيم الجديد " الولوج و النسخ" ضمن اتفاقية مجلس أوروبا حول الجرائم السيبرانية (اتفاقية بودابست). يراجع بهذا الخصوص :

Conseil de l'Europe , Rapport explicatif de la Convention du Conseil de l'Europe sur la cybercriminalité. adoptés par le Comité des Ministres du Conseil de l'Europe à l'occasion de sa 109e Session, le 8 novembre 2001, note 191.

(2) علي حسن محمد الطويلة، التفتيش الجنائي على نظم الحاسوب و الأنترنت دراسة مقارنة، الطبعة الأولى، عالم الكتاب الحديث أريد، الأردن، 2004 ، ص 28 .

(3) محمود عبد الغني فريد جاد المولى، المرجع السابق، ص 110.

نفس الإجراء، إذ يبقى التفتيش المعلوماتي إجراء مستقل بذاته عن باقي الإجراءات التقليدية بما يتميز به من خصائص، لا مناص من تفصيل البحث بشأنها.

الفرع الثاني: خصائص التفتيش المعلوماتي

يتميز التفتيش المعلوماتي بخصائص قد تتوفر في التفتيش المادي، إلا أنها تأخذ بعض سمات الذاتية حال ارتباطها بالتفتيش المعلوماتي وهي طابع الجبر والإكراه (أولاً)، و المساس بحرمة المعلومات (ثانياً).

أولاً: الجبر و الإكراه

يقتضي تفتيش المتهم الحد من حريته الشخصية بالقدر اللازم لتنفيذه و ذلك بحسب أن القهر لا غنى عنه لتنفيذ هذا الاجراء⁽¹⁾، و يشترك التفتيش المعلوماتي في ذلك مع كافة إجراءات التحقيق، فهو تعرض قانوني لحرية المتهم الشخصية بغير إرادته و رغما عنه، فالقانون يوازن بين حق المجتمع في العقاب دفاعاً عن مصالحه التي تنتهك بارتكاب الجرائم، و بين مدى تمتع الفرد بحريته أمام هذا الحق، فيبيح إجراء التفتيش جبراً على صاحب الشأن متى توافرت و وروعت ضمانات معينة، و لذلك فإن التفتيش بمعناه القانوني يُتخذ دون اعتداد بإذن عن من يقع عليه و دون أهمية لرضائه، كل ما هنالك أن صاحب الشأن مع عدم رضائه باتخاذ الإجراء ضده قد لا يقاومه و لا يبدي اعتراضاً إحتراماً منه لسلطان القانون و قد يرفض إجراء التفتيش، فيتخذ اعتراضه مظهراً إيجابياً، و عندئذ يُحوّل القانون للقائم بالتفتيش اتخاذ خطوات معينة تجعل معنى الجبر و الإكراه واقعا و ظاهراً بيقين⁽²⁾.

و صور مقاومة و رفض هذا الإجراء تتخذ مظهرين أحدهما تقليدي و الآخر حديث، فأما المظهر التقليدي فيتجسد في المقاومة الفعلية و الجسدية للقائم بالتفتيش و منعه من الوصول إلى الحاوية المادية للدليل المعلوماتي المستهدف بالتفتيش، و الممثلة في مختلف وسائط التخزين الرقمية على اختلاف أنواعها و أشكالها، و التي قد تتواجد بمسكن المتهم أو

(1) قرار محكمة النقض المصرية، الطعن رقم 757 لسنة 37 جلسة 19/06/1967 س 18 ع 2 ص 838 ق 168، مشار إليه لدى إيهاب عبد المطلب، تفتيش الأشخاص و الأماكن، الطبعة الأولى، المركز القومي للإصدارات القانونية، مصر، 2009، ص 14.

(2) سامي حسني الحسيني، المرجع السابق، ص ص 38-39

شخصه أو سيارته، كالإقدام على تحطيم الجهاز المادّي أو تعريضه للحريق و التّلف و غيرها من صور التّدمير و الإتلاف الذي يراد به محو المعلومات التي تتضمنها دعامة التّخزين الإلكترونيّة.

و هذه الحالة يجرى عليها ما جرى عليه الفكر القضائي التقليدي، و الذي استقر على أنّه للقائم بالتفتيش إتخاذ كافة الإجراءات الضّروية لتحقيق غايته، إذ أنّه متى كان التفتيش مأذون به قانوناً، فاتخاذ ما يلزم من طرق لإجرائه متروك لرأي القائم به، فله أن يدخل المنزل المراد تفتيشه من سطح منزل مجاور و لو كان باستطاعته دخوله من بابه متى قدر أنّ ذلك يمكنه من ضبط عناصر الدليل⁽¹⁾.

و إن كانت الحالة الأولى لا تثير أيّ إشكال يذكر و استقرت حدودها في العمل القضائي، فإنّ الوضع الحديث في استعمال الجبر لتنفيذ إجراء تفتيش أجهزة التّخزين الرّقمية يطرح تساؤلات عديدة، إذ قد ينصاع المتّهم فعلاً لسلطان القانون و لا يبدي أيّ رفض لفكرة تفتيش أنضمته المعلوماتية، فيمكن القائم بالتفتيش من جميع ما بحوزته من وسائط رّقمية طوعاً و اختياراً، إلّا أنّ القائم بالتفتيش قد يفاجئ باستحالة النّفاذ إلى النّظام المعلوماتي لوجود تشفير معقد يحول دون ذلك، و عادة ما يكون هذا الإنصاع للتفتيش له غايات أخرى، أهمها الرّج بالقائم بالتفتيش إلى محاولة استعمال أيّ مفتاح لأجل فك التّشفير، و أيّ خطأ- و هو واقع لا محالة- يفضي إلى الحذف الكلي للمعلومات بشكل تلقائي لوجود برامج خاصة بذلك، فتضيع فرصة إثبات الجريمة.

و بطبيعة الحال فإنّ التّعامل بالإكراه وفق المنطق التقليدي لا يتجاوز حدود الأعضاء المادية في الجسم، أما تجاوز هذا الحد من الإكراه ليصل مداه إلى الجوانب الروحية و النفسية للمتّهم، فإنّ ذلك يتعارض مع حق المتّهم في الصمت، و قد يؤدي التّعامل وفق هذا المنطق إلى البطلان و تجريد الإجراء من أيّ أثر قانوني له بإهدار الدليل المستمد منه⁽²⁾.

(1) حسن صادق المرصفاوي، المرصفاوي في أصول الإجراءات الجنائية: الدّعى الجنائية-الدّعى المدنية-التّحقيق الابتدائي-المحاكمة- طرق الطّعن في الأحكام، الطّبعة الأخيرة، منشأة المعارف، مصر، 1981، ص 305.

(2) انظر إشكالية الصراع بين حق المجتمع في الاثبات و حق المتّهم في الصمت و عدم جواز جبره على البوح بالأرقام الخاصة بنظامه المعلوماتي المستهدف بالتفتيش، الصفحة 298 و مابدها من هذه الأطروحة.

و إن كان الفقه التقليدي يرى أنّ الإكراه عنصراً أولياً في التفتيش، و أنّ الإجراء الذي لا تتوفر له تلك الخاصية لا يمكن اعتباره تفتيشاً⁽¹⁾، و لا تسري عليه أحكام التفتيش الإستثنائية⁽²⁾، فإنّ مثل هذا القول يقودنا إلى طرح تساؤل بخصوص مدى قيام عنصر الجبر في حالة "التفتيش عن بعد" للبيانات المخزّنة ضمن الحوسبة السحابية، طالما أنّ تنفيذ التفتيش يتمّ بدون علم صاحب النظام المعلوماتي أصلاً؟

الحقيقة أنّ إنعدام استعمال السلطة الجبرية المباشرة في التفتيش ليست وحدها مما يقيم عنصر الإكراه، بل في اعتقادنا إنّ أخطر صور الإكراه الذي يمكن أن تلجأ إليها سلطة التحقيق هو التفتيش المعلوماتي بدون علم المتهم و هو التفتيش عن بعد و في سرية تامة⁽³⁾.

إجمال ما تقدّم أنّ عنصر الإكراه هو نوع من الإفتئات على حق الشخص في صون سره و منع الغير من الإطلاع عليه، فالأصل أنّه لا يجوز أن يترتّب على حق الدولة في العقاب مساس بالحق في السرّ من أجل استرداد الدليل المعلوماتي، لما في ذلك من انتهاك لأقدس الحقوق الفردية، غير أنّ مقتضيات فعالية مكافحة الجريمة في ثوبها الرقمي توجب اللجوء إلى هذا الإجراء مع تقييده بمجموعة الضمانات تحول دون تجاوز الغاية منه إلتماً بالشرعية.

ثانياً: المساس بحق الخصوصية المعلوماتية

يقال في الفقه إنّ تفتيش الشخص يعدّ قيذاً على حصانته أو "حرمة الذاتية"، و تفتيش المسكن يعدّ قيذاً أو إستثناء يرد على "حرمة المسكن" أو "حرمة المراسلات"، بمعنى أنّ التفتيش هو مساس بقاعدة "الحرمة" l'inviolabilité للشخص ذاته أو مسكنه أو رسائله⁽⁴⁾.

فهل يتمتّع الفرد بهذا الامتياز على معلوماته؟ و إن كان الأمر كذلك فما المقصود بـ "حرمة المعلومات"؟ ما هو الحق الذي تقوم على حمايته؟

(1) سامي حسني الحسيني، المرجع السابق، ص 39.

(2) توفيق محمد الشاوي، المرجع السابق، ص 78 و ما بعدها.

(3) يطلق على هذا الإجراء في الفقه الفرنسي: perquisition en ligne أو perquisition à distance.

(4) سامي حسني الحسيني، المرجع السابق، ص 40-41.

جرى الفقه قديماً على الإكتفاء بالقول بأنّ التفتيش يقيد حرمة المسكن، و هو قول أجوف لا معنى له، فالحرمة في نظر القانون هي الحماية و الإحترام⁽¹⁾، و قد أضفى المشرع حمياته على هذا المحل باعتباره مكنونا لسر الفرد، و لذلك فإنّ المشرع لم يستهدف رعاية الشّخص كجسم معيّن و لا المسكن كبناء خاص، و إنما السرّ الذي يحمله فقط⁽²⁾، فإن كانت الحصانة المقررة قانوناً تتعلق بالحرية الفردية في عمومها، فلا مناص من القول إذن بأنّ حق السرّ لا يرتكز محله في المسكن أو الشّخص فحسب، بل هو يرتبط بالأصل الذي يبني عليه أيّ "الحرية الفردية بمعناها الواسع"⁽³⁾.

و هذا المبدأ هو الذي يحول دون إرساء قاعدة عامة تضبط التّوقع المعقول للخصوصية، و يجعل بذات الوقت توقعات الخصوصية بعيدة عن تحديد ثابت، بل تتغيّر التّوقعات مع تقدم التّكنولوجيا و الأعراف و الممارسات الاجتماعية السائدة أو التي تطرأ على الهيئة الاجتماعية، و من ثمّ فهي تشمل حرمة المعلومات لأنّها مستودع لسرّ الفرد في الوقت الزّاهن، و الذي بات يعرف بالحق في الخصوصية المعلوماتية⁽⁴⁾.

و في هذا الصّد ذكرت الدائرة الأمريكية الاستئنافية الثانية أنّ "التّقدم التّكنولوجي و اعتماد الأفراد على أجهزة الحواسيب في حياتهم، أمر جعل القرص الصّلب (الحاسوب) أقرب إلى مقر الإقامة من حيث نطاق و كمية المعلومات الخاصة التي قد تحتوي عليها مثل هذه

(1) توفيق محمد الشّاوي، المرجع السابق، ص 125.

(2) Languier (Jean), Languier (Anne-Marie), La protection des droits de l'homme dans le procès pénal dans le sens de la protection des droits des personnes suspectes ou poursuivies depuis l'enquête jusqu'à la fin du procès, Revue internationale de droit pénal, 1966, 37e année, p. 149

(3) سامي حسني الحسيني، المرجع السابق، ص 39.

(4) و هذا الحق أصبح يتمتع بالحماية الدستورية إذ تنص المادة 47 من الدّستور الجزائري :

"لا يجوز إنتهاك حرمة حياة المواطن الخاصة، و حرمة شرفه، و يحميها القانون.

سرية المراسلات و الإتصالات الخاصة بكل أشكالها مضمونة.

لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلّل من السّلطة القضائية، و يعاقب القانون على إنتهاك هذا الحكم.

حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشّخصي حق أساسي يضمنه القانون و يعاقب على إنتهاكه".

الأجهزة"⁽¹⁾، و قد لاحظ هذا القضاء أيضا (الدائرة الأمريكية السادسة) أنه "بالنسبة لغالبية الأشخاص ، فإنّ أجهزة الحاسوب الخاصة بهم هي أكثر الأماكن خصوصية في نظرهم، بل هي أكثر خصوصية من غرف نومهم"⁽²⁾.

و على العموم فإنّه "غالبًا ما يكون الحاسوب الشخصي مستودعا للمعلومات الخاصة التي لا يريد مالك الحاسوب مشاركتها مع الغير، ففي نظر أغلب الناس فإنّ أجهزة الحاسوب الشخصية هي المساحات الأكثر خصوصية"⁽³⁾.

لذا نحن لا نؤيّد توجه بعض الفقه الذي يطالب إطلاق لفظ "المنزل الرّقمي" **domicile numérique** على "النّظام المعلوماتي" بمنطق الدعوة إلى المساواة بينهما في الحماية الإجرائية⁽⁴⁾، لأنّ حرمة هذا الأخير تفوق بكثير حرمة المسكن التقليدي، ذلك أنّ ما يكشفه التفتيش التقليدي من أسرار يبقى منحصرا في إطار ضيق نسبي لا يخرج عن حدود الإطار المكاني و الزماني لتنفيذ التفتيش، أي ضمن نطاق محدّد كالمسكن أو الجسم، و ضمن المدّة المحددة لتنفيذ التفتيش فقط و الذي يتحدد في ضوئه نطاق التفتيش من حيث كم المعلومات.

(1) United States v. Galpin, 720 F.3d 436, 446 (2d Cir. 2013). [Available online]. Retrieved April 3, 2019, from : <https://casetext.com/case/united-states-v-galpin>. ("Advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain.")

(2) و قد ورد تسببها لحكم الدائرة الاستئنافية قولها " تكمن الأهمية هنا في أنّ معظم الناس يعتبرون أجهزة الحاسوب خاصتهم هي مساحة أسرارهم، يتعامل الناس عادة مع غرف النوم كمكان خاص جداً، ولكن عند أيّ حفلة، ستجد كل الضيوف - حتّى الغريب منهم - مدعوون إلى غرفتك حتى أنّهم يضعون معاطفهم على السرير، لكن ما إن يحاول أحد الضيوف استكشاف الحاسوب الخاص بالمضيف، فستكون هذه آخر دعوة يتلقاها".

United States v. Gourde, 440 F.3d 1065, 1077 (9th Cir 2006). [Available online]. Retrieved April 3, 2019, from: <https://casetext.com/case/us-v-gourde-3>. "The importance of this case is considerable because, for most people, their computers are their most private spaces. People commonly talk about the bedroom as a very private space, yet when they have parties, all the guests - including perfect strangers - are invited to toss their coats on the bed. But if one of those guests is caught exploring the host's computer, that will be his last invitation."

(3) United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007). [Available online]. Retrieved April 3, 2019, from: <https://casetext.com/case/us-v-andrus>. ("A personal computer is often a repository for private information the computer's owner does not intend to share with others. For most people, their computers are their most private spaces.")

(4) Olivier Decima ,op cit , p 8.

أما التفتيش المعلوماتي فهو لا يتقيد في ما يكشفه من أسرار بحدود الزمان و المكان لحظة تنفيذ هذا العمل الإجرائي، بل يزيح ستار الكتمان عن كافة أوجه الحياة الخاصة التي بات وعاؤها فعلا يشكّله النظام المعلوماتي الذي تحفظ فيه كل وقائع حياة الفرد اليومية بأدق تفاصيلها، و هذه الحتمية تكاد تكون مقتضى طبيعي للتحوّل نحو مجتمع معلوماتي⁽¹⁾، لذا من الصّعب إعطاء هذا الحق وصفا قانونيا محددًا في الوقت الحالي، لأنّ أوصافه تتعدّد بتعدّد الضمانات القانونية التي ينبغي أن تقرّر لهذا الحق بحسب ما تقضي إليه تكنولوجيا الإعلام و الإتصال من معلومات تدخل في دائرة هذا الحق.

و يترتب على كون التفتيش المعلوماتي يتضمّن مساسا بحق الخصوصية المعلوماتية، فإنّه يخرج عن نطاقه كلّ إجراء لا يمسّ بالخصوصية، فالأصل في القانون أنّ الإطلاع على المعلومات مباح متى لم يتعارض هذا الفعل مع حقّ صاحبه، و من البديهي أنّه ما يباح للأفراد الإطلاع عليه يباح للهيئات القضائية أيضا معاينته، لأنّ المعلومة المحوسبة و المكشوفة لا تتمتع بحرمة خاصّة فهي تفقد هذا الامتياز القانوني أيّا كانت درجة خصوصيتها و فقا للتصور المستقر في ضمير الجماعة، و مثال ذلك إطلاع سلطة التحقيق على أخصّ شؤون الحياة الخاصّة للأفراد و المتاحة للجميع عبر مواقع التّواصل الاجتماعي و إن كانت هذه المعلومات مذهلة للغاية من حيث درجة حرمتها كأصل عام، فإنّ ذلك لا يضيف عليها حماية إجرائية طالما تخلّى صاحب الشّأن عن هذه الحرمة و كشف عن خبيثته، باعتبار أنّ السّرية وجها لازما للخصوصية في أغلب الأحيان.

و إذا كان التفتيش المعلوماتي يمسّ بحق الخصوصية و هو حقّ فرديّ، في سبيل حماية الهيئة الاجتماعية و مكافحة الجريمة، فهو ليس حقا مطلقا لهذه الهيئة بل هو رخصة استثنائية تملّحها ضرورة فعّالية التحقيق، فإذا لم تتوفّر الضّرورة المبرّرة لانتهاك الحرّية الفردية،

(1) و في سياق مقارب يشير الفقه إلى أنّ الطّوفان التكنولوجي على اختلاف أنواعه جعل العالم أشبه «بالتّوب الشّفاف»، إذ كشف العموميات والخصوصيات، فكان محقّق الكاتب الأمريكي (آرثر ميللر)، حينما قال: «بأنّ الكمبيوتر، المتميّز بشراسته التي لا تشعب للمعلومات، وقدرته على عدم الخطأ أو إمكانية نسيان أي شيء، قد يصبح القلب النابض لنظام رقابة فعّال، يحوّل مجتمعا إلى عالم شفاف، ترقد فيه بيوتنا و معلوماتنا المالية و اجتماعاتنا، و حالتنا العقلية و النّفسية و الجسمانية كذلك، عارية تماما، مكشوفة أمام أيّ شاهد». مشار إليه لدى: أشرف عزمي صيام، الحق في الحياة الخاصة في القانون الأساسي الفلسطيني: المفهوم و التحديات، مجلة كلية القانونية الكويتية العالمية، الكويت، السّنة 3 العدد 9، ص 179.

فإنّ التفتيش المعلوماتي في هذه الحالة يكون مخالفاً للشريعة، بل يعتبر اعتداءً على الحريات الفردية لا يقرّه القانون بل يعاقب عليه، لذا فهو مقيد بالضرورة و في حدودها دون تزيّد و لا إساءة أو إفتئات، و هو بهذه الطبيعة الاستثنائية، هل يمكن أن يكون عملاً من أعمال الاستدلال بعيداً عن الإشراف القضائي؟

الفرع الثالث: الطبيعة القانونية للتفتيش المعلوماتي

إنّ تحديد الطبيعة القانونية للتفتيش المعلوماتي لا ينعقد من القواعد العامة التي عالجت طبيعة هذا الإجراء في صورته التقليدية بشكل عام، أيًا كان محلّه المسكن أو الشّخص ذاته أو المعلومات المحوسبة، و هذا الإجراء الجنائي كما سبق و أن أشرنا يعتبر إجراء من إجراءات التّحقيق، فطبيعته القضائية تستوجبها طبيعته الاستثنائية المبرّرة لانتهاك أسرار الأفراد و كشف عوراتهم.

لكن الأشكال المطروح متى يعتبر كذلك؟ هل وفقاً للغاية المتوخّاة منه أم بحسب صفة القائم بالإجراء؟ لقد اختلف الفقهاء في الإجابة عن هذا السّؤال على أربعة اتجاهات و هي النّحو التّالي:

الاتجاه الأول:

يأخذ أصحابه في تحديدهم للطبيعة القانونية للتفتيش بالهدف منه، و بحسب هذا الاتجاه فإنّ غاية هذا الإجراء هو الحصول على الأدلة الجرمية و ضبطها و كشف حقيقتها و إزالة الغموض الذي يحيط بها و ترجيح نسبتها إلى شخص معيّن مثل ضبط برامج غير مشروعة على النّظم المعلوماتية الخاص بالمتّهم و تقديمها كدليل اتّهام ضده أمام المحكمة المختصة، و إلى هذا الاتجاه يميل أغلب الفقه⁽¹⁾.

الاتجاه الثاني:

يحدّد أنصاره الطبيعة القانونية للتفتيش حسب المرحلة الإجرائية التي تكون فيها الدّعى العمومية، فذهب هذا الرّأي الفقهي - مع اعتناقه معيار الغاية من الإجراء - إلى إضافة معيار

(1) هلالى عبد الله أحمد، تفتيش نظم الحاسب الآلي و ضمانات المتّهم المعلوماتي، الطبعة الأولى، دار النّهضة العربية، القاهرة، 1999 ص 51، و علي حسن محمد الطّوّالبة، المرجع السّابق، ص 15.

آخر يتعلّق بالوقت الذي جرى فيه هذا الإجراء، و حسبما إذا كان قد جرى قبل فتح التّحقيق أو بعده، فإذا إتخذ الإجراء قبل فتح التّحقيق كان عملاً من أعمال الاستدلال، بينما يعدّ عمل تحقيق إذا جرى بعد فتح التّحقيق⁽¹⁾.

الاتجاه الثالث:

يعوّل القائلون بهذا الاتجاه على صفة القائم بالتفتيش، فيعتبر الإجراء من أعمال التّحقيق إذا ما قامت به سلطة التّحقيق المنوط بها القيام به دون غيرها، أمّا إذا قام به عضو من أعضاء الضّبطية القضائية غير مخوّل بإجرائه بموجب إذن بالتفتيش، فإنّ التفتيش يعدّ عملاً من أعمال الاستدلال كالتفتيش الوقائي الذي يقتصر هدفه على تجريد المقبوض عليه من شيء خطير يحمله⁽²⁾.

و لقد تعرّض هذا الإتجاه لعدّة مطاعن على أساس أنّ المشرّع الإجرائي لا يعتدّ بصفة القائم بالإجراء⁽³⁾، و يثور هذا النّقد بالذّات حال مباشرة الضّبطية القضائية للتفتيش في حالة التلبس و النّدب، الواقع أنّ عضو الضّبطية القضائية حين يمارس الإجراء في هاتين الحالتين فإنّ القانون يتيح له اتخاذ إجراءات تحقيق لا استدلال، و يخضعه لقواعد معيّنة لا يخضع لها أصلاً بوصفه من الضّبطية القضائية و من ثمّ فالقانون يسبغ على أعضاء الضّبط القضائي عندئذ صفة سلطة التّحقيق⁽⁴⁾.

في حين يرى جانب آخر من الفقه أنّ التفتيش إجراء من إجراءات التّحقيق الإبتدائي فلا يعتبر من جهة إجراء من إجراءات الاستدلال، كما أنّه من جهة أخرى من إجراءات التّحقيق الإبتدائي و ليس من إجراءات التّحقيق النّهائي التي يجوز للمحكمة اتخاذها و لأنّه إجراء من إجراءات التّحقيق فإنّ سلطة التّحقيق - النيابة العامة أو قاضي التّحقيق - هي التي تملكه بحسب الأصل صحيح أنّ القانون قد أجاز للضّبطية القضائية في حالات التلبس بالجريمة تفتيش شخص المتّهم بشروط خاصّة، و لكن هذا التفتيش ليس من إجراءات التّحقيق و إنّما

(1) سامي حسني الحسيني، المرجع السابق، ص 55.

(2) هلاي عبد الله أحمد، المرجع السابق، ص 51.

(3) علي حسن محمد الطّوالبة، المرجع السابق، ص 16.

(4) سامي حسني الحسيني، المرجع السابق، ص 56.

هو من إجراءات جمع الاستدلالات فرضته الضرورة لاعتبارات تتعلق بمهابة الدولة لجمع الأدلة في حالات التلبس بالجريمة على مجرى الظاهر من الأمور لكنه لا يستهدف "بحثاً عن دليل" أو "تنقيبا عن حقيقة" و هو ما تتميز به إجراءات التحقيق⁽¹⁾.

و الحقيقة أنّ هذا التكييف هو ذاته الذي أرساه المشرع الجزائري الذي اعتبر المهام الاستثنائية المخولة للضبطية القضائية في حالة التلبس بمثابة تحريات و قد جاء ذلك واضحا في نص المادة 42 من قانون الإجراءات الجزائية⁽²⁾.

الاتجاه الرابع

يسعى أصحاب هذا الرأي إلى التوفيق بين الاتجاهات السابقة و تحت صيغة معيار مختلط و بحسب أصحاب هذا الاتجاه يعدّ إجراء التفتيش من إجراءات التحقيق عندما تقوم به السلطة المختصة بالتحقيق الابتدائي و بعد تحريك الدعوى العمومية و مباشرتها، بقصد الكشف عن الحقيقة، بمعنى أنّ عمل التحقيق يتضمّن المعايير الثلاثة مجتمعة و هي "الغاية" و "الوقت" و "القائم بالإجراء"⁽³⁾.

و بناء على ما تقدم نرى أنّ الطبيعة القانونية للتفتيش المعلوماتي تحدّد في ضوء الاتجاه الذي يأخذ بالمعيار المختلط، و بناء عليه يعتبر التفتيش إجراءات من إجراءات التحقيق متى باشرته السلطة القضائية، بعد تحريك الدعوى العمومية، بقصد كشف الحقيقة. و يبدو أنّ هذه المعايير الثلاثة (الغاية و الوقت و القائم بالتفتيش) قد استجمعتها المادة 44 من قانون الإجراءات الجزائية كما يقطع بذلك صريح مدلولها، بحيث نصّت على أنّه "لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنّهم ساهموا في الجناية

(1) محمد زكي أبو عامر، الإجراءات الجنائية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2010، ص 362.

(2) تنص المادة 42 من قانون الإجراءات الجزائية الجزائري على أنّه "يجب على ضابط الشرطة القضائية الذي بُلغ بجناية في حالة التلبس أن يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية ويتخذ جميع التحريات اللازمة، و عليه أن يسهر على المحافظة على الآثار التي يخشى أن تختفي و أن يضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة و أن يعرض الأشياء المضبوطة على الأشخاص المشتبه في مساهمتهم في الجناية للتعرف عليها.

(3) سامي حسني الحسيني، المرجع السابق، ص 56.

أو أنهم يحوزون أوراقا أو أشياء متعلّقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدّخول إلى المنزل و الشّروع في التفتيش.

الحقيقة أنّ الطّبيعة القضائية للتفتيش ضمانه جوهرية لحرّيات الأفراد لأجل تحقيق التّوازن التّسبي بين الحق في الإثبات المعلوماتي كضرورة لحماية الهيئة الإجتماعية و بين الحق في الخصوصية المعلوماتية كحاجة تملّحها الفطرة الطّبيعية للفرد، و الذي يعبر عن مظهر خاص من مظاهر حرّيته و استقلاله تجاه الجماعة، فكلّ مساس بـ"الحق في السّر المعلوماتي" و جب اعتباره تفتيشا يخضع لقيود تحفظ هذا التوازن⁽¹⁾.

و إن كان لهذه التّيجة جانب كبير من الصّحة في إقامة معيار يرسم الحدود الفاصلة بين التفتيش المعلوماتي و غيره من الإجراءات، إلا أنّها تثير مسألة غاية في الأهمّية حيث يتحدّد بها الفهم المنشود لهذا المبدأ، و يتّضح من خلالها نطاق هذا الإجراء و مداه، و تتعلّق تلك المسألة بالتّحديد الدّقيق للحظة التي يقع فيها التفتيش المعلوماتي أو المساس بالخصوصية المعلوماتية؟ ألا يتعرض هذا الحق للتّهديد في مراحل سابقة عن التفتيش المعلوماتي؟ بمعنى هل يقع الانتهاك عند "الوصول إلى النّظام المعلوماتي" و ضبطه أم عند "النّفاذ إلى النّظام المعلوماتي" و استكشاف مضمّينه؟ ألا ينطوي استحواد سلطة التّحقيق على معلومات المتّهم إحساسا منه بانتهاك حرمتها حتّى و لو لم يتم استعراضها؟ أليس في ذلك تعرّض لحرّية المتّهم و تقييدا لها؟

يبدو من الواضح أنّ هناك رؤية جديدة لهذه الحقوق، بحيث لا تسعفنا الضوابط التّقليدية في وضع حدود واضحة تفصل بين التفتيش المعلوماتي و الضّبط الرقمي، و رصد هذا المعيار المفقود هو محور دراستنا في المطلب الثّاني.

(1) غير أنّ محكمة النقض الفرنسية كان لها موقفا مختلفا لقي نقدا فقهيّا لادّعا حين اعتبرت أنّ عملية الولوج الأنظمة المعلوماتية المخزّنة ضمن خادم انطلاقا من الأجهزة الإعلام اللّالي الخاصة بالضّبطية القضائية بعد الحصول على الأرقام السّرية أثر عملية تفتيش مادية لا تعتبر بمثابة تفتيش بل مجرد عمل تحقيق بسيط على نحو ما سنعالجه بالتفصيل لاحقا.

المطلب الثاني: التمييز بين التفتيش المعلوماتي و الضبط الرقمي

من الطبيعي أنّ بحث معيار التمييز بين التفتيش المعلوماتي و الضبط الرقمي يفرض علينا الإحاطة علما بمفهوم الضبط الرقمي (فرع أول)، حتى يتحدّد الأساس في التفريق بين الإجراءين (فرع ثاني)، و الذي يبرز بشكل أوضح عند بيان مراحل التفتيش المعلوماتي التي لها ذاتية خاصة أفضت إلى قيام مفاهيم جديدة لهذه الإجراءات عند ارتباطها بالبيئة الرقمية (فرع ثالث).

الفرع الأول: مدلول الضبط الرقمي

إن تحديد مدلول الضبط الرقمي (أولاً) لا يُستكمل إلا بتحديد الأساس القانوني الذي يبرر اعتبار نسخ المعلومات ضبطاً رغم بقاء الأجهزة المادية البيانات الأصلية بحوزة مالكها (ثانياً).

أولاً: تعريف الضبط الرقمي

يعرّف الضبط عموماً بأنه إجراء من إجراءات التحقيق يرمي إلى "وضع اليد على الشيء و استبقاؤه تحت تصرف المحقق لمصلحة التحقيق"، و مصلحة التحقيق التي تبرّر الضبط هي الإثبات و هو يستوي في ذلك مع غيره من إجراءات جمع الأدلة و منها التفتيش⁽¹⁾، فيتحصّل الضبط إذن في وضع اليد على ما يصلح "دليلاً" أو "قرينة" في الجريمة لتقديمه إلى القضاء، فالمقصود به التّحفظ على الأشياء "المادية" التي تشكّل الجريمة أو تكون قد نتجت عنها أو تكون قد وقعت عليها الجريمة و بعبارة أدق التّحفظ على كل ما يفيد في كشف الحقيقة⁽²⁾.

و هذا المفهوم التقليدي يمتدّ ليضمّ البيانات الإلكترونية و قاعدة البيانات بمشتملاتها من ملفات و سجلات و حقول، سواء اتخذت برامج نظم المعلومات أو برامج تطبيقات، عن طريق وضع اليد على وسيط التخزين الإلكتروني، لأنّ المعلومات لا توجد مستقلة عن وعائها المادي، إلاّ أنّه مع مرور الوقت تبين عدم مشروعيتها هذا الإجراء إلى حد كبير جداً، نتيجة ما قد ينجم عنه من أضرار عديدة للأفراد بحكم حاجاتهم إلى الأجهزة المادية طيلة فترة الضبط و

(1) توفيق محمد الشاوي، المرجع السابق، ص 41.

(2) سامي حسن الحسيني، المرجع السابق، ص 303.

خاصة المؤسسات الاقتصادية إذ قد ينجرّ عنه شلل نشاط هذه المؤسسات و يزداد الوضع تعقيدا فيما لو إنصبّ الضبط على الشبكة⁽¹⁾.

أمام هذه المعضلة تم تبني ممارسة حديثة تتجاوب مع واقع التخزين الرقمي تقوم على النسخ الرقمي للبيانات المستهدفة بالتفتيش، إذ أنّ معظم عمليات التفتيش أصبحت تتمّ من خلال نسخ المواد المخزّنة في نظم المعالجة الآلية للبيانات بقصد تفتيشها لاحقا، للتوصل إلى الدليل المعلوماتي، مع ترك الأجهزة المادية و النسخة الأصلية للبيانات بحوزة المتّهم و هو ما يعتبر عنصر من عناصر الموازنة بين حق المجتمع و حقوق الأفراد.

و إجمال ما تقدم أنّ قيام السلطة الإجرائية بالنسخ الرقمي لبيانات المتّهم يمثل ضبطا، بحكم أنّ هذا الإجراء يمكّنها من الحصول على نسخة من البيانات التي تحتفظ بها لاستعمالها في المستقبل كدليل جنائي، و من المؤكد أنّ عرض و استكشاف هذه البيانات المنسوخة يشكّل تفتيشا و لكن الحصول على النسخة نفسها يخدم الوظيفة التقليدية التي تنظّمها إجراءات الضبط، فبمقتضى هذا الإجراء يتمّ تجميد أي معلومات يتمّ نسخها تماما مثل التّحفظ على الممتلكات المادية للمتّهم، فتوليد نسخة إلكترونية للبيانات لا يختلف على إجراءات ضبط منزل بمنع أهله من دخوله و ضبط المتّهم بمنعه من مغادرة مركز معيّن، أي هو إجراء يضمن سيطرة سلطة التّحقيق على الشّخص أو مكان أو الشّيء الذي يرحج أن تكون له قيمة إثباتية⁽²⁾.

غير أنّ هناك فارق بين الضبط المادي و الضبط الرقمي، فالضبط المادي يؤدي إلى تدخل سلطة التّحقيق في سيطرة المتّهم على أملاكه، لكن الأمر على نقيض ذلك بالنسبة لضبط المعلومات، فقيام سلطة التّحقيق بإنشاء نسخة إلكترونية من بيانات المتّهم و لو تعدّدت

(1) يجب التّويه في هذا الصدد على المصطلحات القانونية المستعملة، و التي لم نجد لها استعمالا لدى الفقه عموما سواء العربي أو المقارن، و قد فضلنا اطلاق لفظ "الضبط الرقمي" على المرحلة التي تسبق التفتيش، لأنّ الحجز هنا عرضي يسبق الاطلاع على البيانات، باعتبار أنّ النسخ الكلي هو المقابل الحقيقي لفكرة البيانات، أمّا الضبط النهائي للدليل و الذي يأتي في مرحلة لاحقة عن التفتيش الإلكتروني هو "ضبط معلوماتي" لمجموعة من البيانات المحددة التي تشكل مستهدف هذا الإجراء، لذلك فإنّ المفارقة بين الإثنين تعدّ قائمة حقا إذا تأملنا دور كل منهما.

(2) Orin S. Kerr, Fourth Amendment Seizures of Computer Data, Yale Law Journal, Vol. 119, Issue 4, 2010, pp 711-712.

هذه النسخ لا يؤدي بالضرورة إلى إلغاء حيازة المتهم للنسخة الخاصة به، بل يبقى متمتعاً بكافة حقوقه على النسخة الأصلية.

و من هنا نتوصل إلى أنه يراد بالضبط الرقمي إستبقاء بيانات محوسبة قد تفيد في كشف الحقيقة تحت تصرف سلطة التحقيق ريثما يتم تقديمها للقضاء، و إن كانت هذه القاعدة هي قضائية المنشأ فقد تم تبنيها بالاتفاقيات و التشريعات عموماً⁽¹⁾.

و مثل هذا الأمر لاحظته المشرع الجزائري فنص في المادة 6 من القانون 04-09 "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و أنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحرار ووفقا للقواعد المقررة في قانون الإجراءات الجزائية".

و نحن بدورنا لا نماري في أن النسخ الرقمي إجراء من إجراءات جمع الأدلة، و أن التكييف القانوني السليم لهذا الإجراء هو الضبط، غير أن السؤال الذي يفرض نفسه هنا يتعلق بمضمونه بالاعتبارات الواقعية أو القانونية التي على أساسها يُكَيّف النسخ الرقمي على أنه بمثابة "ضبط"، طالما أن النسخة الأصلية للبيانات تبقى بحوزة المتهم بما فيها وسائط التخزين المادية؟

(1) تنص المادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على: (ضبط المعلومات المخزنة: تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط و تأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة (1) من المادة السادسة والعشرين من هذه الاتفاقية .

هذه الإجراءات تشمل صلاحيات :

أ- ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات.

ب- عمل نسخة معلومات تقنية المعلومات و الاحتفاظ بها.

ج- الحفاظ على سلامة معلومات تقنية المعلومات المخزنة.

د- إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها.

يلتزم كل طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين (1، 2) من المادة السادسة والعشرين من هذه الاتفاقية).

ثانياً: الأساس القانوني لاعتبار النسخ الرقمي بمثابة ضبط

إنّ الجواب على هذا التساؤل غاية في الأهمية، فهو يحدّد الإطار القانوني الذي تقوم عليه نظرية التفتيش الجنائي المعلوماتي، لأنّه لا يتمّ تفتيش نظم المعلومات بغير ضبط معلوماتي مسبق نهائياً، حتّى و لو افترضنا أنّ الضبط إنصب على الدّعمة المادية لأسباب تقنية كوجود تشفير حال دون الضبط الرقمي في موضع التفتيش المادي، فإنّ الغاية من الضبط المادي في هذه الفروض ذاتها و هي الكيانات المعنوية ممثلة في البيانات و ليست الكيانات المادية على الإطلاق، لذا فإنه من غير المنطقي التمييز بين "الضبط المادي للدّعمة الإلكترونية" التي تحتوي على البيانات و "الضبط الرقمي المباشر".

فالقضاء الأمريكي يعتبر عملية نسخ البيانات على أنّها عملية ضبط تخضع للقواعد الإجرائية الإتحادية المنصوص عليها بالمادّة 41 من قانون الإجراءات الجنائية الفيدرالي، على الرّغم من أنّ معظم الأحكام القضائية لا تقدم أيّ تفسير أو سبب حقيقي يبرّر هذا الوضع القانوني. فعلى سبيل المثال في قضية (*United States v Comprehensive Drug Testin*) أكّدت الدّائرة التاسعة على "إعادة" نسخ من المعلومات التي أجريت أثناء تنفيذ عملية التفتيش إلى أصحابها، و أشارت المحكمة إلى المعلومات على أنّها "بيانات مضبوطة" *data seized* و "المواد المضبوطة" *seized materials*⁽¹⁾، دون بيان اسباب ما انتهت إليه بهذا الخصوص.

و إذا كان القانون أيضاً في غيبة من التّعرض لهذه المسألة، فإنّ الفقه الأنجلوسكسوني قد ذهب مذاهب شتى في معالجة الأساس المعتمد في اعتبار النسخ الرقمي بمثابة ضبط و هناك ثلاثة مقاربات فقهية في هذا الموضوع:

الاتجاه الأول: الضبط الرقمي يتعارض مع الحق في الحذف

اقترح بعض الفقهاء أنّ النسخ الرقمي ينبغي اعتباره ضبطاً لأنّ إجراء ينطوي على تعارض مع حق الفرد في "حذف بياناته" *The right to delete*، فهذا الحق يخوّل للفرد سلطة

(1) *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010), [Available online]. Retrieved April 26, 2019, from : <https://casetext.com/case/us-v-comprehensive-drug-testing-inc>.

التحكم في ملكيته و متابعة ما قد يعتريها بما فيها النسخ، فالضبطية القضائية لا يكون بمقدورها تدمير البيانات أو حذفها ما لم تقم بضبطها مسبقاً⁽¹⁾.

و هذا التوجه الفقهي لا يخلو من النقد لأنّ الاعتماد على "الحق في الحذف" كأساس لهذه المقاربة يقيم ضرورة تحديد ما الذي يمكن أن يربّبه هذا الحق الجديد لصاحبه، على سبيل المثال إذا كان لدى الفرد بريد إلكتروني مخزّن على خادم و قرّر أن يقوم بحذفه، هل يوفّر له "الحق في الحذف" حق مطالبة مزوّد خدمة الأنترنت بحذف هذا البريد الإلكتروني، أم أنّ هذا الحق فقط قائم حال محاولة سلطة التحقيق عمل نسخة من الملفات؟⁽²⁾.

علاوة على ذلك فأيّ معنى يبقى لهذا الحق إذا كانت هذه البيانات مكشوفة للعامة حتّى و لو افترضنا أنّ قصد هذا الفقه يقتصر على البيانات المجرّمة فهذه الأخيرة أيضاً قد تتاح لغير صاحب الشأن بشكل أو بآخر، عندما يكشف هذا الأخير طوعاً عن معلوماته، فبمجرد الاطلاع يفقد هذا الحق معناه.

الاتجاه الثاني: الضبط الرقمي يتعارض مع الحق في الحياة الحصرية للمعلومات

أمّا المعيار الثاني الذي اعتمده جانب كبير من الفقه فيرجع إلى "الحق في الحياة الحصرية" من منطلق أنّ حصول السلطة القائمة بالتنقيش على نسخة من بيانات المتّهم يعارض الحق في الحياة المطلقة للفرد على معلوماته الشخصية "right to exclusive possession" أي بمعنى آخر استثنائه بهذه المعلومات على نحو يحقّق استبعاد الغير عنها، فعندما تقوم سلطة التحقيق بنسخ البيانات أو المعلومات التي هي في الأصل ليست في حيازتها و غير متاحة لها، فهي تنتزع بذلك حق استخدام البيانات بشكل حصري عن صاحبها و يصبح لها بذلك سلطة استغلال تلك البيانات، صحيح لا يزال لدى المالك نسخة من

(1) Paul Ohm, The Fourth Amendment Right to Delete, Harvard Journal of Law. Vol 119, (2005), pp 13-17.

(2) Orin S. Kerr, Fourth Amendment Seizures of Computer Data, op cit, p 719.

البيانات لكن حقه في استبعاد الغير عنها قد تم انتزاعه⁽¹⁾، و هذا التفسير اعتمده القضاء الأمريكي (الدائرة الاستئنافية الفيدرالية الثانية) و ذلك في قضية **States v. Ganius United**⁽²⁾.

و يضيف هذا الجانب من الفقه أنّ مفهوم الحيازة "المطلقة" و "الحصرية" التي تجعل النسخ ضبطا تقتصر على النسخ الدقيقة فحسب، لأنّ الحق في استبعاد الغير عن البيانات يجب أن يقتصر على النسخ الدقيقة و لا يمتد إلى الملخصات باعتبار أنّ درجة التعارض مع الحيازة الحصرية في هذه الفروض تكون بنسبة أقل⁽³⁾.

و في ذات السياق يرى بعض الفقهاء الذين يناصرون هذا النهج، أنّ إجراء نسخ المعلومات على الرغم من أنّه لا يؤثر على النسخة الأصلية من البيانات التي تبقى بحوزة

(1) Mark Taticchi, Note, Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures, George Washington Law Review ,Vol 78 , 2010, p 478.

(2) في سنة 2014 ، و في قضية **Ganius v. States United** اعتمدت الدائرة الاستئنافية الثالثة أساس "الحق في الحيازة الحصرية". و في تنفيذ إذن بالتفتيش المعلوماتي لجهاز كمبيوتر خاص بمحاسب للحصول على أدلة على احتيال العملاء المحتملين، قام المحققون بنسخ ثلاثة محركات أقراص صلبة، و التي تضمّت أيضا الملفات الرقمية الخاصة بالمحاسب و بعد مرور سنتين و نصف، حصل المحققون على إذن ثان تفتيشا عن تلك الملفات نفسها لدليل على تورط المحاسب ذاته في جريمة منفصلة تماما و قال المحاسب بصفته متهما، إنّ الاحتفاظ المطول لملفاته الرقمية التي لا تستجيب للإذن القضائي الأول يشكّل ضبطا غير معقول و وافقت الدائرة الثانية على أنّ مصلحة المتهم في الحيازة تشمل "السيطرة الحصرية على ملفاته" و أنّ الاحتفاظ الحكومي بالنسخة ينطوي على تدخل بصورة مجدية في تلك المصلحة، و من ثم فهذا التصرف يشكّل ضبطا و لأن الحكومة احتفظت بتلك البيانات لفترة طويلة دون مبرر كاف، فإنّ الضبط كان غير معقول، و لم تحدد المحكمة عند أي نقطة تجاوز الضبط نطاق "المعقولة" أو المشروعية، و لاحظت أنّ الحكومة قد تكون لها مصالح مشروعة في الاحتفاظ بالبيانات، مثل المصادقة على القرص الصلب (أصالة الدليل المعلوماتي) إلا أنّها أكدت على "الفترة الطويلة" التي احتفظت بها الحكومة بالبيانات جعلت الضبط غير معقول و استجابات لطلب الحذف المعجل.

لمزيد من التفصيل راجع تعليق الفقه على هذا الحكم (مقال بدون مؤلف):

Recent CaseFourth Amendment search and seizure and evidence retention Second Circuit Creates a Potential "Right to Deletion" of Imaged Hard Drives .United States v. Ganius, 755 F.3d 125 (2d Cir. 2014) Harvard Law Review: Volume 128, Number 2, 2014, p743-750.

(3)Mark Taticchi, Note, Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures, Geo Wash L Rev, Volume 78, (2010), p 479.

المالك، فإنّه يحرم هذا الأخير من شيء ذي قيمة و يتداخل مع الاستخدام الحصري لصاحب الشأن، تماماً كما هو الحال حين تعرض الفرد لسرقة بياناته⁽¹⁾.

الاتجاه الثالث: الضبط الرقمي تجميد للأدلة المعلوماتية

أما المقاربة الثالثة فهي تقوم على منطق بسيط لا يخرج عن حدود منطق الضبط التقليدي، فالنسخ الرقمي يعتبر بمثابة ضبط لأن الوسيلة الإجرائية المعروفة بالضبط في التعديل الدستوري الرابع أو القاعدة التقليدية بشكل عام، هي ذاتها الوسيلة الإجرائية الحديثة التي تعرف بـ "التجميد" *The reason is that the Fourth Amendment power to seize is the power to freeze*، فالهدف من الضبط هو السيطرة و التحكم في مسرح الجريمة و الأدلة التي قد تتواجد عليه و الأمر كذلك عند إنشاء نسخة إلكترونية من البيانات، فهو إجراء يعمل على تجميد البيانات لاستخدامها كدليل جنائي في المستقبل، تماماً كما يؤدي ضبط الممتلكات المادية إلى تجميدها، فهو يضيف إلى سيطرة سلطة التحقيق أدلة لم تكن تحت سيطرتها قبل النسخ، فإنشاء نسخة إلكترونية لا يختلف كثيراً عن ضبط المنزل أو الخنجر فجميع هذه الأنواع من المضبوطات في نهاية المطاف تضمن سيطرة القائم بالتحقيق على الشخص أو المكان أو الأشياء التي يرجح أنّها ذات قيمة إثباتية⁽²⁾.

نحن نرى أنّ النسخ المعلوماتي ضبطاً لأنه إجراء من إجراءات جمع الأدلة يرمي إلى المحافظة على مسرح الجريمة و تأميناً له و منع الغير من العبث به، لما قد يوجد عليه من آثار تشكل عنصراً للدليل المعلوماتي، قد يتعارض مع حق المتهم في حذف بياناته و قد يتعارض مع حقه في حيازته المطلقة و الحصرية عليها، لكن في جميع الأحوال يبقى تكيف هذا الإجراء مستمد من الغاية منه و هو التّحفظ على كل معلومات يعتقد أنّ تكون مفيدة في كشف الحقيقة، فإنّ كان الضبط المادي يقيد حقوق الأفراد المادية على الشيء الذي يقع عليه الضبط فإنّ الضبط الرقمي يقيد الحق في الحيازة المادية المطلقة للفرد على معلوماته و ينتزع منه حقه في استثناء الغير من وضع يده عليها أو على نسخة منها.

(1) Susan W. Brenner & Barbara A. Frederiksen, Computer Searches and Seizures: Some Unresolved Issues, Michigan Telecommunications and Technology Law Review, Vol. 8, Issue 39, p 109 : ("When copying files, officers physically remove files from the owner's possession. Therefore, it seems the act of copying should be a seizure. The officers are taking the owner's property the information contained in the files.")

(2) Orin S. Kerr, Fourth Amendment Seizures of Computer Data, op cit, p 709.

الفرع الثاني: معيار التمييز بين التفتيش المعلوماتي و الضبط الرقمي

قد يظهر للوهلة الأولى أنّ تبني المفاهيم التقليدية للتفتيش في البيئة الرقمية لا يطرح أيّ إشكالية، لكن الحقيقة خلاف ذلك إذ هي أكثر تعقيدا و مثارا للجدل، لأنّ تبسيط هذا المجال المعقّد من الإجراءات الجنائية هو منحى خاطئ، ينعكس بشكل سلبي على الحريات الفردية و في مقدمتها الحق في الخصوصية، الأمر الذي حدا بالفقه الأمريكي إلى لفت النظر إلى إشكالية أثارت جدالا خصيبا بين الفقهاء حول معيار التمييز بين الضبط و التفتيش متسائلا عن العمل الذي يعد منطلقا لوقوع التفتيش و الحد الفاصل بينهما.

من السهل تحديد متى يبدأ التفتيش المادي (التقليدي) و متى ينتهي، لأنّ القاعدة الإجرائية التقليدية كانت مبنية دائما على الفرضية المادية لمحل التفتيش، فتفترض ارتباط هذا الإجراء الجنائي بشيء يشغل حيّزا ذا بُعد مادي، محددا بشكل ناف للجهالة سواء كان هذا المحل مسكنا أو شخصا أو مراسلات، إذ يتمّ الشروع في التفتيش باستكشاف معلومات حول المحل الذي جرى تفتيشه، فتحديد اللحظة التي يستهل فيها التفتيش في إطار هذا النهج التقليدي أمر بسيط للغاية، و المعيار المعتمد في ذلك هو تعيين اللحظة التي يحدث فيها انتهاك الخصوصية، على سبيل المثال فإنّ تفتيش المسكن يحدث في الوقت الذي يتمّ فيه فاتح باب هذا المبنى أو الشقة السكنية و ينتهي بمغادرة القائم بالتفتيش لهذا المسكن، و هذه الحقائق هي من البديهيات لدى فكر الإثبات التقليدي⁽¹⁾.

غير أنّ ترجمة هذا المعيار - القائم على انتهاك التوقع المعقول للخصوصية كنقطة لانطلاق التفتيش - في البيئة الرقمية يثير العديد من التساؤلات، هل يحدث التفتيش المعلوماتي عند معالجة الحاسوب للبيانات و قراءتها؟ أم عندما يقوم الحاسوب بإخراج هذه البيانات إلى شاشة العرض أو الطابعة؟⁽²⁾، هل يقع الضبط عند سحب البيانات من القرص الصلب؟ أم عندما يغادر القائم بالتفتيش و بحيازته وسيط التخزين؟ أم عندما يفقد المالك القدرة

(1) و هذا المعيار المادي تضمنته المادة 44 من قانون الإجراءات الجزائية الجزائري و هو ما نستشفه من عبارة " لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص...مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش".

(2) Orin S. Kerr, Searches and Seizures in a Digital World, op cit, p 551.

على تغيير و حذف البيانات؟ أم عند عزل البيانات ذات الصلة بموضوع التحقيق عن تلك التي لا علاقة لها بالموضوع؟⁽¹⁾.

هل مجرد الولوج إلى النظام المعلوماتي يعدّ تفتيشاً؟ و هل يعدّ كذلك فيما لو إنصبّ الإطلاع فقط على بيانات الملف في شكلها الخام (bit)، أو اقتصر الاستعراض فقط على بيانات سطحية كحجم الملف، أو طبيعته (نصوص أو صور) دون الإطلاع على محتواه، هل محاولة لجوء القائم بالتفتيش النفاذ إلى محتويات وسيط التخزين مع تعذر فتحها و استعراضها لوجود نظام تشفير حال دون ذلك، يعدّ عملاً من أعمال التفتيش أو يبقى في حدود الضبط فقط ؟ هل مغادرة النظام بمثابة انتهاء عملية التفتيش بما يحضر القيام به مجدداً بدون إذن قضائي جديد؟

في ضوء هذا التّعقد، يرى جانب من الفقه الأمريكي أنّ الحد الفاصل بين وقوع التفتيش المعلوماتي من عدمه هو مدى قيام الإطلاع البشري على البيانات المخزّنة، إذ تتمّ عمليات التفتيش المعلوماتي عن طريق توجيه أوامر إلى جهاز الحاسوب لمعالجة البيانات و من ثمّ إرسالها إلى جهاز المراقبة أو ما يسمى بجهاز العرض أو وحدة المخرجات، فإذا ما تعرضت هذه المعلومات للإطلاع البشري - السلطة القائمة بالتفتيش - فإنّه في هذه اللحظة على وجه التحديد يحدث التفتيش المعلوماتي بالمعنى الذي يريده القانون و هو ما يسمى بالنهج القائم على الاستعراض أو الكشف "exposure-based approach"⁽²⁾، فوفقاً لهذا الجانب من الفقه إذا لم تخضع البيانات للملاحظة البشرية المباشرة بالعين المجردة، فإنّ كافة الإجراءات السابقة التي تتخذها السلطات الإجرائية لا تعتبر تفتيشاً.

و في الحقيقة إنّنا لا نؤيّد مطلقاً مسلك هذا الجانب من الفقه، لأنّه يقيد التكييف القانوني للإجراء بتحقيق انتهاك "حق السرّ" وفقاً لمنظور هذا الحق بمفهوم تقليدي أو مادي و ليس من منطلق المفهوم الواسع "للحرية الفردية" و ما يتفرع عنه من حقه في الأمن و السكينة، و محاولة إسقاط هذا المفهوم على التفتيش المعلوماتي يقودنا إلى القول أنّه عند النفاذ إلى النظام المعلوماتي مع استحالة فتح الملفات التي يحتويها لا يعدّ بمثابة تفتيش لأنّه لا يتحقّق معه الإطلاع البشري على أيّة معلومات، و نفس الوضع يتحقّق فيما لو تمّ فعلاً الولوج إلى

(1) Josh Goldfoot, op cit, p 133.

(2) Orin S. Kerr, op cit, p 547.

القرص الصلب و تبين في نهاية المطاف أنه خال تماما من أي معلومات أو أن صاحب الشأن لم يسبق له استعمال ذاكرة الجهاز نهائيا.

ألا يعدّ الإجراء في هذه الفروض تفتيشا دقيقا لمستودع السرّ، و لو أجزنا هذا الفرض لصح القول بأنّ دخول مسكن خال من الموجودات لا يعدّ بمثابة تفتيش و الأمر خلاف ذلك، لذا نرى الإصرار على أنّ حرمة المعلومات مستمدة من حرمة الحياة الخاصة للأفراد، و يجب أن لا يقتصر مدلولها على "الحق في السرّ" بمفهوم ضيق فالنّافذ إلى النّظام المعلوماتي يعتبر تدخلا في الحياة الخاصة أيّا كان محتوى دعامة التّخزين الرّقمية و لو كانت خالية من البيانات أو لم تتضمن أية بيانات محرّجة أو غير قانونية.

و من مظاهر الدّلالة على التّوسع في مفهوم التّفتيش في سياق التّفتيش عن الأدلّة المعلوماتيّة ما يكشف عنه حكم حديث صادر عن المحكمة العليا ببنسلفانيا الأمريكية في قضية **Commonwealth v. Fulton** و الذي خلصت من خلاله المحكمة إلى أنّ الفعل البسيط المتمثل في تشغيل الهاتف المحمول يشكّل تفتيشا و يجب خضوعه للمقتضيات التي يفرضها التّعديل الدستوري الرّابع، من منطلق أنّ هذا الإطلاع ينطوي على مساس بالحرية الفردية بحكم الكم الهائل من البيانات الشّخصية الموجودة على الجهاز و التي تعتبر العامل الحاسم في تحديد التّكييف الصّحيح لهذا الإجراء، و ذكرت المحكمة أنّه لا يوجد فرق بين رصد شاشة العرض الداخليّة و الخارجيّة للهاتف المحمول و بين تفتيش سجل المكالمات إذ يؤدي كلا الإجراءين للوصول ليس فقط إلى "مجرد أرقام هواتف"، بل و أيضا إلى "أي معلومات تعريف شخصية قد يضيفها الفرد" إلى جهات الاتصال الخاصة به، بما في ذلك صورة المتصل أو الاسم المعين للمتصل أو مرسل الرّسالة النّصية⁽¹⁾.

و هناك اتجاه فقهي سلك مسلك التّوسع المبالغ فيه، مدفوعا باعتبارات واقعية تبرّر عدم إنطباق المفاهيم القانونية التّقليدية على المستجدات التي أفرزتها الثّورة الرّقمية، فيرى هذا الاتجاه أنّ التّفتيش إجراء استثنائي يقيدّ حقا فرديا هو الحق في الخصوصية، أمّا الضّبط فهو يقيدّ حقا فرديا ماليا على الشّيء محل الضّبط كحق الملكية و الحيّزة لما فيه من تعطيل لحق المالك في استعمال ملكيته، إلّا أنّ ترجمة هذا المفهوم في البيئة الرّقمية يجعل نسخ الملفات-

(1) Commonwealth v. Fulton, 179 A.3d 475 (Pa. 2018). [

التي درج القضاء الأمريكي على اعتباره يدخل في خانة الضبط- هو بمثابة تفتيش، لأن الحق الذي يقيد الضبط الرقمي لا يقتصر على حق الملكية طالما أن الأجهزة الرقمية و كذا النسخة الأصلية من البيانات المضبوطة تبقى بحوزة المالك، بل يمتد هذا التقييد إلى الحق في الخصوصية و حرمة البيانات التي وقع عليها الضبط⁽¹⁾.

و تدعيما لموقفه يرى هذا الجانب من الفقه أنه إذا ما اعتبرنا أن الخصوصية تقوم على السرية و استقلال الفرد بأسراره فإن هذه الحقوق تصبح عرضة للخطر متى تم النسخ الرقمي، و يستند في دعم موقفه إلى أحكام قضائية عديدة اعترفت بوضوح بخطر الضبط الرقمي على الحق في السرية⁽²⁾، مبررا موقفه بحجة أخرى مؤداها أن حصول الحكومة على نسخة من بياناته الشخصية يناقض حق الفرد في استقلاليته بأسراره المعلوماتية، بحيث يزداد هذا الإنتهاك خطرا كلما تواصل الضبط من حيث النطاق الزماني، بدليل ذلك التوجس السائد لدى الأفراد خيفة من إطلاع الحكومة على محتوى المضبوطات التي هي في حيازتها، لذا كان من الطبيعي في نظره اعتبار إجراء الضبط الرقمي في هذه الحالة بمثابة تفتيش لانطوائه على تقييد لحق شخصي.

(1) لمزيد من التفصيلات بشأن الجدل الفقهي الدائر حول الحدود الفاصلة بين الضبط المعلوماتي و التفتيش المعلوماتي راجع بصفة خاصة مقال (بدون مؤلف) بعنوان:

Note: «Digital Duplications and the Fourth Amendment», HARV. L. REV. Vol. 129, 2016, pp 1048 et ss.

(2) و من بين أهم الأحكام القضائية التي تعرّضت إلى أن الضبط المعلوماتي يقيد الحق في الخصوصية و هو ما يكشف عنه الحكم الصادر عن محكمة Eastern بنيويورك في حكمها الصادر بتاريخ 17 ماي 2012 في معرض فصلها في مدى مشروعية طول مدة الضبط المعلوماتي حيث أشارت في إحدى حيثيات حكمها "تحتوي صورة المستند على نفس المعلومات الموجودة في المستند الأصلي، إلى الحد الذي يكون لدى مالك المستند اهتمامات تتعلق بالخصوصية فيما يتعلق باحتفاظ الحكومة بالمستند الأصلي، سيكون لدى المالك شواغل تتعلق بالخصوصية متطابقة مع احتفاظ الحكومة بنسخة من هذا المستند. على سبيل المثال، يمكن أن يؤدي ضبط حساب بريد إلكتروني شخصي، بالإضافة إلى الأدلة التي تقع ضمن نطاق إذن التفتيش، إلى الكشف عن اتصالات شخصية بين زوج يغش زوجته أو اتصالات بين الفرد و عائلته بخصوص حالة طبية محرجة، تقع هذه الاتصالات بوضوح خارج نطاق إذن البحث في هذه الحال، و بالتالي فإن احتفاظ الحكومة على المدى الطويل بصور هذه الرسائل يمثل نفس المخاوف المتعلقة بالخصوصية حال احتفاظ الحكومة بالرسائل الأصلية".

United States v. Metter, 860 F. Supp. 2d 205, 212 (E.D.N.Y. 2012).

و قد لقيت هذه الحجة صداها لدى القضاء الأمريكي الذي بات يعترف بخطر الضبط الرقمي على الحريات الفردية، و من تطبيقات ذلك ما قضت به المحكمة الابتدائية لمنطقة كولومبيا في قضية *Klayman v Obama* أين خلصت إلى أنّ مجرد عملية "جمع البيانات الوصفية" تشكّل تفتيشاً، و أمرت الحكومة ليس فقط بوقف عملية تحليل البيانات، بل و محو المعلومات التي هي في حيازتها⁽¹⁾، بيد أنّ معظم الجهات القضائية لم تتراجع عن سوابقها بهذا الشأن، و استقرت على أنّ النسخ الرقمي يعتبر مجرد ضبط و لا يتجاوز إلى التفتيش⁽²⁾.

من هنا يبدو جلياً أنّ طبيعة البيانات الرقمية قد أضفت نوعاً من الغموض على الحدود الفاصلة بين الإجرائين إذا لم تؤدي في الحقيقة إلى طمسها بشكل كلي، و في تقديرنا ينبغي التسليم بكون كل من "الضبط" و "التفتيش" في البيئة المعلوماتية يقيدان "حقاً شخصياً" هو الحق في الخصوصية، من منطلق ما تتمتع به المعلومات من حرمة تجاوزت بكثير حرمة المساكن و المراسلات التقليدية، غير أنّها يختلفان في درجة هذا التقييد، فبينما يمثل الضبط الرقمي مجرد تهديد لهذا الحق، فإنّ التفتيش المعلوماتي يتعدى ذلك إلى درجة أخطر و هو انتهاك هذا الحق⁽³⁾.

و لو تأملنا جيداً في نصوص الإتفاقية الأوروبية لمكافحة الجرائم المعلوماتية⁽⁴⁾، و الإتفاقية العربية لمكافحة جرائم تقنية المعلوماتية⁽¹⁾، لوجدنا أنّ دلالتها تقطع بكون المعيار

(1) *Klayman v. Obama*, 13-cv-851 (D.D.C. Feb. 10, 2014).

(2) و في هذا الصدد لجأ القضاء الأمريكي إلى حماية الحق في الخصوصية إزاء التفتيش المعلوماتي عن طريق تقييد النطاق الزمني للضبط، بخصوص هذه الإشكالية راجع الصفحة 232 و ما بعدها من هذه الأطروحة.

(3) و هذه الحقيقة قد سلّمت بها المحكمة الأوروبية لحقوق الإنسان حين اعتبرت أنّ مجرد جمع بيانات الإتصال و الإحتفاظ بها يعدّ بمثابة تدخل في الخصوصية سواء أتمّ الإطلاع على تلك البيانات و استخدامها لاحقاً أم لا، بل حتى مجرد إلتقاط معلومات الاتصالات ينشئ تدخلاً في الخصوصية.

CEDH, arrêt S. et Marper c. Royaume Uni, 4 décembre 2008 nos 30562/04 et 30566/04, §67, « le simple fait de la conservation ou de la mémorisation de données à caractère personnel par les autorités publiques (...) doit passer pour emporter des conséquences directes sur la vie privée de l'individu concerné, que ces données soient utilisées par la suite ou non ».

(4) حيث تنص المادة 19 من هذه اتفاقية بودابست التي وردت تحت عنوان (تفتيش و ضبط البيانات المعلوماتية المخزنة) : "يجب على كلّ طرف أن يتبنى الإجراءات التشريعية و أية إجراءات أخرى يرى أنّها ضرورية من أجل تخويل سلطاته المختصة سلطة التفتيش أو الولوج بريقة مشابهة: لنظام معلوماتي أو لجزء منه و كذلك للبيانات المعلوماتية المخزنة فيه و على أرضه ... لدعامة تخزين معلوماتية تسمح بتخزين بيانات معلوماتية...".

الفاصل بين وقوع التفتيش من عدمه هو تحقق "النفاذ إلى النظام المعلوماتي"، و قد عبّرت عن ذلك صراحة في قولها "تلتزم كلّ دولة طرف بتبني الإجراءات الضّرورية لتمكين سلطاتها المختصة من التفتيش أو "النفاذ إلى النظام المعلوماتي" *perquisitionner ou à accéder d'une façon similaire* (2).

و قد تطرقت المذكرة التفسيرية لهذه الإتفاقية إلى معالجة هذه الإشكالية و لو بشكل ضمني ضمن البند رقم 138 منها، و نلمس ذات التوجه لدى المشرّع الإجمالي الفرنسي إذ أنّ مدلول عبارات نص المادة 57 فقرة أولى من قانون الإجراءات الجزائية كانت واضحة بحيث اعتبرت أنّ التفتيش يقع بتحقيق النفاذ و الولوج إلى النظام المعلوماتي (3).

أمّا بالنّسبة إلى التشريع الجزائري فالملاحظ أنّ صياغة النص لا تعكس نيّة و إرادة المشرّع، حيث نصّت المادة 5 من القانون الجزائري 09/04 على أنّه "يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية المختصة في إطار قانون الإجراءات

(1) تنص المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية الواردة تحت عنوان: "تفتيش المعلومات المخزّنة" على مايلي: تلتزم كل دولة طرف بتبني الإجراءات الضّرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى أ- تقنية معلومات أو جزء منها و المعلومات المخزّنة فيها أو المخزّنة عليها ب - بيئة أو وسيط تخزين معلومات تقنية معلومات و الذي قد تكون معلومات التقنية مخزّنة فيه أو عليه...).

(2) الجدير بالذكر أنّ المادة 26 من الاتفاقية العربية مستلهمة من المادة 19 من الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية، إلّا أنّ الترجمة يشوبها عدم الوضوح و الدقّة و يظهر ذلك في عبارة (تمكين السلطة المختصة من التفتيش" أو "الوصول" إلى تقنية المعلومات)، و لفظ "الوصول" يفيد لغة بلوغ الشيء، بما يستفاد منه أنّ الوصول إلى المنظومة المعلوماتية التي كانت بعيدة عن أنظار سلطات إنفاذ القانون معناه الاستحواذ أي الضبط، و ذلك خلافا لقصد المشرّع العربي، الذي إنصرفت نيّته إلى اعتبار التفتيش واقع متى تمّ النفاذ إلى النظام المعلوماتي و هو ما يتطابق مع مدلول المصطلح المترجم Accès و الفارق بين المصطلحين بليغ، فالأول يكيّف على أنّه ضبط و الثاني يأخذ مدلول التفتيش.

(3) Article 57-1 De la Loi française n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, JORF n°129 du 5 juin 2003 dispose que : " Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial" .

الجزائية ... الدخول بغرض التفتيش و لو عن بعد، إلى: (أ) منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها. (ب) منظومة تخزين معلوماتية...⁽¹⁾.

إذ المستفاد من هذا النص أنّ النفاذ إلى النظام المعلوماتي إجراء تقني مستقل عن التفتيش، أي بمثابة إجراء يسبق وقوع التفتيش و من مستلزماته، يقتصر المقصود منه على الوصول إلى محل التفتيش (البيئة المعلوماتية)، أمّا التفتيش بالمعنى القانوني فيراد به وسيلة لجمع الأدلة يتم من خلالها الإطلاع على هذه المعلومات باعتبارها محلا له حرمة الأسرار.

و كما أشرنا إليه سابقا، فإنّ هذا التفسير ينطوي في حقيقته على قدر من التجاوز في فهم جوهر "قاعدة الحرمة" إذ لا يقف مدلولها على "الحق في السر" بل كل ما يحيط "بأمن الفرد و هدوئه و استقلاله"، فيتحقق التفتيش متى طال محلا له حرمة خاصة و لو لم يفض إلى الإطلاع على أي شيء معاقب عليه. إذ لو أجزنا حكم نص المادة 5 المشار إليها أعلاه لأصبح النفاذ إلى النظام المعلوماتي طليقا من غير أي قيد على السلطة الإجرائية و يصبح حينئذ من العبث الحديث عن الحرية الفردية، فالنص الإجرائي بصيغته الحالية مخالف لمقتضى المادة 26 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، لذا يتعيّن إعادة

(1) الحقيقة أنّ هذا المعيار مفقود لدى التشريعات العربية، خاصة في ضوء الصياغة التشريعية الرديئة للقواعد الإجرائية المعلوماتية، التي تثير الغموض و اللبس بشأن موقف التشريعات تجاه هذه المسألة، و يكفي الإطلاع على المادة 06 من القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات و التي وردت تحت عنوان الأوامر القضائية المؤقتة حتى يتم التأكد من هذه الحقيقة حيث تنص: "لجهة التحقيق المختصة - بحسب الأحوال- أن تصدر أمراً مسبباً، لمأموري الضبط القضائي المختصين، لمدة لا تزيد على 30 يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر مما يلي:

1- ضبط أو سحب أو جمع أو النّحفظ على البيانات و المعلومات أو أنظمة المعلومات، و تتبعها في أيّ مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه، و يتم تسليم أدلتها الرقمية للجهة مصدرة الأمر على ألا يؤثر ذلك على استمرارية النّظم و تقديم الخدمة إن كان لها مقتضى.

2- البحث و التفتيش و الدخول و النفاذ إلى برامج الحاسب و قواعد البيانات و غيرها من الأجهزة و النّظم المعلوماتية تحقياً لغرض الضبط..."

و باستقراء الفقرة الأخيرة يلاحظ الخلط في المفاهيم و التعبير عن ذات الإجراء بألفاظ مختلفة (البحث و التفتيش و الدخول و النفاذ) بشكل يوحي استقلالها عن بعضها البعض، رغم وحدة المقصود و هو التفتيش و لا ريب أنّ ذلك يشكل شائبة في الصياغة الشرعية لقاعدة إجرائية يفترض فيها الدقة لتعلقها بالحرّيات الفردية.

صياغته على نحو يوسع من مفهوم التنقيش المعلوماتي الذي يراد به في نظرنا "النفاذ إلى النظام المعلوماتي بحثاً عن عناصر الحقيقة"⁽¹⁾.

و من التطبيقات القضائية الحديثة التي تؤكد التفسير الذي توصلنا إليه، ما يكشف عنه الحكم الصادر عن المحكمة العليا الفيدرالية الأمريكية سنة 2018 في قضية *Carpenter v. United States* التي توصلت إلى "أنّ المعلومات المتعلقة بالتحديد الجغرافي لموقع المتّهم التي تمّ الحصول عليها من خلال سجلات شركات الاتصالات اللاسلكية (مزود الخدمة) كانت نتاج عملية تنقيش"⁽²⁾.

و في تعليقه على هذا الحكم يرى الفقه أنّ التنقيش قد وقع في مرحلة من مراحل هذه العملية، بحيث يمكن القول أنّ التنقيش تسبب في الحصول على المعلومات، و أنّ المهم في نظر المحكمة هو "النتيجة" و ليس "العملية" أي يحدث التنقيش بمجرد الحصول على المعلومات⁽³⁾.

غير أنّ هذا الحكم من جهة أخرى يكتفه الكثير من الغموض و يطرح تساؤلاً عميقاً مؤداه هل يقع التنقيش عند "الحصول على المعلومات" أو عند "النفاذ إلى المعلومات"؟

واقع الأمر أنّ المحكمة أجابت بـكنا الفرضيتين، ففي نظر المحكمة فإنّ التنقيش الإلكتروني يحدث عند النفاذ إلى سجلات موقع الهاتف *access to cell-site* و يظهر ذلك

(1) Article 5, alinéa 1 de Loi n° 09-04 du 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication stipule que "Les autorités judiciaires compétentes ainsi que les officiers de police judiciaire, agissant dans le cadre du code de procédure pénale et dans les cas prévus par l'article 4 ci-dessus, peuvent, **aux fins de perquisition, accéder**, y compris à distance".

و مؤدى عبارة "يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية المختصة في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عليها في المادة 4 أعلاه، **بهدف التنقيش، الولوج، و لو عن بعد**، أنّ النفاذ إلى النظام المعلوماتي يتحقق به التنقيش و بذات الوقت هو مرادفا له و ليس مستقلاً عنه.

(2) Supreme Court of the United States, *Carpenter v. United States*, No. 16-402, 585 U.S. (2018).

(3) Orin Kerr, *When Does a Carpenter Search Start and When Does It Stop?*, [Available online]. Retrieved November 26, 2019, from [://www.lawfareblog.com/when-does-carpenter-search-start-and-when-does-it-stop](http://www.lawfareblog.com/when-does-carpenter-search-start-and-when-does-it-stop).

بجلاء في بعض أشطر الحكم، على سبيل المثال نذكر منها بشكل موجز قول المحكمة⁽¹⁾:
 "تعرض هذه الحالة السؤال عما إذا كانت الحكومة تجري تفتيشاً بموجب التعديل الدستوري الرابع عندما تقوم بالنفاذ إلى سجلات الهاتف المحمول التي تتيح حقائق شاملة لتحركات المستخدم في تاريخ سابق"، "السماح للحكومة بالنفاذ إلى هذه السجلات يتعارض مع التوقع المعقول للحق في الخصوصية"، "بمجرد نقرة زر، يمكن للحكومة النفاذ إلى مستودع من معلومات المتعلقة بالموقع الجغرافي دون أي تكاليف تقريباً"، "وبناءً عليه، عندما تمكنت الحكومة من النفاذ إلى هذه السجلات، انتهكت توقعات المتهم المعقولة بالخصوصية في جميع تنقلاته"، "نحن نرفض منح الدولة سلطة النفاذ غير المقيد إلى قاعدة بيانات شركة الاتصالات اللاسلكية الخاصة بمعلومات الموقع الفعلي".

و على نقيض ذلك اعتبرت المحكمة في شطر لآخر من حكمها أنه بمجرد حصول سلطة التحقيق على المعلومات يكون التفتيش واقعا دون حاجة إلى النفاذ إلى هذه السجلات و استطلاع محتوياتها و يستفاد ذلك من قول المحكمة⁽²⁾: "تتضمن القضية المعروضة علينا

(1) جاء في هذا الحكم:

1 "This case presents the question whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements."

2 "Allowing government access to cell-site records contravenes that expectation."

3 "With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense."

4 "Accordingly, when the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements."

5 "We decline to grant the state unrestricted access to a wireless carrier's database of physical location information."

(2) من بين ما جاء بهذا الحكم:

1 "The case before us involves the Government's acquisition of wireless carrier cell-site records revealing the location of Carpenter's cell phone whenever it made or received calls."

2 "The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment."

3 "Having found that the acquisition of Carpenter's CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records."

4 "The Government's acquisition of the cell-site records here was a search under that Amendment."

5 "Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one get a warrant."

استحوذت الحكومة على سجلات موقع الهاتف اللاسلكي التي تكشف عن موقع المتهم وقت إجراء أو تلقي مكالمات،" كان استحوذت الحكومة على سجلات موقع الهاتف بمثابة تفتيش بالمعنى المقصود بمقتضى التعديل الدستوري الرابع"، "بعد أن وجدنا أن الاستحوذ على سجلات موقع الهاتف يشكل عملية تفتيش نستنتج أيضاً أن الحكومة يجب أن تحصل عموماً على إذن بناء على أسباب محتملة قبل الحصول على مثل هذه السجلات"، "كان حصول الحكومة على سجلات موقع الهاتف هنا عبارة عن تفتيش بموجب التعديل الدستوري الرابع"، "قبل إجبار شركة الاتصالات اللاسلكية على تسليم سجلات موقع الهاتف الخاصة بالمستخدم، يكون التزام الحكومة قائماً بوجود الحصول مسبقاً على إذن قضائي".

بمعزل عن التعارض الذي شاب الحكم، فمع التسليم جدلاً بكون الحصول على النظام المعلوماتي لا يشكل تفتيشاً في اعتقادنا، فإنه على خلاف ذلك يعتبر مجرد النفاذ إليه تفتيشاً بالمعنى الذي يريده القانون، و لو لم يتم استعراض المحتوى المعلوماتي الذي تضمنته. و الحقيقة أن إشكالية الحدود الفاصلة بين الضبط و التفتيش لم تطرح في البيئة المادية لسبب بسيط يجد أساسه في كون "الضبط" كان دوماً أثراً "للتفتيش"، أي أن الضبط يجري لاحقاً للمساس بالسر، ف ضبط شيء في المسكن يوجب دخوله و تفتيشه، و عند تطبيق هذا النهج على التفتيش المعلوماتي نصطدم بحقيقة فرضتها التقنية و هي لزوم وقوع الضبط أولاً قبل التفتيش، و هي النتيجة التي تقودنا إلى طرح تساؤل حول مدى صحة هذه الفرضية و أثرها في الإخلال بالتوازن بين الحريات الفردية و حق الدولة في الوصول إلى الحقيقة و استنفاثها لحقها في العقاب؟

الفرع الثالث: مراحل التفتيش المعلوماتي و الضبط الرقمي

تتميز مراحل تنفيذ عملية التفتيش عن الأدلة المعلوماتية في مظاهرها بطابع خاص يضيف عليها طابعاً من الذاتية، إذا ما قورنت بخطوات التفتيش عن الأدلة المادية، ففي عمليات التفتيش التقليدية تحصل الضبطية القضائية القائمة بالتفتيش على إذن بالإطلاع على مكان مادي معين، بحثاً عن دليل مادي ما و هو ما يعرف بألية التفتيش ثم الاسترجاع "Mechanism Search-and-Retrieve"⁽¹⁾، أي الدخول إلى المسكن و تفتيشه و ضبط الدليل

(1) Orin S. Kerr, Search Warrants in an Era of Digital Evidence, Mississippi Law Journal, Vol 75, Issue 1, 2005, p 97.

المادي المحدد في الإذن القضائي، و هذه الخطوات في تنفيذ عملية التفتيش تسري على المسكن و الشخص و مراسلاته، أي حقيقة أن تنفيذ التفتيش يتم ضمن خطوة واحدة و هي أن يكون الضبط معاصرا للتفتيش، و هي من المسلمات في فكر الإثبات التقليدي، و تجد لها تنظيما في القانون و استقرارا في التعامل القضائي معها.

في مقابل ذلك يؤدي تنفيذ الإذن بالتفتيش عن الدليل المعلوماتي إلى إضافة خطوة ثانية، إذ تسعى هذه السلطة للحصول على إذن بالتفتيش ضمن مساحة مادية يحددها و يصفها الإذن القضائي بحثا عن أجهزة التخزين الرقمية (دعامات التخزين الإلكترونية)، ثم تستحوذ السلطة الإجرائية على هذه الأجهزة التي تم العثور عليها خلال التفتيش المادي للتحليل خارج الموقع "Off-Site" في وقت لاحق، و ذلك ضمن مخابر التحليل الحاسوبي الشرعي المتخصصة و هي عملية قد تستغرق أسابيع أو أشهر و هو ما يعرف بآلية الاسترجاع ثم التفتيش "Retrieve-And-Search Mechanism"⁽¹⁾.

و من هذا المنطلق فإن التفتيش المعلوماتي يتم عبر خطوتين "Two-Stage Approach"، تعرف الخطوة الأولى بمرحلة "التفتيش المادي" (Physical Search Stage)، عندما تدخل السلطة الإجرائية المختصة بالتحقيق الموقع المطلوب تفتيشه تسترجع أجهزة التخزين الرقمية المحددة في الإذن القضائي و ينصب الضبط على الأجهزة الإلكترونية التي يرجح أنها قد تحتوي على أدلة ذات صلة بالجريمة موضوع التحقيق، و في معظم الحالات، تقوم هذه السلطة الإجرائية إما بإنشاء "نسخة رقمية" للقرص الصلب "Digital Duplication" أو ضبط الدعامات المادية.

و تعرف الخطوة الثانية بمرحلة التفتيش المعلوماتي (Electronic Search Stage) و التي تتعلق بالبحث عن الأدلة المعلوماتية، و التي عادة ما تتم بعد فترة طويلة من البحث عن الأدلة المادية، و يبدو هنا من الواضح أن فعالية التفتيش المعلوماتي تفرض ضرورة التفتيش المادي أولا يعقبه الضبط المادي و يليه التفتيش المعلوماتي، و هو ما يوضح حجم التباين بين آلية التفتيش عن الأدلة المادية" و "آلية إسترجاع الأدلة المعلوماتية"⁽²⁾.

(¹) Orin S. Kerr, Loc.Cit.

(²) Orin S. Kerr, Search Warrants in an Era of Digital Evidence, op cit, p 91. ("The dynamic is physical search, physical seizure, and then electronic search.").

بيد أنّ جانب من الفقه يرى أنّه من الخطأ التفكير في "عملية الاسترداد ثم التفتيش" هذه كنموذج فريد من نوعه للتفتيش المعلوماتي، وأنّ معظم عمليات التفتيش لا تتطلب خروجاً عن عملية التفتيش ثم الاسترداد المعتادة باستثناء بعض الحالات النادرة التي تختلط فيها الوثائق بحيث لا يمكن تصنيفها عملياً في الموقع، و يقوم هذا النقد على أن تطبيق هذه القاعدة يجرّ إلى الضبط الشامل قبل إجراء التفتيش على نحو يؤدي إلى انتهاك صارخ لحق المتّهم في الخصوصية نتيجة استبقاء سلطة التحقيق لهذه البيانات بحوزتها⁽¹⁾.

و هو رأي شاذ نخالفه لعدم وجود أي بديل عملي آخر يسمح باسترجاع الدليل المعلوماتي دون الإستناد إلى هذه القاعدة لسهولة و سرعة تدمير هذا النوع من الأدلة، أمّا بشأن تشابك و اختلاط البيانات فهي من الأمور المسلّم بها في الوقت الراهن نتيجة القدرة الهائلة للتخزين الرقمي الذي تتمتع به الأجهزة الرقمية الحديثة زيادة على التعقيد التقني الذي يفرضه المجرم على نظامه المعلوماتي منعا من الوصول إليه. و قد أبدى القضاء الأمريكي تمسكه بهذه القاعدة، مشيراً إلى أنّ خصوصية عمليات التفتيش المعلوماتي تتطلب إتخاذ "خطوات معاكسة" لعمليات التفتيش التقليدية⁽²⁾، إلى غاية تبني هذا الاجتهاد الفقهي بتعديل نص المادة 41 من قانون الإجراءات الجنائية الفيدرالي سنة 2009 تحت وطأة الطبيعة الفردية للأدلة المعلوماتية التي اقتضت إتباع هذا النهج، لأنّه من المتعدّر فحص كلّ البيانات التي يحتويها وسيط التخزين الرقمي لحظة التفتيش المادي، خاصة إذا تمّ التفتيش في مسكن المتّهم و تعددت وسائط التخزين أو شملها التشفير بحيث تستغرق عملية التفتيش أوقات طويلة جداً فتتعدّد صور الانتهاك و تزداد خطورة، لأنّه يطلّ حرمة المسكن و سكينته شاغليه طيلة فترة التفتيش، فضلاً على انتهاك حرمة المعلومات، و لا ريب أنّ هذا الإجراء غير مشروع تماماً و لا يحتاج إلى نص يقرّر عدم مشروعيته⁽³⁾.

(1) James T. Stinsman , computer seizures and searches rethinking the application of the plain view doctrine, Temple Law Review, Vol. 83.(2011) , p1100.

(2) See In re Search of 3817 W. West End, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004) ("It is frequently the case with computers that the normal sequence of 'search' and then selective 'seizure' is turned on its head.").

(3) في سياق مقارب يعلّق الفقه حول هذا الحق قائلاً " للمتّهم بوصفه إنساناً الحق في أن يحيى حياته الخاصة بعيداً عن تدخل الغير و بمنأى عن العلانية فالحق في الحياة الخاصة هو من حقوق الإنسان التي أكدها الإعلان العالمي لحقوق الإنسان ، فالحياة الخاصة هي قطعة غالية من كيان الإنسان لا يمكن إنتزاعها منه و إلاّ تحوّل إلى أداة

فالتعقيد التكنولوجي للمعلومات و تزايد سعة التخزين الرقمي يفرض تغيير عملية تنفيذ التفتيش المعلوماتي من خطوة واحدة إلى خطوتين، مما يجعل تغيير القواعد القانونية حتمية طبيعية لتغيير الحقائق التي أفقدت التوازن بين حق المجتمع في مواجهة الجريمة و حق الفرد في صون حريته و في ضوء هذه الحقيقة يثور التساؤل فيما إذا كان المشرع الجزائري قد تطرق إلى الخطوات بالتنظيم الذي يحفظ فعالية الإجراء و شرعيته؟

المبحث الثاني

مقدمات التفتيش عن الأدلة المعلوماتية

يعدّ الضبط جائزا في نطاق الغاية منه و هي إظهار الحقيقة، غير أنّ واقع التخزين الرقمي بما فرضه من كم هائل للبيانات بشكل مختلط و معقد مع لجوء المجرم إلى جعل الملف بريء حجابا للملف المجرّم، أمر يوجب الضبط أولا يليه التفتيش، و هو ما يتجاوز الغاية من التفتيش كمبدأ عتيد يحمي الحريات الإنسانية إلى التوسع في ضبط كل ما يحوزه المتهم من بيانات سواء بشكل مباشر (مطلب أول)، أو عن طريق مزود الخدمات (مطلب ثاني).

المطلب الأول: الضبط العرضي الشامل للبيانات الموجودة بحوزة المتهم

إنّ الضبط العرضي الشامل لما يحوزه المتهم من دعائم تخزين رقمية يشكّل توسعا في الاستثناء على حساب القاعدة الأصلية، إذ أنّ "آلية الاسترجاع ثم التفتيش"، تشكّل مظهرا من مظاهر تراجع الشرعية لحساب الفعالية، و يحقّ لنا التساؤل في ضوء ذلك على أساس مشروعيته (مطلب أول) و تنظيمه التشريعي (مطلب ثاني) و ضوابطه (مطلب ثالث).

صمّاء خالية من القدرة على الإبداع الإنساني، فالإنسان بحكم طبيعته له أسراره الشخصية و مشاعره الذاتية و صلاته الخاصة و خصائصه المتفردة و لا يمكن للإنسان أن يتمتع بهذه الملامح إلا في إطار مغلق يحفظها و يهيئ لها سبيل البقاء، و تقتضي حرمة الحياة الخاصة أن يكون للإنسان حق إضفاء السرية على مظاهرها و أثارها و من هنا كان الحق في السرية وجها لازما للحق في الحياة الخاصة لا ينفصل عنه". راجع أحمد فتحي سرور، المرجع السابق، ص 753.

الفرع الأول: أساس مشروعية الضبط العرضي الشامل للبيانات الموجودة بحوزة المتهم

إن دور الشريعة في نطاق الحياة الخاصة لا يمكن إدراكه أو تلمس حقيقته إلا من خلال التعرف على ما قد يترص بتلك الحياة و يحيط بها من مخاطر، يتحقق وقوعها قبل وقوع التفتيش، و الذي تعتبر مشروعيته نتيجة من نتائج المبدأ الأساسي الذي تقوم عليه كثير من النظم القانونية ألا و هو مبدأ ترجيح المصالح العامة على المصلحة الخاصة عند الضرورة، و طبقا لهذا المبدأ تعطي الهيئة الاجتماعية لنفسها السلطات و الحقوق اللازمة لحماية مصالحها العليا و لو أدى ذلك إلى تقييد الأفراد و حقوقهم في الحدود التي ينص عليها القانون⁽¹⁾.

و من هنا فإن الضبط الرقمي ليس سوى إحدى تطبيقات هذا المبدأ الذي يقوم على ترجيح حق الجماعة على حق الفرد عند التعارض، و هو الحق في الإثبات الجنائي و التوصل إلى إظهار الحقيقة الواقعية، و لأنه لا وجود لحق مطلق في القانون، فإن الإشكالية تبرز واضحة ما هو أساس مشروعية الضبط الرقمي الشامل كحق تبرره ضرورة التوصل إلى الدليل المعلوماتي؟

لم يطرح هذا السؤال لدى فكر الإثبات التقليدي لكون الضبط المادي دوما كان مرتبطا بحدود التفتيش، فنطاق الضبط تحدده الغاية من التفتيش، بل هو أثر مباشر للتفتيش في معظم الأحيان، إذ لا يتجاوز الضبط حدود الإذن و إلا كان باطلا، و مبدأ عدم تجاوز الغاية من التفتيش يعدّ من المبادئ العتيدة في الإجراءات الجنائية الذي تقوم عليه قاعدة مشروعية الدليل الجنائي إذ يترتب على تجاوز هذا المبدأ بطلان التفتيش و صيرورة الدليل المستمد منه مجرد واقعة مادية تخلو من أي قيمة قانونية، غير أنّ انعكاس خطوات التفتيش بصيرورة الضبط من مقدمات التفتيش و من مستلزمات تنفيذه، بدل أن يكون أثرا له، واقع جعل فعالية التفتيش مرتبطة بالضبط العرضي الشامل و إلا فقد التفتيش معناه.

لقد بات من المسلم به في الوقت الزاهن ذلك الإنتشار المذهل لوسائل تقنية المعلومات بين مختلف شرائح المجتمع، و مع تزايد استعمالها سعت الشركات المصنّعة إلى العمل على زيادة سعة التخزين الرقمي لهذه الأجهزة، بحيث أصبح أصغر جهاز رقمي بإمكانه تخزين

(1) توفيق محمد الشاوي، المرجع السابق، ص 123.

ملايين المعلومات، تختلف في تواجدها داخل النظام المعلوماتي من حيث طبيعتها و حجمها أو حتى مكان تواجدها على نحو يستحيل معه معرفة ما إذا كان جهاز تخزين معين يحتوي على أدلة معلوماتية معينة أم لا قبل ضبطها و إخضاعها للتفتيش.

و هذه الممارسة القضائية تشكّل تهديدات كبيرة للخصوصية بدلاً من ضبط الدليل المعلوماتي على وجه التحديد دون التوسع الشامل للضبط المعلوماتي، و هناك جملة من الاختلافات القائمة بين الأدلة المعلوماتية و الأدلة المادية التي تتطلب "الضبط الرقمي العرضي الشامل أولاً"، و "التفتيش في وقت لاحق":

أولاً، من المؤكّد أنّه سيتمّ خلط المعلومات **Intermingling Of Documents** التي تشكّل دليلاً على وجود نشاط إجرامي ضمن بيانات أخرى غير ذات صلة بمسهدف التفتيش، و نظراً للحجم الهائل لسعة تخزين الأجهزة الرقمية، سيكون حجم البيانات على أي جهاز رقمي كبيراً، و هذا يعني أنّ أي وسيط تخزين رقمي يتمّ ضبطه و يحتوي على أدلة على الإجرام سيشمل أيضاً كميات هائلة من البيانات التي يحتمل أن تكون حميمة، مما يثير مخاوف خطيرة بشأن الخصوصية⁽¹⁾.

فالبحث عن الرسائل النصية للهاتف الخليوي قد لا يكشف فقط عن الاتصالات بين الجناة، و لكن يكشف أيضاً رسائل نصية خاصة غير مرتبطة بالجريمة موضع التحقيق، و ينطبق الشيء نفسه على الأشكال الأخرى من البيانات، مثل تاريخ البحث على الأنترنت الذي يكشف عن استفسارات حول الأعراض الصحية أو تعاطي مواد طبية معينة، و وفقاً للمحكمة العليا الفيدرالية الأمريكية "عادة ما يعرض تفتيش الهاتف المحمول للحكومة أكثر من التفتيش الشامل للمنزل"⁽²⁾.

ثانياً، يختلف الدليل المعلوماتي عن الأشكال الأخرى من الأدلة، لأنّ طبيعتها كبيانات مجرّمة أو دليلاً عن الجريمة ليست دائماً واضحة، و هذا ما يعقّد جهود فرز الأدلة المعلوماتية عما تختلط به من بيانات أخرى لا علاقة لها بالجريمة، لأنّ هذه البيانات عادة ما

(¹) Berman Emily, Digital Searches, the Fourth Amendment, and the Magistrates' Revolt, Emory Law Journal, Emory University School of Law, Vol 68, Issue 1, 2018, p 7.

(²) Riley v. California, 134 S. Ct. 2473 (2014).

تكون "مخفية أو مضغوطة أو محوطة أو مفخخة" بطرق تجعل من المستحيل اكتشافها دون الوصول إلى أعداد كبيرة من الملفات الخارجة عن نطاق الإذن القضائي⁽¹⁾.

و أبعد من ذلك ففي بعض الحالات يمكن أن يكون الملف البريء ستارا للملف المجرّم لأنّ القدرات التخزينية في البيئة الرقمية و هي تستوعب هذا الكم غير المحدود من المعلومات لم تتفاعل كلياً مع القانون الجنائي حيث لم يتم التّوصل إلى إمكانية قيامها بعملية فرز ذاتية داخلية للملفات البريئة و تلك المجرّمة التي تعدّ موضوعاً للدليل الجنائي موضوع التفتيش⁽²⁾. و قد توسّعت هذه الرّؤية نتيجة لاعتراف القضاء بعدم وجود منهج لمحرك بحث محدّد يمكن اللّجوء إليه لتقصي الدليل المعلوماتي لحظة التفتيش المادي دون ضرورة الضبط الشامل⁽³⁾.

فالإشكال هنا هو إشكال عملي بحث، عندما يكون لدى سلطة التّحقيق سبب محتمل و قرائن قوية للاعتقاد بأنّ ملفاً معلوماتياً معيّناً موجوداً في مكان ما من المسكن و يشكّل دليلاً جنائياً، فإنّها عادة تجهل مواصفات جهاز التخزين الإلكتروني الذي يحتوي على هذا الدليل بالتّحديد دون غيره من الأجهزة، قد يكون لدى المتّهم عدد من أجهزة التخزين الرقمية و أقراص مدمجة و غيرها، و لا يمكن للسلطة الإجرائية التي تنفذ إذن التفتيش أن تفتش جميع أجهزة التخزين في الموقع، (موقع التفتيش المادي) لأنّ ذلك يتطلب وقتاً طويلاً، البديل العملي الوحيد لحل هذه الإشكالية هو اللّجوء إلى ضبط معظم أو جميع أجهزة التخزين الرقمية و تفتيشها خارج الموقع في وقت لاحق⁽⁴⁾.

ثالثاً، علاوة على الأسباب المساقاة آنفاً، قد يترتّب على محاولة تفتيش وسائط التخزين في الموقع الإضرار بالأدلة نفسها، ففي بعض الحالات فإنّ استخدام الحاسوب قد يغيّر الأدلّة المسجّلة على القرص الصّلب، كما أنّ أجهزة الحاسوب المتّصلة بالإنترنت هي أيضاً عرضة للخطر، لإمكانية الوصول إلى المعلومات المخزّنة عن بعد و حذف البيانات و تدميرها، بناءً

(1) United States v. Hill, 459 F.3d 966, 974-75 (9th Cir. 2006).

(2) عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي المرشد الفيدرالي الأمريكي لتفتيش و ضبط الحواسيب توصلاً إلى الدليل الإجراء في التّحقيقات الجنائية، ص 23.

(3) حول موضوع مدى فعالية و دستورية استراتيجية التفتيش في ضوء القضاء الأمريكي راجع الصفحة 240 و ما بعدها من الرسالة.

(4) Orin S. Kerr , Ex Ante Regulation of Computer Search and Seizure, Virginia Law Review, Vol 96, Issue 6, 2010, p 1249.

على ذلك فإنّ أفضل طريقة عموماً لمراجعة وسائط التخزين تكون خارج الموقع حيث يمكن لخبراء التحليل الحاسوبي الشرعي ضمان سلامة البيانات⁽¹⁾.

واقع الأمر أنّ سعة التخزين الضخمة لأجهزة التخزين الرقمية، إضافة إلى سهولة إخفاء الأدلة و سهولة حذفها و لو عن بعد هي مبررات عملية للضبط الشامل قبل التفتيش، و إذا كان على سلطة التحقيق أن "تجد إبرة في كومة القش"، و كان هذا التفتيش قد يستغرق أسابيع أو أكثر، يجب على سلطة التحقيق الإختيار من بين ثلاثة خيارات متاحة. أولاً، يمكنها ضبط كافة البيانات و إجراء التفتيش المعلوماتي اللاحق خارج الموقع. ثانياً، يمكن أن تجلب عدد قليل من المحققين أو من تندبهم إلى موضع تواجد أجهزة التخزين الرقمية، و البقاء هناك لبضعة أسابيع لإنهاء عملية التفتيش المعلوماتي. و ثالثاً، يمكنهم ببساطة التسليم بعدم إمكانية إجراء التفتيش نهائياً لأنّ عمليات التفتيش تستغرق وقتاً طويلاً جداً، و من بين هذه الخيارات الثلاثة، الخيار الأول هو الخيار الأقل سوءاً⁽²⁾.

و بالنظر إلى هذا الواقع فإنّ القضاء المقارن يتجه نحو التسليم بمشروعية و صحة الضبط العرضي الشامل أو المفرط الذي تجاوز نطاق الإذن القضائي، و ذلك تأسيساً على مبررات تقنية محضة أهمها عدم قابلية الملفات الحاسوبية للتجزئة، و هو ما استندت إليه محكمة النقض الفرنسية⁽³⁾ و كذا المحكمة الأوروبية لحقوق الإنسان⁽⁴⁾، و إما لضمان تفتيش موجز نسبياً ضمن مساكن المتهمين، غير أنّ هذه الجهات القضائية لم ترسم حدوداً موضوعية لهذا النهج المتساهل⁽⁵⁾.

(1) H. Marshall Jarrett, et al, op.cit, p 78.

(2) 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, p 11.

(3) Cass. Crim., 30 novembre 2011, n° 10-81749 ,Bull. crim. 2011, n° 243, Cass. Crim. 27 novembre 2013, n°12-85.830, Bulletin criminel 2013, n° 242.

(4) CEDH, AFFAIRE MESSIER c. FRANCE, 30 juin 2011, 25041/07, § 43.

(5) و وفقاً للدائرة السادسة فإنّ التعقيد التقني الذي تتميز به البيانات المعلوماتية يتطلب اللجوء إلى كافة محتويات الجهاز لتحديد الملف المستهدف بالتفتيش بما يجعل الضبط الكلي معقولاً و قد تأكد هذا التحليل في عديد من القضايا مثل قضية Guest v. Leis و هو النهج الذي سلكته الدائرة التاسعة في قضية United States v. Hay التي استندت إلى التفسير الذي تضمنته الإفادة الخطية للضبطية القضائية التي بينت الأسباب الداعية إلى ضبط النظام المعلوماتي بأكمله و أخذه خارج الموقع بسبب الوقت، و الخبرة المطلوبة، و كذا السيطرة على هذه البيئة لإجراء تحليل سليم". و في

و تعتبر الدائرة التاسعة الجهة القضائية الوحيدة في الولايات المتحدة الأمريكية التي استلزمت شرطا إجرائيا إضافيا لأجل مشروعية الضبط العرضي الموسع، بحيث توجب على الضبطية القضائية ضرورة تقديم المبررات الكافية للضبط الشامل ضمن الإفادة الخطية (طلب الاذن بالتفتيش) و ذلك في قضية *United States v. Hill*⁽¹⁾.

و ما نتوصل إليه أنه عندما يتعلق الأمر بالأدلة المعلوماتية يصعب تحديدها بإجراء تفتيش سريع، إذ ليس من الممكن مطالبة سلطة التحقيق بالتدقيق في كل هذه المعلومات بحثاً عن البيانات التي تستجيب للإذن القضائي وقت التفتيش المادي و ضبط المعلومات التي تعدّ موضوعاً للدليل الجنائي فقط دون غيرها من المعلومات لحظة التجميع " فالضبط الموسع هو إجراء لازم و متواصل ضمن إجراءات التفتيش عن الأدلة المعلوماتية"⁽²⁾.

و بناء على الإعتبارات الواقعية التي ساقها القضاء و الفقه لتبرير مشروعية الضبط العرضي الشامل، يتضح جلياً أنّ متطلبات فعالية التفتيش تقتضي التوسع في الضبط الرقمي في البداية ثم إخضاع المضبوطات للتفتيش المعلوماتي لاحقاً، و في ذلك ترجيح واضح لاعتبارات الفعالية على حساب الشرعية لأنّ التوسع في الاستثناء أصبح هو القاعدة، و مما

ضوء هذا الواقع التكنولوجي لاحظ القضاء أنّ أضيق عملية تفتيش و ضبط محتمل ترجح الحصول على الأدلة الموضحة في الإذن هي في معظم الحالات تفتيش جهاز الحاسوب و جميع الأقراص المتاحة، يراجع بهذا الخصوص الأحكام التالية:

Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001).

United States Giberson, 527 F.3d 882, 886 (9th Cir. 2008).

United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999).

(¹) جاء في قرار الدائرة التاسعة الصادر بتاريخ في 11 أوت 2006 في قضية *United States v. Hill* ما يلي: "نحن نتفق مع المحكمة الابتدائية أنه في ظل هذه الظروف فإن اشتراط إجراء التفتيش في الموقع و عزل المواد الإباحية للأطفال قبل إزالة كل وسائط التخزين، لا يؤدي اغفاله إلى بطلان التفتيش. ومع ذلك، فإنّ هذا لا يعني أنّ الحكومة لديها سلطة إجراء تفتيش عشوائي عند التماس أو تنفيذ أذن التفتيش المعلوماتي. فعلى الرغم من أنّ تكنولوجيا المعلومات قد تبرّر من الناحية النظرية الضبط الشامل للأسباب المبيّنة أعلاه، فإنّه يقع على الحكومة أن تثبت للقاضي من الناحية الواقعية لماذا تكون هذه السلطة الواسعة للتفتيش و الضبط معقولة في الحالة قيد النظر. فقد تكون هناك حالات لا يكون فيها للحكومة أساس للاعتقاد بأنّ التفتيش المعلوماتي ينطوي على نوع من التعقيدات التكنولوجية التي من شأنها أن تجعل التفتيش الفوري في الموقع و إزالة الأدلة ذات الصلة أمراً غير عملي. وبالتالي، يجب أن يكون هناك حدوداً قبل أن تلجأ الحكومة "لضبط كومة قش للتفتيش عن الإبرة".

(²) *Berman Emily*, op cit, p 8. « **the reality that over-seizing is an inherent part of the electronic search process** ».

يؤسف له هو عجز الفقه و القضاء حتى الآن عن إيجاد حدود ترسم نطاق التفتيش المادي و الضبط الرقمي بحيث أصبحت هذه المراحل الإجرائية فعلا طليقة من غير قيد، فهناك فجوة كبيرة عند محاولة تطبيق المبادئ الإجرائية التقليدية على التفتيش المعلوماتي بحيث يختل التوازن بين متطلبات الفعالية و الشرعية.

الفرع الثاني: الموقف التشريعي من مشروعية الضبط العرضي الشامل للبيانات الموجودة بحوزة المتهم

جاء في التوصية الرابعة من توصيات المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات في مجال حركة إصلاح الإجراءات الجنائية و حماية حقوق الإنسان و الذي عقد في ريو دي جانيرو البرازيل في الفترة من 4-9 سبتمبر 1994 " في مرحلة التحقيق الإبتدائي، و التي تسبق مرحلة المحاكمة، فإن قرينة البراءة تتطلب إذا ما اتخذت وسائل قسرية تطبيق مبدأ التناسب *Le Principe De Proportionnalité* الذي يقيم علاقة معقولة بين جسامه الإجراءات القسري في مساسه بالحقوق الأساسية من ناحية، و بين مدى تناسب هذا الإجراء وفقا للقصد المتوخى منه من ناحية أخرى..."⁽¹⁾.

كما أشار ذات المؤتمر أنه و نظرا للتعدد و تنوع البيانات المدرجة في نظم معالجة البيانات، فإن تنفيذ المكناات القسرية المنوطة برجال السلطة العامة يجب أن يكون متناسبا مع الطابع الخطير للانتهاك و لا يسبب سوى الحد الأدنى من إعاقة الأنشطة القانونية للفرد، كما يجب عند بدء التحريات أن يوضع في الاعتبار بالإضافة إلى القيم المالية التقليدية كل القيم المرتبطة بتكنولوجيا المعلومات مثل ضياع فرصة اقتصادية، التجسس، انتهاك حرمة الحياة الخاصة فقط أو مخاطرة الخسارة الاقتصادية، كلفة إعادة بناء تكامل البيانات كما كانت من قبل.

و بناء على هذه التوصيات يثار الإشكال حول موقف التشريعات و على وجه التحديد التشريع الجزائري فيما إذا كان قد تمكن من مراعاة هذا المبدأ في مجال الضبط الرقمي؟

لا ريب أن الضبط مسموح به في نطاق الغاية منه، و الغاية المبررة للضبط هي كشف الحقيقة، فوجود صلة بين الجريمة و البيانات التي يتم ضبطها هو معيار الضبط و ما زاد

(1) Association internationale de droit penal , XVIème Congrès International de Droit Pénal , (Rio de Janeiro, Brésil/Brazil, 4-10 Septembre 1994) , Revue Internationale de Droit Penal , 1-2 éme trimestres Editions ERES, Paris 1995, p 35.

عن ذلك يعتبر تعسفا يجبر إلى بطلان الإجراء، و هو ما يعبر عنه بمبدأ التناسب الذي يقتضي لزوم قصر نطاق الضبط الرقمي على البيانات التي تفيد في إظهار الحقيقة، و لأنّ التغيرات في الحقائق تتطلب تغييرا في القواعد القانونية نجد أنّ المشرع بمقتضى القانون 09/04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و مكافحتها قد نص على جواز الضبط الرقمي في حالتين:

الحالة الأولى، عالجتها المادة 6 و التي نصت "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و أنّه ليس من الضروري حجز كل المنظومة، يتمّ نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحرار وفقا للقواعد المقررة في قانون الإجراءات الجزائية...".

و الحالة الثانية، تطرقت إليها المادة 7 من نفس القانون و التي ورد فيها "إذا استحال الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية يتعيّن على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة".

إنّ المتأمل لهذه النصوص يتجلى له بوضوح أنّ المشرع الجزائري لا يزال يعتمد المنهج التقليدي في تنفيذ التفتيش، و هو النهج القائم على خطوة واحدة أي الضبط لحظة التفتيش، على الرغم من أنّ الواقع التطبيقي يفرض خلاف ذلك، إذ يستحيل تصور النجاح في الوصول إلى الدليل المعلوماتي و استرداده وفقا لهذا المنطق التقليدي، خاصة في الوقت الراهن الذي يشهد طفرة غير مسبوقة في مجال سعة التخزين الرقمي، سواء التخزين الرقمي المحلي الممثل في مختلف الأجهزة أو ضمن الخوادم (الحوسبة السحابية)، مع وجود برامج تشفير بالغة التعقيد و مجانية منشورة على الشبكة العنكبوتية تتجاوز في غالب الأحيان خبرات الضبطية القضائية التي تجري التفتيش في الموقع.

و كما سبق و أن رأينا كيف واجه القضاء الأمريكي هذه الإشكالية بميل واضح نحو اعتبارات الفعالية، إلى أنّ تدخل المشرع بتعديل القاعدة 41 من القواعد الفيدرالية للإجراءات الجنائية سنة 2009 معترفا بالطبيعة الفريدة لعمليات التفتيش و الضبط في البيئة المعلوماتية أين أجاز الضبط العرضي الكلي للبيانات في مرحلة أولية ثم إخضاع المواد المضبوطة إلى

مراجعة لاحقة⁽¹⁾. و السؤال المثار هنا هل يجوز الضبط الإجمالي العرضي بناء على إذن بالتفتيش المعلوماتي وفقا للتبظيم التشريعي الجزائري الذي لم ينظم الخطوة الأولى من التفتيش؟

قدمنا أن الضبط الرقمي إجراء مستقل تماما عن التفتيش المعلوماتي و أنه يشكل قيذا على الحق في الخصوصية و إن لم تصل خطورة هذا القيد إلى درجة انتهاك هذا الحق، إلا أنه قد يتحقق هذا الخطر في فترة ما من فترات الضبط متى طالمت مدته فهو بهذا التميز له صفة استثنائية، و الصفة الاستثنائية لهذا النوع من إجراءات التحقيق يترتب عليها نتيجة هامة تميزها عن الإجراءات العادية، و هذه النتيجة هي أنها واردة في القانون على سبيل الحصر، فلا يجوز للمحقق أن يقوم بأي إجراء يترتب عليه مساس بحريات الأفراد أو حقوقهم أو يفرض عليهم إلتزامات إيجابية إلا إذا كان هناك نص صريح في القانون يجيز هذا الإجراء⁽²⁾.

فكلما كان هناك "خطر المساس بالحرية الفردية" عندما تباشر الدولة الإجراءات اللازمة للكشف عن الحقيقة، تعين على المشرع أن يتدخل في هذه الحالة لكي يقرر الحدود التي تتطلبها المصلحة الاجتماعية للمساس بالحرية الفردية من خلال الإجراءات الجنائية، و السلطة التشريعية هي التي تملك وحدها تقرير القيم الاجتماعية، و الأحوال التي يجوز فيها المساس بالحرية في حدود معينة، و ذلك بالقدر اللازم لتحقيق التوازن بين مصالح المجتمع و حقوق الفرد، و تطبيقا لذلك قضت محكمة النقض الفرنسية بأن المشرع وحده من يملك المساس بحرية الأفراد⁽³⁾.

لذا نحن نعتقد أن هذه النتيجة مفترض طبيعي لمبدأ الشرعية الإجرائية، فإذا كان من البديهي أن كل إجراء استثنائي يقيد حقوقا فردية و جب خضوعه لمقتضيات الضرورة المبررة له و في حدودها إلتزاما بالشروط و القيود التي فرضها القانون، فمن باب أولى يعد عملا غير مشروع القيام بإجراء لم يجزه القانون أصلا⁽⁴⁾، و هذا القصور التشريعي يجعل المشرع مطالب

(1) Berman Emily, op cit, p 52.

(2) توفيق محمد الشاوي، المرجع السابق، ص 130.

(3) أحمد فتحي سرور، الشرعية الدستورية و حقوق الإنسان في الإجراءات الجنائية، بدون رقم الطبعة، دار النهضة العربية، القاهرة، 1995، ص 235.

(4) و هذه الضمانة الإجرائية و إن كانت من المبادئ العامة التي لا تحتاج إلى نص يقرها للإلتزام بحكمها، إلا أننا نجد أن المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات في مجال حركة إصلاح الإجراءات الجنائية

بالتدخل بتنظيم نطاق الضبط الرقمي العرضي و مدته. و تنظيم التفتيش من خطوة واحدة إلى خطوتين، لأن القاعدة الحالية لا تجيز الضبط الأولي فإذا ما اتخذته سلطة التحقيق كان عملها مشوبا بعدم المشروعية⁽¹⁾.

و في الحقيقة لا يوجد سوى التشريع الفيدرالي الأمريكي الذي عالج هذه المسألة أمّا باقي التشريعات فتخضعها للقواعد التقليدية باعتبار أنّ معظم التشريعات المقارنة بما فيها الإتفاقية العربية لمكافحة جرائم تقنية المعلومات مستلهمة حرفيا من الإتفاقية الأوروبية لمكافحة الجريمة المعلوماتية و التي بدورها أغفلت معالجة تنظيم مرحلة التفتيش المادي و الضبط الرقمي بخصوص البيانات التي في حوزة المتهم.

و إذا كان هذا حال التشريع الإجرائي فيما يتعلّق بالضبط العرضي الشامل في الفرض الأول الذي تكون فيها البيانات التي يُعتقد أنّها تشكّل موضوعا للدليل المعلوماتي بحوزة المتهم، فإنّ السؤال يثار بخصوص مدى شرعية التنظيم الإجرائي لمقدمات التفتيش

و حماية حقوق الإنسان و الذي عقد في ريو دي جانيرو البرازيل في الفترة من 4-9 سبتمبر 1994 قد نص عليها مؤكدا " لتجنب تعسف السلطات الرسمية، فإن القيود التي ترد على حقوق الإنسان عن طريق رجال السلطة العامة لا يمكن أن تكون مقبولة إلا في الحالة التي تكون فيها مرتكزة على قواعد قانونية واضحة و دقيقة و متماشية مع المعايير الدولية لحقوق الإنسان، الانتهاكات غير المشروعة لحقوق الإنسان التي يرتكبها رجال السلطة العامة يمكن أن تبطل الدليل المتحصّل منه بالإضافة إلى تقرير المسؤولية الجزائية لرجل السلطة العامة الذي انتهك القانون".

(1) قد تتعرض هذه النتيجة التي توصلنا إليها إلى النقد على أساس المغالاة في تصوير ذاتية الضبط الرقمي، في وقت يمكن تجاوز هذه الإشكالية بالرجوع إلى القاعدة العامة التي تضمنتها المادة 42 من قانون الإجراءات الجزائية التي أجازت "ضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة" دون الحاجة إلى تنظيم إجرائي خاص بالضبط المعلوماتي، لأن الخطوة الأولى من التفتيش المعلوماتي (مرحلة التفتيش المادي و مرحلة الضبط المعلوماتي) و يجب أن تبقى بغير نطاق يحددها، لعدم وجود بديل عملي آخر يضمن التوصل إلى الدليل قبل التفتيش عن كافة أجهزة التخزين الرقمية و ضبطها، لأنّه يستحيل معرفة محتويات هذه الأجهزة و ما إذا كانت فعلا تحتوي على الدليل المعلوماتي المستهدف بالتفتيش أم لا قبل إجراء الضبط العرضي الشامل و تفتيشها لاحقا، و مثل هذا القول على صحته فإنّه يتجاهل الفارق الكبير بين أثر الضبط المادي و الضبط المعلوماتي على الحريات الفردية، بحكم ضخامة البيانات المخزّنة التي لا علاقة لها بالواقعة الإجرامية، فتطبيق هذا النص في البيئة الرقمية يختلف من حيث آثاره حال تطبيقه في البيئة المادية بشكل له انعكاسات بالغة الخطورة على الحريات، لذا يجب أن يحضى هذا الإجراء بتنظيم خاص في مرحلة التفتيش المعلوماتي عن طريق "تضييق النطاق الزمني للتفتيش" و استبعاد الأدلة العرضية، وفق ما سنعالجه لاحقا عند الحديث عن أسلوب تنفيذ تفتيش النظام المعلوماتي و ضوابط هذا العمل الإجرائي في "مرحلة ما بعد التفتيش".

المعلوماتي في الفرض الذي تكون فيه بيانات المتهم بحوزة طرف آخر و هو "مقدم الخدمات"؟

المطلب الثاني: ضبط بيانات المتهم الموجودة بحوزة مزود الخدمة

من الطبيعي أن يقدم الجاني على محو البيانات فور إتمام مشروعه الإجرامي، لذا يتعين على سلطة التحقيق التفتيش عن هذه البيانات لدى مزود الخدمة و التي يحفظها في إطار أداء خدماته و يتم ضبطها بموجب آلية الأمر بالحفظ و التسليم، ما يقتضي منا تحديد مفهوم هذا الإجراء الجزائي المستحدث (فرع أول)، و تحديد ضماناته و قيوده (فرع ثاني)، و نطاقه (فرع ثالث).

الفرع الأول: الحفظ العاجل للبيانات المعلوماتية المخزنة و تسليمها

يعتبر إجراء الحفظ العاجل لبيانات المعلوماتية المخزنة و تسليمها، من الإجراءات الوقائية المستحدثة في النظم الإجرائية الرأهنة، وقد تمت الإشارة إلى هذا الإجراء الجزائي لأول مرة ضمن لائحة الجمعية العامة للأمم المتحدة رقم (63-65) المؤرخة في 22 جانفي 2001 المتعلقة بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، إذ نصت المادة الأولى فقرة "و" على "ضرورة سماح الدول الأعضاء لجهاتها المختصة بالاستدلال أمر مزود الخدمات بالحفظ السري للمعطيات الإلكترونية المتعلقة بالتحقيقات الجنائية"⁽¹⁾.

عموما عرّف البرلمان الأوروبي ضمن مقترحه رقم 2018/0108 المتعلق بأوامر إنتاج و حفظ الأدلة الجنائية الإلكترونية بين دول الإتحاد الأوروبي هذا الإجراء بكونه يمثل قرارا ملزماً صادراً عن السلطة المختصة إلى مزود الخدمة يطالب من خلاله هذا الأخير بالمحافظة على دليل إلكتروني لطلب توليده لاحقاً⁽²⁾، و عرّف أيضا الأمر بالإنتاج (التسليم، التقديم،

(¹) لائحة الجمعية العامة للأمم المتحدة رقم (63-65) المؤرخة في 22 جانفي 2001 المتعلقة بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، وثيقة رقم: A/RES/56/121 .

(²) Article 2 alinéa 2 de la Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale COM/2018/225 final - 2018/0108 (COD) stipule: «injonction européenne de conservation»: une décision contraignante d'une autorité d'émission d'un État membre imposant à un fournisseur de services proposant des services dans l'Union et établi ou représenté dans un autre État membre de conserver des preuves électroniques en vue d'une demande ultérieure de production »

التوليد، الإفصاح) بأنه القرار الملزم الموجّه إلى مزود الخدمة لإنتاج دليل إلكتروني⁽¹⁾، و يطلق على هذا الإجراء بإجراءات التجميد السريع «procédure de congélation rapide».

ما يلاحظ في هذا الصدد أنّ التنظيم القانوني لإجراء حفظ البيانات المعلوماتية المخزّنة و إجراء انتاجها و تسليمها إلى سلطات التحقيق قد ورد بشكل منفصل ضمن الاتفاقيات الدولية و التشريعات الداخلية بشكل يوحي باستقلال الإجراءات عن بعضهما البعض، إلا أنّنا نرى خلاف ذلك على نحو ما سنبينه لاحقاً.

و عندنا فإنّ الأمر بالحفظ العاجل للبيانات المخزّنة هو إجراء جزائي وقائي يرد به صدور قرار من سلطة التحقيق المختصة إلى مزود الخدمة يتضمن إلزاماً بحفظ البيانات المخزّنة لديه بتاريخ سابق عن صدور الأمر بالحفظ و العمل على تأمينها من خطر التعديل و الحذف و ذلك لفترة زمنية محدّدة متى توافرت أسباب معقولة و قرائن كافية ترجّح أن تكون هذه البيانات كاشفة للحقيقة⁽²⁾، أمّا الأمر بالإنتاج فهو أمر مرتبط بالأمر بالحفظ يوجّه إلى مزود الخدمة لتسليم البيانات المعلوماتية التي تضمّنها أمر الحفظ السابق.

إنّ هذه الوسيلة الإجرائية في الحقيقة تمثّل نهجا مختلفا عن باقي الوسائل الإجرائية التقليدية، و تظهر فعاليتها في كونها تكفل عدم فشل التفتيش المعلوماتي لا لسبب سوى تجنب حذف البيانات خلال فترة التحقيقات الطويلة نسبياً، ففي كثير من الأحيان يتطلّب تعيين الجاني الذي ارتكب الجريمة تحليلاً لبيانات الحركة و يمكن أن يساعد بروتوكول الأنترنت الذي استعمله الجاني بوجه خاص سلطات التحقيق على تعقبه، بل و من الممكن في بعض الحالات تعيين أحد الجناة رغم أنّه كان يستعمل أجهزة أنترنت طرفية عمومية لا تتطلب الإفصاح عن الهوية طالما كانت سلطة التحقيق تملك النفاذ إلى بيانات الحركة ذات الصلة، و من الصّعوبات الرئيسية أنّ بيانات الحركة ذات الأهمية الكبيرة تحذف في كثير من الأحيان

(¹) Article 2 alinéa 1 de la Proposition de règlement du Parlement européen et du Conseil op, cit, stipule: «injonction européenne de production»: une décision contraignante d'une autorité d'émission d'un État membre imposant à un fournisseur de services proposant des services dans l'Union et établi ou représenté dans un autre État membre de produire des preuves électroniques »

(²) و تعريفنا للأمر بالحفظ العاجل للبيانات المعلوماتية المخزّنة مستلهم من تعريف المشرّع الأوروبي لتعريف الأمر بالحفظ الأوروبي - أي الصادر عن دولة عضو في الإتحاد الأوروبي إلى مزود خدمات يقع مقره ضمن دولة أخرى تابعة للإتحاد الأوروبي.

بصورة تلقائية بعد فترة قصيرة من الوقت إلى حد ما، و سبب هذا الحذف الأوتوماتيكي هو إنتهاء أيّ عملية مثل إرسال بريد إلكتروني أو النفاذ إلى الأنترنت أو تنزيل ملفات يعني إنتهاء الحاجة إلى بيانات الحركة التي تولدت أثناء العملية و التي تمكّن من إجراء العملية⁽¹⁾.

من منظور إقتصادي يهتمّ معظم مقدمي الأنترنت بحذف المعلومات بأسرع ما يمكن نظرا لأنّ تخزينها لفترة طويلة يتطلّب سعة تخزينية كبيرة و مكلفة جدا و مع ذلك فإنّ الجوانب الإقتصادية لا تشكّل السبب الوحيد لقيام سلطة التّحقيق بالمسارعة في التّحقيق⁽²⁾، إذ أنّ التّوجه التشريعي الحالي لمعظم الدّول التي تراعي الحق في الخصوصية المعلوماتية يقوم على إلزام مزوّد الخدمات على حذف بيانات الحركة بعد زوال أسباب حفظها من التّاحية التّقنية و حظر تخزينها وفق ما تمليه مثلا أحكام الفقرة الأولى من المادة 6 من التّوجيه الأوروبي رقم 85 لسنة 2002 المتعلّق بخصوصية الاتصالات الإلكترونيّة حيث تنص على أنّه "يجب حذف بيانات حركة السّير المتعلّقة بالمشاركين و المستعملين التي يعالجها و يخزّنها مقدم شبكة اتصالات إلكترونية للجمهور أو إخفاء هويتها بعد توقف الحاجة إليها لأغراض إرسال رسالة..."⁽³⁾.

تحرص المذكرة التفسيرية لاتفاقية بودابست في تصديرها لهذه المادّة على ذكر الهدف المتوخى منها و هو إعطاء السّطات المختصّة إمكانية الأمر أو الحصول بطريقة مشابهة على الحفظ العاجل للبيانات المخزّنة، و يتطلّب الحفظ حماية البيانات التي سبق وجودها و تخزينها من كل ما يعرضها لخطر التّغيير أو التّجريد من صفتها أو حالتها الرّاهنة، فهو يتطلّب أن تكون البيانات مصانة على نحو آمن من كل تغيير أو إتلاف و الحفظ لا يتطلّب

(1) ماركو جيري، فهم الجريمة السيبرانية: الظواهر و التّحديات و الاستجابة القانونية، منشورات الإتحاد الدّولي للاتصالات، سوسيرا، 2014، ص 284.

(2) المرجع نفسه، ص 284.

(3) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques « 1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1 »

بالضرورة أن تكون البيانات "مجمّدة" و بالتالي لا يمكن أن تستخدم أو يتمّ الحصول على صورة منها بواسطة المستخدمين الشرعيين و الشّخص الذي يصدر إليه الأمر⁽¹⁾.

و لم تحدّد كل من الإتفاقية بوايست⁽²⁾، و كذا الإتفاقية العربية لمكافحة جرائم تقنية المعلومات⁽³⁾، الطّريقة التي يجب من خلالها أن يُحفظ بالبيانات، فالأمر متروك لكلّ دولة في أن تقيّم النّمادج الملائمة للحفظ و تحديد ما إذا كان في بعض الحالات يمكن لإجراء التّحفظ على البيانات أن يشمل أيضا تجميدها، إنّ عبارة "يأمر أو... يحصل بطريقة مشابهة" الهدف منها التّرخيص بتطبيق وسائل قانونية أخرى للتّحفظ غير الأمر القضائي أو الإداري

(¹) السيادة التي يتمتع بها القانون تفترض أن يلتزم مضمون القانون باحترام الشّريعة وفقا للمبادئ التي يتطلّبها الدّستور، فإذا جاء "القانون" مخالفا للدّستور لحقه عيب عدم المشروعية الدّستورية، و إذا جاء "العمل" مخالفا للقانون لحقه عيب عدم المشروعية "القانونية"، و الشّريعة الدّستورية يلتزم بها المشرّع في وضع القانون كما يلتزم بها القائمون على تطبيقه و تنفيذه، و كل مخالفة للشّريعة عند تطبيق القانون يلحقها عدم المشروعية على أنّ الشّريعة القانونية لا تكتسب قيمتها إلاّ بالالتزام بالشّريعة الدّستورية. يراجع بهذا الخصوص: أحمد فتحي سرور، الشّريعة الدّستورية و حقوق الإنسان في الإجراءات الجنائية، المرجع السابق، ص 259.

(²) تنص المادة 16 من اتفاقية بوايست " الحفظ العاجل لبيانات الحاسوب المخزّنة:

يعتمد كل طرف من يلزم من تدابير تشريعية و تدابير أخرى و ذلك حتّى يمكن لسلطاتها المختصة الأمر أو طلب العمل بصورة عاجلة على حفظ بيانات بعينها على حاسوب بما في ذلك خط سير البيانات المخزّنة بواسطة نظام حاسوبي و خاصة في حالة وجود أسس للإعتقاد بإمكانية تعرض بيانات حاسوبية بصفة خاصة للفقد أو التّعديل.

في حالة قيام طرف بتفعيل الفقرة 1 أعلاه بواسطة إصدار أمر إلى شخص ما بحفظ بيانات حاسوبية مخزّنة بعينها بحوزة الشّخص أو تحت سيطرته فإنّه يتعيّن على هذا الطّرف أن يعتمد ما يلزم من تدابير تشريعية و إجراءات أخرى لإلزام ذلك الشّخص بأن يحفظ و يحافظ على سلامة بيانات الحاسوب المذكورة بالقدر اللازم لفترة زمنية لا تزيد عن 90 يوما على الأكثر حتى تتمكن السلطات المختصة من السّعي لكشفها، كما يمكن لكل طرف تجديد هذا الأمر".

(³) تنص المادة 23 من الاتفاقية العربية " : التّحفظ العاجل على البيانات المخزّنة في تقنية المعلومات :

تلتزم كل دولة طرف بتبني الإجراءات الضّرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزّنة بما في ذلك معلومات تتبع المستخدمين و التي خزّنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد أنّ تلك المعلومات عرضة للفقدان أو التّعديل.

تلتزم كل دولة طرف بتبني الإجراءات الضّرورية فيما يتعلق بالفقرة (1) بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزّنة والموجودة بحيازته أو سيطرته و من أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتّجديد، من أجل تمكين السلطات المختصة من البحث و التّقصي.

تلتزم كل دولة طرف بتبني الإجراءات الضّرورية لإلزام الشّخص المسؤول عن حفظ تقنية معلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي".

أو تحقيق من الشرطة أو النيابة على سبيل المثال و في بعض الدول لا ينص قانون الإجراءات الجزائية على أوامر الحفظ و في هذه الحالة فإنّ البيانات لا يتمّ التّحفظ عليها إلاّ من خلال عمليات التفتيش و الضبط أو الأمر بإنتاج البيانات⁽¹⁾.

غير أنّه ينبغي الحذر من الخلط بين إجراء "حفظ البيانات" أو كما تسميه المحكمة الأوروبية لحقوق الإنسان "الإلتزام بالإحتفاظ الشّامل لبيانات الإتصال" و بين إجراء الأمر بالحفظ العاجل لبيانات حركة السّير أو ما يطلق عليه "إجراء التّجميد السّريع لبيانات حركة السّير"، أمّا "الإلتزام بالإحتفاظ الشّامل لبيانات حركة السّير"، فهو نهج مختلف لكفالة عدم فشل التفتيش، إذ يلزم مزود الخدمة بحفظ بيانات الحركة لجميع المستخدمين بدون إستثناء خلال مدة محدّدة قد تتجاوز سنتين لاستغلالها في التّحقيقات الجنائية مستقبلا.

على أنّ مسألة تثار هنا تتعلّق بموقف المشرّع الجزائري بخصوص الآلية الإجرائيّة التي إنتهجها لحفظ البيانات و الحيلولة دون تمكن المجرم من حذفها قبل استردادها.

الفرع الثاني: التّنظيم التشريعي للأمر بالحفظ العاجل للبيانات المخزّنة

سبق و أنّ أشرنا أنّ الأدلة المعلوماتيّة تتميّز بسرعة تبخّرها و تلاشيها لذا يمثل الوقت جانبا مهما في التفتيش المعلوماتي، لأنّه عادة ما تمر فترة زمنية بين تنفيذ الجريمة و اكتشافها و تبليغ سلطات التّحقيق بها، و لذلك من المهم سن آليات إجرائيّة تمنع حذف البيانات ذات الصّلة مباشرة بعد الشّروع في التّحقيق، و عندنا فإنّ السّؤال المطروح فيما إذا كان المشرّع اعتمد آلية "الإلتزام بالحفظ الشّامل للبيانات أو "الأمر بالحفظ العاجل للبيانات المخزّنة"؟

بالرجوع إلى نص المادّة 10 من القانون 04-09 نجدها تنص "في إطار تطبيق أحكام هذا القانون يتعيّن على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتّحريات القضائيّة لجمع و تسجيل المعطيات المتعلّقة بمحتوى الاتصالات في حينها و بوضع المعطيات التي يتعيّن عليهم حفظها وفقا للمادة 11 أدناه تحت تصرف السلطات المذكورة...".

المستفاد من صياغة هذا النّص أنّ المشرّع لم يعتمد "إجراء الأمر بالحفظ العاجل لبيانات الحركة" و إنّما تبنى نهجا آخر و هو "استبقاء البيانات" أو "الإحتفاظ بالبيانات"

(1) Conseil de l'Europe, Rapport explicatif de la Convention du Conseil de l'Europe sur la cybercriminalité ,op cit, Clause n° 160.

Rétention des données، و يفرض إلّتزام استبقاء البيانات على مقدمي الخدمات الإحتفاظ ببيانات الحركة لفترة معيّنة من الوقت، مع أنّ كافة التّشريعات الأوروبية و العربية قد تبنت كلا النهجين، نهج "الإحتفاظ بالبيانات" و نهج "الأمر بالحفظ العاجل للبيانات".

و من الأمثلة النّمونجية على هذا المسلك ما يقضي به التّوجيه الأوروبي رقم 24 لسنة 2006 المتعلّق بحفظ البيانات و الّذي يعتبر بمثابة قانون أوروبي تلتزم باعتماده كافة دول الإتحاد الأوروبي ضمن تشريعاتها الداخليّة⁽¹⁾، كما تم إدراج آلية الأمر بالحفظ العاجل لبيانات الحركة ضمن التّعديلات المدخلة على قوانين هذه الدّول كما سيأتي بيانه لاحقاً، و نتيجة لإطلاق مصطلحات متشابهة على هاتين الوسيّلتين فقد وقع الكثير من الفقه في الخلط بين الإجراءين⁽²⁾، و عدم التّفريق بينها و بين باقي الإجراءات التّقليدية⁽³⁾.

(¹) Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE .

(²) يكاد يجمع الفقه في الجزائر على أنّ مدلول نص المادتين 10 و 11 القانون الجزائري رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها، يدل دلالة واضحة على أنّ المشرّع الجزائري قد تبنى إجراء الأمر بالحفظ العاجل للبيانات المخزّنة لدى مزود الخدمات، و هذا الرّأي في اعتقادنا ليس صحيح على الإطلاق و لا يوجد أيّ مبرّر يفسّر موقف هذا الفقه، و غني عن البيان أنّه لا يجوز التّوسع في تفسير النصّ على نحو يجاوز إرادة المشرّع باستحداث إجراء جزائي فيه مساس بالحريّة الفردية لم ينص عليه هذا الأخير. حول الرّأي الفقهي الّذي يرى مشروعية الأمر بالحفظ العاجل للبيانات المخزّنة في التّشريع الجزائري راجع: شرف الدين وردة، الإثبات الجنائي بالأدلة الإجرائية دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق و العلوم السياسيّة جامعة بسكرة، 2017، ص 357 - ربيعي حسين، آليات البحث و التّحقيق في الجرائم المعلوماتية، أطروحة دكتوراه كلية الحقوق و العلوم السياسيّة، جامعة باتنة 1، 2016، ص 232 - بن فريدة محمد، الإثبات الجنائي للجرائم المعلوماتية، أطروحة دكتوراه كلية الحقوق و العلوم السياسيّة، جامعة الجزائر 1، 2015، ص 179 - إبراهيمي جمال، المرجع السّابق، ص 103).

(³) في حين ذهب جانب آخر من الفقه (يوسف منصّرة، المرجع السّابق، ص 248) إلى أنّ مشروعية هذا الإجراء مستمدة من أحكام قانون العقوبات، بالقول بجواز لجوء النّيابة العامة إلى هذا الإجراء يجد سنده التّشريعي في نص المادة 187 مكرر من قانون العقوبات الّتي تنص على أنّه "يعاقب بالحبس من شهرين إلى سنة أشهر و بغرامة من 1000 دج إلى 10.000 دج أو بإحدى هاتين العقوبتين فقط كل من لا يمثّل لأمر تسخير صادر و مبلغ وفقاً للأشكال التّنظيمية" و قد عبّر عنه هذا الباحث بمصطلح "تسخير معطيات الاتّصال"، بمقتضاها يجوز لوكيل الجمهوريّة أو بناء على إذن من هذا الأخير الإجازة لضباط الشّرطة القضائيّة تسخير أي شخص أو هيئة خاصة أو عامة يحتمل حيازتها لوثائق مفيدة للتّحري، بما فيها المنظومة المعلوماتية أو معالجة إسمية للمعطيات و لا يكون

على أنه يلاحظ أنّ المشرّع الجزائري لم يفرّق بين البيانات المتعلقة بحركة المرور و البيانات المتعلقة بالمشاركين، إذ يقع على مزود الخدمة الاحتفاظ بها جميعاً⁽¹⁾.

و مع ذلك فإنّ الباحث يرى أنّ عبارة "حفظ" التي استعملها المشرّع توحى بأنّه لا يعير اهتماماً لمسألة ضمان سلامة و أمن المعطيات من خطر التّغيير أو التّعديل و يظهر ذلك بجلاء من خلال استقراء المادّة 11 من القانون 04-09 التي جاء فيها "مع مراعاة طبيعة و نوعية الخدمات يلتزم مقدمو الخدمات بحفظ.... تحدّد مدة حفظ المعطيات المذكورة في هذه المادّة بسنة واحدة من تاريخ التّسجيل" إذ لا جدوى من المعطيات التي تم حفظها أي تسجيلها إذا لم يتم ضمان سلامتها و أمنها، و هكذا يكون المشرّع مدعو إلى تغيير صياغة النّص على نحو يلزم بمقتضاه مزودي الخدمات بضمان حفظ و أمن و سلامة المعطيات المتعلقة بحركة السّير⁽²⁾.

التّعذر بالسّر المهني عائقاً في تسليمها، و الحقيقة أنّ هذا الرّأي ينطوي على قدر من الخلط بين مقتضيات الأمر بالتّسليم و "الإلتزام بالحفظ الشّامل لبيانات حركة السّير"، فالأمر بالتّسليم بمفهوم تقليدي يقتصر على إلزام الشّخص الطّبيعي أو المعنوي بتسليم ما بحوزته مما قد يفيد في كشف الحقيقة أي التسخيرة، فإذا لم يلزم مزود الخدمات بحفظ البيانات فإنّ الأمر بالتّسليم يصبح بدون جدوى لأنّ الإجراء الأخير يقتصر الهدف منه على إجبار مزود الخدمة بتسليم المعطيات دون أن يضمن سلامتها من التّعديل و الحذف، فتسلّم إلى السّلطة القائمة بالتّفتيش وفقاً لوضعيتها لحظة طلبها، في حين يضمن الأمر بالحفظ المحافظة على البيانات المخزّنة بالوضع التي هي عليه دون تغيير أو تعديل أو حذف منذ نشأتها إلى غاية طلب تسليمها، فمفهوم *la réquisition judiciaire* ينطبق في البيئة المعلوماتية على الأمر بالإنتاج *l'injonction de produire*، و ليس الأمر بالحفظ و حجتنا في ذلك أن بيانات المحتوى ليست من طائفة البيانات التي يلتزم مزود الخدمة قانوناً بحفظها فكيف يمكن أمره بتسليمها؟

حول هذه المسألة راجع:

Philippe Belloir. Les réquisitions judiciaires en matière de délinquance numérique. Revue Lamy droit de l'immatériel ex Lamy droit de l'informatique, n°92, 2013, pp 49-53.

(1) و قد إستوحى المشرّع الجزائري هذا النّص حرفياً من المادّة 13-10 R10 من قانون البريد و الاتصالات الفرنسي:

Article R10-13 du C.P.T.E Créé par Décret n°2006-358 du 24 mars 2006 - art. 1 JORF 26 mars 2006.

(2) الجدير بالذّكر أنّ جميع الاتفاقيات و التّشريعات الدّاخلية نصّت على هذا الإلتزام المزدوج الملقى على عاتق مزود الخدمات، بحيث يقع لزاماً عليه "حفظ البيانات" و "ضمان سلامتها"، أنظر مثلاً المادّة 16 فقرة 02 من إتفاقية بودابست، المادّة 23 فقرة 02 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات و المادّة 31 فقرة (2-د) من إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإجراء و حماية البيانات ذات الطّابع الشّخصي و المادّة 23 من مشروع إتفاقية الأمم المتحدة للتعاون في مكافحة الجريمة الإجراء.

و السؤال المثار بشأن موقف المشرع الجزائري في الحقيقة لا يعنق من المقاربة الفلسفية التي تشكل محور الدراسة، فيما إذا كان المشرع بموقفه هذا قد حقق التوازن بين الفعالية و الشرعية في الوصول إلى الحقيقة؟

قدمنا أن "الإلتزام بالإحتفاظ الشامل لبيانات حركة السير" يفرض على مقدم الخدمة حفظ بيانات الحركة لفترة معينة من الوقت قد تستغرق مدة إبقاء السجلات لمدة تصل إلى 24 شهرا في النهج المقارنة، و يمكن لسلطات التحقيق النفاذ إلى البيانات اللازمة لتحديد الجاني حتى بعد ارتكابها بشهور عديدة، و من منظور مقدم الخدمات يعتبر "إجراء التجميد السريع للبيانات" أقل تقييدا من "الإلتزام بالحفظ الشامل للبيانات"، حيث لا يحتاج مقدمو الخدمات إلى تخزين جميع البيانات الخاصة بكافة المشتركين، و لكن عليهم بدلا من ذلك كفالة عدم حذف بيانات محدّدة بمجرد استلام "أمر بالحفظ العاجل للبيانات المخزّنة".

و يتيح "الأمر بالحفظ العاجل للبيانات" مزايا عديدة طالما أنه ليس من الضروري حفظ البيانات المتجمّعة لملايين المستخدمين و لكن يكفي فقط حفظ البيانات المتصلة بالأشخاص المحتملين للاشتباه في التّحقيقات الجنائية، و مع ذلك فمن المهم أن يشار إلى أن "الإحتفاظ الشامل بالبيانات" يتيح مزايا في الحالات التي يتم فيها حذف البيانات بعد ارتكاب الجريمة مباشرة، ففي هذه الحالات لا يمكن للأمر بالحفظ العاجل للبيانات - "الإلتزام بالحفظ الشامل للبيانات" أن يمنع حذف البيانات ذات الصلة⁽¹⁾.

في الحقيقة يحتدم الصّراع بين التّأنيّة "الفعالية" و "الشرعية" بخصوص هذه الوسيلة بشكل كبير جدا، فموقف المشرع الجزائري يميل إلى ترجيح اعتبارات الفعالية، لأنّ إجراء الأمر بالحفظ العاجل للبيانات لا يتيح المحافظة عليها طالما أنّ مزودي الخدمات يفضلون إزالتها بمجرد استكمال الخدمة، و ذلك لسبب إقتصادي بحت تجنبا من تحمل أعباء الحفظ و التخزين بالنظر إلى حجمها الذي يفوق قدرة العقل البشري على التّصور، بينما تمثّل المادّة 11 من قانون 04/04 إهدارا كلياً لمبدأ الشرعية لأنّه ورد مناقضا لمبدأ التناسب و الضّرورة بحيث يشترط الإحتفاظ بعدد كبير من فئات بيانات الإتصال و لكل مشترك بدون استثناء حتّى و لو لم يكن موضع إتهام، بل يطال أيضا كافة البيانات حتّى و لو كانت تتمتع بامتياز السرية المهنية.

(1) ماركو جيروي، المرجع السابق، ص 285.

و ما يؤكد هذه النتيجة التي توصلنا إليها ليس فقط تركيز كافة الإتفاقيات الدولية على الأمر بحفظ البيانات بدل الإلتزام الشامل بحفظ البيانات، بل توجه مختلف المحاكم الدستورية الأوروبية إلى تقرير عدم دستورية هذا الإجراء⁽¹⁾، و تأكّد ذلك أيضا بقرار محكمة العدل الأوروبية الصادر بتاريخ 08 أفريل 2014 القاضي ببطلان "التوجيه الأوروبي الصادر بتاريخ 15 مارس 2006 Directive 2006/24/CE المتعلّق بإلزام مزودي الخدمات بالإحتفاظ بالبيانات التي تمّ إنشاؤها أو معالجتها بمناسبة توفير خدمات الإتصالات الإلكترونية المتاحة للجمهور" لأنّه في نظر المحكمة يفضي إلى تدخل واسع النطاق في الحياة الخاصة للأفراد و حماية البيانات الشخصية، دون أن يقتصر ذلك التّدخل على ما هو ضروري قطعاً و جاء في الفقرتين 85، 59 من هذا الحكم:

(¹) لقد اعتبر أنّ التّوجيه الأوروبي لحفظ البيانات "الأداة الأكثر تعديا على الخصوصية في تاريخ الإتحاد الأوروبي" بل انتهاك غير مسبوق للحقوق الأساسية" لذا كانت المحاكم الداخلية لدول الإتحاد الأوروبي سباقة إلى إعلان عدم دستورية هذا التّوجيه، حيث أنّه خلال أكتوبر 2009 ألغت المحكمة الدستورية الرومانية التّوجيه 24 لسنة 2006 لأنّه يخالف المادة 8 من الإتفاقية الأوروبية لحقوق الإنسان و أشارت المحكمة من بين أمور أخرى إلى "الطّبيعة السّمولية لمطلب الإحتفاظ بالبيانات لأنّه ينطبق على الجميع سواء كانوا قد ارتكبوا جرما بالفعل أو يشتبه ارتكابهم هذا الجرم، و قالت المحكمة أنّ نطاق التّوجيه يكتفه الغموض و أنّ القواعد تفتقر إلى الضّمانات الكافية ضد سوء الاستخدام".

و خلال سنة 2010 حذت المحكمة الدستورية الإتحادية الألمانية حذو سابقتها أين قرّرت بأنّ الأحكام التنفيذية الألمانية تنتهك للحق في سرية الاتصالات المنصوص عليها في الدستور و أشارت إلى أنّ "هذه القواعد من شأنها أن تشعر الأفراد بتعرضهم الدائم للمراقبة الأمر الذي يفسد عليهم التمتع بالحقوق الأساسية المختلفة، أمّا الإحتفاظ بالبيانات في حدود معيّنة بغرض حماية المصالح الأمنية الهامة قد يكون له ما يبرره و لكن القواعد الحالية كانت مبالغ فيها جدا".

و أكدت المحكمة الدستورية التشيكية أيضا في مارس 2011 أنّه نظرا لكثافة و اتساع نطاق التّدخل في الخصوصية لا يمكن تبرير القواعد على أنّها قيد لازم على الحق في الخصوصية و أشارت في هذا الصّد إلى أنّ الإحتفاظ بالبيانات التي تشترطها القواعد لم تؤثر كثيرا على إحصائيات الجريمة و خصوصا في ظل الإمكانيات التكنولوجية الجديدة التي تساعد على تجنب الكشف على الهوية" و أضافت المحكمة إلى أنّ الأغراض التي تبرّر الإحتفاظ بالبيانات هي أغراض واسعة جدا و لا توجد ضمانات كافية".

لمزيد من التّفصيل بخصوص الأحكام الصّادرة عن المحاكم الدستورية لدول الإتحاد الأوروبي راجع: توبي مندل، أندرو بوديفات، وين واجندر، ديسكي هوتن، نتاليا توريس، دراسة استقصائية عالمية حول خصوصية الأنترنيت و حرية التّعبير، منظمة الأمم المتحدة للتربية و العلم و الثقافة (اليونسكو)، فرنسا، 2012، ص ص 71-73.

"من ناحية، ينطبق التوجيه 24/2006 بطريقة شاملة على جميع الأشخاص الذين يستخدمون خدمات الإتصالات الإلكترونية، و لكن الأشخاص الذين يتم تخزين بياناتهم ليسوا حتى بشكل غير مباشر في موقف يرحح أن يكونوا عرضة للمتابعة الجنائية، وهذا ينطبق حتى على الأشخاص الذين لا توجد أدلة تشير إلى أن سلوكهم قد يكون له صلة و لو بطريقة غير مباشرة بجرائم خطيرة. علاوة على ذلك، لا يقدم هذا التوجيه أي استثناء، بحيث ينطبق حتى على الأشخاص الذين تخضع مراسلاتهم بموجب قواعد القانون الوطني للسرية المهنية.

و من ناحية أخرى، رغم أن الغاية المرجوة من التوجيه المساهمة في مكافحة الجريمة الخطيرة، فإن التوجيه لا يتطلب قيام علاقة بين البيانات التي يقصد الاحتفاظ بها وتهديدها للسلامة العامة، و لا يقتصر على الاحتفاظ بالبيانات المتعلقة بفترة زمنية محددة أو منطقة جغرافية أو دائرة من الأشخاص الذين يحتمل أن يكونوا متورطين بأي شكل من الأشكال في انتهاك خطير أو لغيرها من الدواعي، لمنع الجرائم الخطيرة و كشفها أو متابعة مرتكبيها"⁽¹⁾.

و قد أوصت منظمة الحقوق الرقمية الأوروبية الاستغناء على "الإلتزام بالاحتفاظ الشامل بالبيانات"، و اعتماد إجراء الأمر بالحفظ العاجل للبيانات المخزنة، و جمع البيانات المستهدفة التي تساعد في تحقيقات محددة وفقا لما تم الإتفاق عليه دوليا في الإتفاقية

(¹) Cour européenne de justice, arrêt de la Cour dans les affaires jointes C-293 / 12 et C-594 / 12, Digital Rights Ireland et Seitlinger et autres, arrêt du 8 avril 2014, par. 58 et 59, «

58 En effet, d'une part, la directive 2006/24 concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves. En outre, elle ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel.

59 D'autre part, tout en visant à contribuer à la lutte contre la criminalité grave, ladite directive ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves. ».

الأوروبية لمكافحة جرائم المعلوماتية، إلا أنّ المشرّع الأوروبي اكتفى بإدخال تعديلات على إطار الإحتفاظ الشّامل بالبيانات بدلا من إلغائه باعتباره أداة قيّمة لنظم العدالة الجنائية.

و في هذا السّياق نحن نرى أنّه ينبغي على المشرّع الجزائري إحاطة هذا الإجراء ببعض الضّمّانات و أهمها وجوب خفض مدة استبقاء البيانات لدى مزوّد الخدمة التي حدّدها بمدة سنة كاملة، و قصر نطاقها إلى ما لا يجاوز 180 يوما من تاريخ التّسجيل أسوة بالمشرّع المصري هذا من جهة⁽¹⁾، و من جهة أخرى تشديد العقوبة الجزائية على مزودي الخدمات في حالة مواصلة الإحتفاظ بهذه البيانات بعد إنقضاء الأجل المقرّر قانونا للإحتفاظ بها بدل الاكتفاء بعقوبة الغرامة⁽²⁾. و من البديهي أنّه و في ظل هذه التّوصيات المقدمة إلى المشرّع الجزائري بخفض مدة الإحتفاظ بالبيانات، يتعيّن عليه أيضا اعتماد آلية "الأمر بالحفظ العاجل لبيانات حركة السّير" أسوة بالتشريعات المقارنة، نظرا لما تحقّقه من فاعلية في المحافظة على الدّليل المعلوماتي و تمكين سلطات التّحقيق من استرداده قبل حذفه، و هذه التّوصية تقودنا إلى التّطرق إلى ضمانات التي يجب أن تحاط بهذا الإجراء الجزائي عند اعتماده.

الفرع الثالث: قيود الأمر بالحفظ العاجل للبيانات المعلوماتية المخزّنة

تفرض موجبات الشّرعية الإجرائية إحاطة هذا الإجراء الجزائي بعدد من القيود تكفل رسم حدودا موضوعية له، فلا يكون شاملا إلتزاما لمبدأ التّناسب (أولا)، و حدودا زمنية فلا تستغرق مدته فترة تناقض الحق في الدّخول في طي النّسيان (ثانيا)، و أن يخضع دائما لرقابة القضاء و إشرافه (ثالثا).

أولا: القيود الموضوعية للأمر بالحفظ

أشارت المذكرة التفسيرية لإتفاقية بودابست إلى أنّ سلطة "أن يأمر أو يحصل بطريقة أخرى على الحفظ السّريع للبيانات الإلكترونية" تنطبق على كل نوع من أنواع البيانات المعلوماتية المخزّنة، و بالتّالي يمكن أن تشمل على أي نوع من البيانات المحدّدة في الأمر بالحفظ، مثال ذلك مستندات تجارية أو طبية أو شخصية، فالأطراف يجب أن يؤسّسوا هذه الإجراءات من أجل تطبيقها بالأخص عندما تكون ثمة أسباب تدعو للاعتقاد بأنّ البيانات

(1) المادة 02 من القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.

(2) انظر المادة 65 فقرة 02 من القانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الصّادر بالجريدة الرّسمية عدد 34 .

قابلة على وجه الخصوص للفقد أو التعديل، و يمكن أن يشمل ذلك أيضا على سبيل المثال البيانات التي لا يتم الاحتفاظ بها إلا لفترة وجيزة، و كما هو الحال عند تبني سياسة محو البيانات بعد فترة معينة أو أنّ البيانات يتم محوها منهجيا عندما يكون وسيط التخزين مطلوبا من أجل تسجيل بيانات أخرى⁽¹⁾.

كما أشارت الفقرة 1 من المادة 16 صراحة إلى "البيانات المتعلقة بالمرور" بغرض الإشارة إلى الإنطباق الخاص لهذه النصوص على هذا النوع من البيانات، عندما يتم تجميعها و الاحتفاظ بها عن طريق مقدّم الخدمة فإنّه لا تكون بصفة خاصة محتفظ بها إلا لفترة وجيزة يضاف إلى ذلك إنّ الإشارة إلى البيانات المتعلقة بالمرور يقيم أو ينشئ علاقة بين الإجراءات المشار إليها في المادتين 16، 17.

غير أننا نرى أنّ التفسير الوارد بالمذكرة الإيضاحية لإتفاقية بودابست لا معنى له و فاقد لقيمته، لأنّ عبارات نص المادة 16 واضحة و لا تحتاج إلى تفسير بخصوص نطاق الأمر بالحفظ، بحيث ورد النصّ عاما و شاملا لجميع البيانات بدون استثناء (بيانات المرور، بيانات المحتوى، بيانات المشترك)، و إن جاء التركيز على بيانات المرور فإنّ المذكرة التفسيرية أرجعت ذلك إلى سرعة زوال هذا النوع من البيانات و أيضا لقيمتها في نسبة الجريمة إلى مقترفها، و من ثم لا يترتب البطلان إذا ما جاء أمر الحفظ شاملا، و الشمول في أمر الحفظ لم تستثنه أيّ إتفاقية دولية⁽²⁾ أو تشريع داخلي⁽¹⁾.

(1) Conseil de l'Europe, Rapport explicatif de la Convention du Conseil de l'Europe sur la cybercriminalité, op cit, Clause n° 29.

(2) و يلاحظ في هذا الشأن أنّ مشروع إتفاقية الأمم المتحدة للتعاون في مكافحة الجريمة الإلكترونية هو الآخر لم يرسم حدودا لنطاق الأمر بحفظ البيانات المعلوماتية المخزنة حيث تنص المادة 23 منه "التعجيل في حفظ البيانات الحاسوبية المخزنة:

1- تتخذ كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من إصدار الأوامر أو التعليمات المناسبة أو على نحو مماثل كفالة التعجيل في حفظ بيانات حاسوبية محدّدة تشمل بيانات المعلومات، وعلى الأخص حيثما وجدت أسباب تدعو للاعتقاد بأنّ هذه البيانات معرضة تحديداً للحذف أو التسخن أو التعديل.

2 - في حال تنفيذ الدولة الطرف أحكام الفقرة 1 من هذه المادة بموجب أمر صادر لشخص ما بحفظ بيانات محددة مخزونة بحوزة هذا الشخص أو موجودة تحت سيطرته، تتخذ الدولة الطرف تدابير تشريعية و غيرها من التدابير القانونية اللازمة لإجبار ذلك الشخص على حفظ تلك البيانات و صون سلامتها للمدة الزمنية اللازمة، على أن يكون

غير أنّ صفة التّوسّع التي ينطوي عليها أمر الحفظ، يقتصر مدلولها على جميع البيانات حسب التّقسيم المتعارف عليه (بيانات المرور، بيانات المحتوى، بيانات المشتركين) من حيث النوع، دون أن تفيد معنى الشّمول العام، بحيث يقع باطلاً كل أمر بالحفظ العاجل للبيانات المخزنة لا يراعي مبدأ التّناسب و الضّرورة، فلصّحته وجب أن يكون الأمر بالحفظ مقيداً من حيث موضوعه ببيانات محدّدة بغض النّظر عن نوعها، و أن تكون مرتبطة بالقضية التي يجري التّحقيق فيها، و أن يراعي قدر الإمكان تحديد تاريخ تولدها بحصرها في النّطاق الزّمني لوقوع الجريمة دون أن يمتدّ إلى تاريخ سابق عن حدوثها، تحقيقاً لمبدأ التّناسب بين حق الدّولة في إتخاذ هذا التّدبير و بين مصلحة الفرد في حماية حقه في الخصوصية.

فهذا الإجراء لا يتعلّق سوى بالبيانات المعلوماتية الموجودة قبل صدور أمر الحفظ أو كانت في طور التّخزين عند إصدار الأمر بالحفظ العاجل، لذا فإنّه من الأهمية بمكان إقامة تفرقة بين مصطلحي "حفظ البيانات" و "الاحتفاظ و أرشفة البيانات"، فرغم أن للكلمتين معنيين متجاورين في اللّغة الشّائعة لكن لهما معنى مختلف في لغة المعلوماتية. إذ أن عبارة "حفظ البيانات" تعني حفظ بيانات سبق وجودها في شكل مخزّن و حمايتها من كل شيء يمكن أن يؤدي إلى إتلافها أو تجريدها من صفتها الرّاهنة، في حين فإنّ عبارة "الاحتفاظ بالبيانات" تعني حفظ بيانات لدى حائزها بالنّسبة لمستقبل البيانات في طور الإنتاج و التّوالد فأرشفة البيانات يشير إلى تجميع البيانات في الوقت الحاضر و حفظها أو حيازتها في أرشيف أي وضعها في ترتيب معيّن و الإحتفاظ بها في المستقبل و معنى ذلك أنّ "أرشفة البيانات" عبارة عن عملية تخزين للبيانات على عكس "حفظ البيانات" الذي يعني النّشاط الذي يضمن للبيانات سلامتها و سرّيتها⁽²⁾.

ذلك لمدة أقصاها 180 يوماً، لتمكين السّطات المختصّة من السّعي إلى الكشف عن تلك البيانات. و يجوز للدّولة الطرف أن تنص على إمكانية تجديد ذلك الأمر في وقت لاحق.

3 - تتخذ كل دولة طرف ما قد يلزم من تدابير تشريعية و غيرها من التّدابير لإجبار الشّخص المكلف بحفظ البيانات على الحفاظ على سرية ما ينفذ من هذه الإجراءات خلال المدة الزّمنية المنصوص عليها في تشريعاتها المحلية...."

(1) أنظر مثلاً المادة 60 من قانون الإجراءات الجزائية الفرنسي، المادة (39) المعدّلة بمقتضى قانون 25 ديسمبر 2016 المعدّل لقانون التّحقيق الجنائي البلجيكي Code d'instruction Criminelle.

(2) هلاي عبد الله أحمد، المواجهة الجنائية لجرائم المعلوماتية في النّظامين المصري و البحريني على ضوء اتفاقية بودابست، المرجع السّابق، ص 182.

و هذا الضمان الإجرائي نصّت عليه ديباجة التّوجيه الأوروبي رقم 93 لسنة 2011 مؤكدة بأنّ هذه الوسيلة الإجرائية لا تسمح بالإحتفاظ سوى بالبيانات المخزّنة بالفعل لدى مزوّد الخدمة وقت إستلام الأمر، و لا يجوز الوصول إلى بيانات توالدت بتاريخ لاحق لتبليغ الأمر إلى مزوّد الخدمة، و نعتقد أنّ هذا الضّابط الإجرائي يعتبر بمثابة حد فاصل بين التّفتيش و المراقبة، ففي حالة ما إذا تضمّن الأمر بالحفظ واجب جمع أو تسجيل المعلومات المرسلّة بواسطة تكنولوجيا المعلومات والاتصالات في الوقت الحاضر أو بالنّسبة للبيانات المتوالدة مستقبلا، فإنّ هذا الإلتزام يجعل الإجراء بمثابة اعتراض للمراسلات، و يخرج من دائرة التّفتيش، و هو ما يترتّب عليه البطلان نظرا لاختلاف الضّوابط الإجرائية بين التّفتيش و المراقبة بشكل كبير جدا و جاز في هذه الحالة لمزوّد الخدمة الإمتناع عن الإنصياع للأمر لعدم مشروعيته عن طريق منحه الحق في الإعتراض أمام القضاء.

و يوجد أيضا ضابط إجرائي آخر لم تشر إليه الاتفاقيات الدّولية المار بيانها، و قد إستدرکه المشرّع الأوروبي ضمن مقترح التّوجيه المتعلّق بأوامر تقديم و حفظ الأدلّة الجنائية الإلكترونيّة بين دول الإتحاد الأوروبي، و يتعلّق بنوع الجريمة موضوع التّحقيق، بحيث يكون التّوسّع و الضّيق في نطاق الأمر بالحفظ مقيد أيضا بطبيعة الجريمة من حيث درجة خطورتها، باعتبار أنّ بيانات المشتركين و بيانات النّفاذ أقلّ خطورة على الحق في الخصوصية إذا ما قورنت ببيانات المحتوى، فإنّ الفئة الأولى من البيانات قد يستغرق الأمر بالحفظ بمناسبة التّحقيق في شتى الجرائم بينما يخضع الأمر بحفظ الفئة الثّانية (بيانات المحتوى) لقيود أشدّ صرامة⁽¹⁾.

فلا يجوز أن يصدر أمر بحفظ البيانات المتعلّقة بالمحتوى إلّا إذا كان بقصد جمع دليل معلوماتي لإثبات جريمة لا تقل عقوبتها عن ثلاثة سنوات أو كانت تمثّل جريمة من جرائم الإحتيال و التزوير المرتكبة بشكل كلي أو جزئي بوساطة نظم المعلومات⁽²⁾، و جرائم

(¹) Commission européenne, Proposition de règlement du parlement européen et du conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, 2018/0108(COD), Strasbourg, 17 avril 2018 (EXPOSÉ DES MOTIFS clause n 31.)

contrefaçon des moyens de paiement autres que les espèces (JO L 149 du 2.6.2001, p. 1).

الإستغلال الجنسي للقصر⁽¹⁾، و الجرائم الإرهابية⁽²⁾، و ذلك منعا من اللجوء المفرط لهذه الوسيلة القسرية، إذ يُستبعد من نطاق التطبيق عدداً كبيراً من الجرائم التي تعتبرها الدول الأعضاء أقل خطورة.

و مع ذلك فإنّ البرلمان الأوروبي لم يستبعد إمكانية اللجوء إلى هذه الوسيلة الإجرائية متى كانت العقوبة المقررة للجريمة تقلّ عن ثلاثة سنوات و لكن يمكن أن تسبّب ضرراً خطيراً ، لاسيما في الحالات التي يكون فيها الضرر الفردي منخفضاً و لكنه يمتدّ إلى عدد كبير من الضحايا بشرط عدم إمكانية إثباتها سوى من خلال الدليل المعلوماتي⁽³⁾.

و من الضمانات الهامة التي أغفلت التشريعات النص عليها، و هي عدم جواز إصدار أمر بالحفظ و لو إنصبّ على بيانات المرور فقط، إلاّ بشأن التحقيق في الجرائم التي ارتكبت بالفعل سواء كان مرتكب الجريمة معروفاً أو مجهولاً لدى سلطة التحقيق، و معنى ذلك أنّه يقع باطلاً كل أمر يرمي إلى حفظ البيانات بقصد التحقيق في أفعال تحضيرية و من جهة أخرى فإنّ هذه البيانات تكون محفوظة لدى مزود الخدمة بقوة القانون طبقاً للإلتزام بالحفظ الشامل للبيانات، و هنا وجب التنويه إلى مسألة غاية في الأهمية تقيم فارقاً بليغاً بين الأمر بالحفظ العاجل للبيانات و بين الإلتزام بحفظ البيانات، فالتشريع الجزائري أسقط بيانات المحتوى من نطاق الإلتزام بالحفظ و هدفه هو المحافظة على الحريات الفردية، إلاّ أنّ هذا النوع من الأدلة غالباً ما يشكّل دليلاً كاملاً ينصبّ مباشرة على الواقعة موضوع الإثبات⁽⁴⁾.

(¹) Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO L 335 du 17.12.2011, p. 1).

(²) Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

(³) Voir l'Article 5 de la Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale COM/2018/225 final - 2018/0108 (COD) .

(⁴) لا تستثني الكثير من التشريعات فئة بيانات المحتوى من إلتزام الحفظ الواقع على عاتق مزود الخدمات رغم خطورتها على الحريات الفردية كالتشريع المصري (المادة 6 من القانون رقم 175 لسنة 2018) و التشريع السوري (3 ، 8 من المرسوم التشريعي السدوري رقم 17 لسنة 2012).

و لا مرأى أنّ إدخال هذه الفئة من البيانات ضمن الإلتزام باستبقاء البيانات يشكّل إهدارا صارخا للتشريعية الإجرائية و كشافا صارخا لستار السرية بشكل غير ضروري و هو موقف جميع التشريعات المقارنة لاسيما التشريعات الأوروبية⁽¹⁾، و لا سبيل للخروج من هذا المأزق سوى بتبني الأمر بالحفظ العاجل لبيانات المحتوى لأنّه يستهدف فردا محددا قامت في حقه مجموعة من القرّائن التي ترجح ضلوعه في ارتكاب الجريمة موضوع التحقيق و مع حصره ضمن نطاق زمني مرتبط بالواقعة الإجرامية لأنّ الموقف التشريعي الحالي يهدر الفعالية و الشرعية معا.

ثانيا: القيود الزمنية للأمر بالحفظ العاجل للبيانات

لا ريب أنّ الأمر بالحفظ العاجل للبيانات الحاسوبية يمثّل وسيلة قسرية تتطوي على مساس بالحق في الخصوصية، إذ أنّ واقعة تواصل و استمرار حفظ البيانات و تخزينها تشكّل تعارضا مع حق الفرد في الدّخول في طي النّسيان *Le droit à l'oubli numérique*، و يعني ذلك أنّ المشكلة تتمثل في القدرة على الإحتفاظ بالبيانات الشخصية لدى طرف آخر لمدة زمنية قد تطول و هو ما يهدّد الأفراد مستقبلا بظهور بياناتهم⁽²⁾.

لهذا السّبب نجد أنّ إتفاقية بودابست قد حرصت على أهمية تحديد المدّة القصوى لنطاق الأمر بحفظ البيانات المعلوماتية المخزّنة تحقيقا لمبدأ التّناسب و الضّرورة، بحيث لا يجوز أن يجبر مزوّد الخدمة بحفظ و سلامة هذه البيانات لمدة تفوق 90 يوما، و قد اعتبرت أنّ هذه المدّة الزمنية كافية للسّماح للسلطات المختصة لاتخاذ إجراءات قانونية أخرى

(¹) Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, le paragraphe 13 dispose que « La présente directive ne porte que sur les données générées ou traitées par suite d'une communication ou d'un service de communication et non sur le contenu proprement dit des informations communiquées. Les données devraient être conservées de manière à éviter qu'elles ne soient conservées plus d'une fois. Les données générées ou traitées, lors de la fourniture des services de communications concernés, concernent uniquement les données qui sont accessibles. En particulier, s'agissant de la conservation des données concernant le courrier électronique par l'internet et la téléphonie par l'internet, l'obligation de conserver les données peut ne s'appliquer qu'à l'égard des données émanant des propres services des opérateurs ou des fournisseurs de réseau. »

(²) معاذ سليمان الملا، فكرة الحق في الدّخول في طي النّسيان الرّقمي في التشريعات الجزائية الإجرائية الحديثة دراسة مقارنة بين التشريع العقابي الفرنسي و التشريع الجزائري الكويتي مجلة كلية الحقوق الكويتية العالمية، الكويت، العدد 3، الجزء 1، 2018، ص 118.

كالنّقتيش و الضّبط و الولوج إلى البيانات أو الحصول بطريقة مشابهة أو إرسال أمر بالإنتاج (التّقديم و التّسليم) بغرض الكشف على هذه البيانات و الإفصاح عنها إلاّ أنّها أجازت تجديد الأمر بالحفظ⁽¹⁾.

و نفس الإطار الزّمني تبنته الإتفاقية العربية لمكافحة جرائم تقنية المعلومات⁽²⁾، أمّا مشروع اتفاقية الأمم المتحدة للتّعاون في مكافحة الجريمة الإلكترونية فإنّه أجاز إجبار مزوّد الخدمة بحفظ البيانات و صون سلامتها لمدة زمنية أقصاها 180 يوما، لتمكين السّطات المختصة من السّعي إلى الكشف عن تلك البيانات مع إمكانية تجديد الأمر لاحقا⁽³⁾، في حين نجد أن إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني و حماية البيانات ذات الطّابع الشّخصي قد مددت هذا النّطاق الزّمني بشكل مبالغ فيه يصل إلى سنتين كاملتين⁽⁴⁾، و هو ما يناقض الغاية من حفظها، في وقت يحدث هذا التّوجه الأخير للمشرّع الإفريقي تناقضا في الإلتزامات الدّولية المفروضة بموجب الإتفاقيات المساقاة آنفا حين مصادقة الدّولة على هذه الإتفاقيات معا.

بالعودة إلى التّشريع المقارن نجد أنّ المشرّع الفرنسي ساوى بين مدة الإلتزام العام الملقى على عاتق مزودي الخدمات في إطار الإحتفاظ الشّامل للبيانات حركة السّير بموجب المادّة 34 من قانون البريد الإتصالات الإلكترونية و المادّة 01 من المرسوم 2006/358 المتعلّق

(1) Conseil de l'Europe, Rapport explicatif de la Convention du Conseil de l'Europe sur la cybercriminalité . Clause n° 29.

(2) المادة 23 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

(3) المادة 23 مشروع إتفاقية الأمم المتحدة للتّعاون في مكافحة الجريمة الإجرائية.

(4) نصّت المادة 31 فقرة (2-د) من اتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإجرائي و حماية البيانات ذات الطّابع الشّخصي "تلتزم الدّول الأطراف بوضع التّدابير التّشريعية اللاّزمة لضمان أنّه، و إذا كانت ضرورة المعلومات تملي ذلك، و على وجه الخصوص إذا كانت هنا أسباب تدعو للإعتقاد بأنّ المعلومات المخزّنة في نظام الكمبيوتر هي عرضة بشكل خاصّ للفقدان أو التّعديل، فإنّ لقاضي التّحقيق أن يصدر أمرا قضائيا لأيّ شخص بصون و حماية سلامة البيانات التي في حوزته أو تحت سيطرته لمدة لا تزيد عن عامين، و ذلك لضمان حسن سير التّحقيق. و أيّ شخص يؤتمن على هذه البيانات أو أي شخص آخر مسؤول عن الحفظ على هذه المعلومات عليه الحفاظ على سرية البيانات".

بحفظ معطيات الإتصالات الإلكترونية⁽¹⁾، مع مدة الأمر بالحفظ في سياق التّحقيق إذ نصّت المادة 60 ق إ ج على جواز المطالبة بحفظ البيانات لمدة سنة، دون أن ينص على جواز تجديدها⁽²⁾.

أما التّشريعات العربية كالتّشريع القطري⁽³⁾، و البحريني⁽⁴⁾، فقد حافظا على المدة التي حددها الإتفاقية العربية و المقدر بـ 90 يوماً كحد أقصى مع جعلها قابلة للتّجديد بموجب أمر مسبّب قبل ثلاثة أيام من إنقضاء المدة الأولى، أما التّشريع المصري فقد قلّص المدة بشكل كبير جداً بحيث لا يجوز أن تتجاوز 30 يوماً و هذه المدة غير قابلة للتّجديد سوى مرة واحدة⁽⁵⁾، أما قانون الكامولت التّمودجي المتعلّق بالجرائم الحاسوبية و الجرائم المتصلة

(1) Article 1 du Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques JORF n°73 du 26 mars 2006.

(2) Article 60-2 du code de procédure pénale stipule que " Sur demande de l'officier de police judiciaire, ou sous le contrôle de ce dernier, de l'agent de police judiciaire, intervenant par voie télématique ou informatique, les organismes publics ou les personnes morales de droit privé, à l'exception de ceux visés au d du 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 précité et au 2° de l'article 80 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent.

L'officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés au 1 du I de l'article 6 de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, de prendre, **sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs...**».

(3) المادة 21 من القانون القطري رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإجرائية الصّادر بالجريدة الرّسمية عدد 15 بتاريخ 20/10/2014.

(4) المادة 12 من القانون قانون البحريني رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات الصّادر بالجريدة الرسمية رقم 3178 المؤرخة في 09 أكتوبر 2014.

(5) تنص المادة رقم (06) من التّشريع المصري السّالف ذكره "الأوامر القضائية المؤقتة".

لجهة التّحقيق المختصّة - بحسب الأحوال - أن تصدر أمراً مسبباً، لمأموري الضّبط القضائي المختصين، لمدة لا تزيد على 30 يوماً قابلة للتّجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر مما يلي:

بالحاسوب فقد قلّص المدة إلى 7 أيام فقط قابلة للتجديد بموجب المادة 15 منه⁽¹⁾، و هو ما يحسب لهذا التشريع في محاولة منه لترجيح اعتبارات الشرعية قدر الإمكان و حفظ الحق في الدخول في طي النسيان.

أما مقترح البرلمان الأوروبي المتعلق بأوامر إنتاج و حفظ الأدلة الجنائية الإلكترونية بين دول الإتحاد الأوروبي، فقد أشارت دباخته إلى تقليص النطاق الزمني للأمر بالحفظ إلى مدة أقصاها 60 يوما ما لم يبلغ مزود الخدمة بالأمر بالتسليم، فإن لم يتلق مزود الخدمة خطوات رسمية أخرى يتحم على هذا الأخير حذف البيانات بعد فوات أجل 60 يوما من تاريخ تبليغه الأمر بالحفظ⁽²⁾، و هو ما ينطبق على الفترة الزمنية التي حددتها إتفاقية بودابست بموجب المادة 29 و الإتفاقية العربية لمكافحة جرائم تقنية المعلومات بمقتضى المادة 37 بخصوص الأمر بالحفظ الدولي.

ثالثا: الإشراف القضائي على إجراء الأمر بالحفظ العاجل للبيانات و تسليمها

لا قيمة للشرعية بنوعيتها (الدستورية و القانونية) ما لم يتوافر الضمان القضائي الذي يكفل حماية الحقوق و الحريات من خطر المساس بها عند إتخاذ الأمر بإجراء حفظ البيانات المعلوماتية المخزنة، فإذا كانت الضمانات التي توفرها قاعدة مشروعية الدليل الجنائي للمتهمين تقتضي معاملتهم بوصفهم أبرياء حتى يصدر حكم بات بإدانتهم من ناحية، و تتطلب أن يكون القانون هو الأداة التي تنظم استعمال الحرية من ناحية أخرى، فإن هذه

1- ضبط أو سحب أو جمع أو التّحفظ على البيانات والمعلومات أو أنظمة المعلومات، و تتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه، و يتم تسليم أدلتها الزمنية للجهة مصدرة الأمر على ألا يؤثر ذلك على إستمرارية النّظم و تقديم الخدمة إن كان لها مقتضى.

2- البحث و التفتيش و الدخول و النّفاذ إلى برامج الحاسب و قواعد البيانات و غيرها من الأجهزة و النظم المعلوماتية تحقيقا لغرض الضبط.

3- أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني، موجودة تحت سيطرته أو مخزنة لديه، و كذا بيانات مستخدمي خدمته و حركة الاتصالات التي تمت على ذلك النّظام أو الجهاز التقني، و في كل الأحوال يجب أن يكون أمر جهة التّحقيق المختصة مسببا.."

(1) ماركو جيري، المرجع السابق، ص 287.

(2) Article 10 de la proposition de règlement (la Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale COM/2018/225 final - 2018/0108 (COD) .

الضمانات تكون عديمة الأثر ما لم تكن هناك سلطة قوية تكفل مراعاتها و تضمن بذاتها احترام الحرية الشخصية و ترد الاعتداء الواقع عليها⁽¹⁾.

و كون الأمر بالحفظ من مقدمات إجراء الضبط الرقمي، فهو بذلك يعتبر عملا من أعمال التحقيق و معنى ذلك أنه عمل قضائي لأن التحقيق وظيفة قضائية، فالصفة القضائية في من يأمر أو يأذن بالأمر بالحفظ ضمنا هاما باعتباره إجراء يقيد الحق في الخصوصية المعلوماتية. و هذا المبدأ المعبر عنه بأن "القضاء هو الحارس الطبيعي للحرّيات"⁽²⁾ يتمتع بالطابع الدستوري، و في هذا الصدد تنص المادة 46 من الدستور الجزائري "لا يجوز انتهاك حرمة حياة المواطن الخاصة، و حرمة شرفه، و يحميها القانون... لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلّل من السلطة القضائية...".

الحقيقة أن هذا الضمان الدستوري يثير تساؤلا بالغ الأهمية يتعلّق مضمونه بالمقصود "بالسلطة القضائية"؟ هل سلطة إصدار الأمر بحفظ البيانات الحاسوبية المخزنة و إنتاجها يقتصر على سلطة التحقيق أم يمتدّ أيضا إلى سلطة الإتهام؟

لم تجب كل من إتفاقية بودابست و الإتفاقية العربية لمكافحة جرائم تقنية المعلوماتية على هذا التساؤل، بيد أنّ إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني و حماية البيانات ذات الطابع الشخصي جعلت سلطة إتخاذ هذا الإجراء من إختصاص سلطة التحقيق على وجه التّحديد بموجب نص صريح قاطع الدلالة (المادة 31 فقرة 3 بند ج).

(1) عادل عبد البديع آدم حسين، قاعدة مشروعية الدليل الجنائي، رسالة دكتوراه، جامعة القاهرة، مصر، 2014، ص 154.

(2) ترجع جذور هذا المبدأ في النظام اللاتيني للقانون الفرنسي القديم، الذي كان يقرّ مبدأ الإختصاص القضائي في مسائل المساس بالحق في الملكية الخاصة، بوصفه حقا طبيعيا مقدسا، فقد روي أنّ القاضي الذي حمى الحقوق المالية يمكنه أيضا أن يحمي غيرها من الحقوق الفردية الأساسية التي يحميها إعلان الثورة الفرنسية لحقوق الإنسان 1789، و من هنا تقرّر في ذلك الوقت مبدأ "أنّ السلطة القضائية تحمي الحرية الفردية" و قد جاء الدستور الفرنسي الصادر سنة 1958 فأكد هذا المبدأ في المادة (66) منه، التي نصّت على أنّ "السلطة القضائية تحرس الحرية الفردية" كما عبّر الدستور الحالي على هذا المبدأ إذ نصّ في المادة (94) منه على أنّ إستقلال القضاء و حصانته و حيده ضمانات أساسية لحماية الحقوق و الحرّيات ". مشار إليه لدى: عادل عبد البديع آدم حسين، قاعدة مشروعية الدليل الجنائي، رسالة دكتوراه، جامعة القاهرة، مصر، 2014، ص 204.

و في هذا الإطار نجد أنّ المشرّع الفرنسي خوّل النيابة العامة هذه السّلطة و لكن بإذن من قاضي الحرّيات و الحبس بموجب المادّة 60 فقرة 02 من قانون الإجراءات الجزائية، و هو موقف المشرّع المصري⁽¹⁾، و إن خوّل التّشريع القطري و البحريني هذه السّلطة إلى النيابة العامة⁽²⁾، فإنّ التّشريع البحريني جعل أمر تجديد هذه المدة الزمنية من إختصاص المحكمة الجنائية الكبرى⁽³⁾.

أمّا بخصوص مقترح البرلمان الأوروبي المتعلّق بأوامر إنتاج و حفظ الأدلّة الجنائية الإلكترونيّة بين دول الإتحاد الأوروبي فهي تحدّد السّلطة المختصة بإصدار الأمر بالحفظ و الإنتاج بحسب طبيعة البيانات المستهدفة و أثرها على الحق في الخصوصية، فنظرا لكون الأمر بحفظ بيانات المشترك و بيانات النّفاذ أقلّ تقييدا للحرية الفردية فقد أجازت لجهة الاتّهام سلطة اللّجوء إلى هذه الوسيلة ضمن هذه الحدود الموضوعية، أما إذا تعلّق الأمر ببيانات

(1) المادة 06 من القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات السابق ذكرها.

(2) المادة 21 من القانون القطري رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإجرائية تنص "للنيابة العامة أن تأمر كل ذي صلة بتسليم الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإجرائية أو بيانات المرور أو معلومات المحتوى ذات الصلة بموضوع الجريمة أو ما يفيد في كشف الحقيقة و للنيابة العامة أن تأمر بالتحفظ على الأجهزة و الأدوات أو الوسائل المستخدمة في ارتكاب الجريمة".

(3) تنص المادة 12 من القانون قانون البحريني رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات "

1- للنيابة العامة أن تأمر أيّ شخص بالقيام على وجه السرعة بالحفاظ على سلامة بيانات معيّنة لوسيلة تقنية المعلومات، بما في ذلك بيانات خط السير المخزّنة داخل نظام تقنية المعلومات، تكون في حيازته أو تحت سيطرته وبالإبقاء على سلامة هذه البيانات متى رأت الحاجة لذلك لإظهار الحقيقة في أية جريمة و توافرت لديها دلائل تحمّلها على الإعتقاد بأنّ هذه البيانات عرضة للفق أو التّغيير.

2- للنيابة العامة أن تأمر الشّخص المشار إليه في الفقرة (1) من هذه المادة بالحفاظ على البيانات والإبقاء على سلامتها لمدة لا تزيد على تسعين يوماً، و للمحكمة الكبرى الجنائية منعقدة في غرفة المشورة أن تأذن للنيابة العامة، بناء على طلب مشفوع بالمبررات يقدّم قبل إنقضاء المدة المشار إليها بثلاثة أيام، مد هذه الفترة لمدة أو لمدد متعاقبة لا يزيد مجموعها على تسعين يوماً أخرى. و على المحكمة -كلما أمكن ذلك- سماع أقوال الشّخص المشار إليه.

3- للنيابة العامة أن تأمر الشّخص المشار إليه في الفقرة (1) من هذه المادة بالمحافظة على سرية الأمر الصّادر له وفقاً لأحكام أيّ من الفقرتين (1) و (2) من هذه المادة لمدة لا تزيد على تسعين يوماً، قابلة للتّجديد لمدة أو لمدد متعاقبة لا يزيد مجموعها على تسعين يوماً أخرى..".

المحتوى فلا يجوز أن يصدر الأمر بالحفظ و التسليم سوى من قبل سلطة التحقيق (قاضي المحكمة أو قاضي التحقيق)⁽¹⁾.

في هذا السياق أشارت المذكرة التفسيرية لاتفاقية بودابست إلى أنّ عبارة "الأمر أو الحصول بطريقة مماثلة" تشير إلى إمكانية استخدام أساليب قانونية أخرى لتحقيق الحفظ بالاكتفاء بأمر قضائي أو إداري أو توجيهات من المدعي العام أو الشرطة" بحيث تتيح هذه العبارة مرونة مقصودة بغية تمكين الدول من تنفيذ هذا الإجراء بشكل سريع⁽²⁾.

لذا يرى جانب من الفقه أنّ أهمية الأمر بالحفظ لا تتحقّق سوى بالتّصرف الفوري و السّريع، فيكون من المفيد التّخلي عن اقتضاء صدور إذن قضائي مسبق و تمكين الإدعاء أو الضّبطية القضائية من إصدار أمر بالحفظ لأنّ ذلك سيمكّن تلك السّلطات المختصة من التّصرف بسرعة أكبر، أما حماية حقوق المتّهم فتتحقّق في المرحلة الإجرائيّة الموالية للأمر بالحفظ أي في مرحلة الإنتاج و الإفصاح عن مضمون هذه البيانات أين يفرض الضّمان القضائي⁽³⁾.

و تحقيقاً لهذه الغاية نجد أنّ المشرّع البلجيكي قد بادر بإدخال تعديلات على قانون التّحقيق الجنائي بمقتضى قانون 25 ديسمبر 2016 الرّامي إلى تحسين أساليب التّحقيق الجنائي المعلوماتي، أين سمحت المادّة 3 من هذا القانون لأيّ ضابط من ضباط الشرطة القضائية إذا كان هناك سبب للاعتقاد بأنّ البيانات المخزّنة أو المعالجة أو المنقولة عن طريق نظام حاسوبي عرضة بشكل خاص للضياع أو التّعديل، أن يأمر بموجب قرار كتابي شخص أو أكثر من الأشخاص الطبيعيين أو الأشخاص الاعتباريين للحفاظ على البيانات الموجودة في حوزتهم أو سيطرتهم، و في حالة الإستعجال يجوز التّخلي عن شرط القرار المكتوب مع إستدراكه لاحقاً تحت طائلة عقاب مزوّد الخدمة في حالة إتخاذه موقفاً سلبيّاً⁽⁴⁾.

(¹) l article 04 de la Proposition de règlement du parlement européen et du conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, 2018/0108(COD), Strasbourg, 17 avril 2018.

(²) Conseil de l'Europe, Rapport explicatif de la Convention du Conseil de l'Europe sur la cybercriminalité, Clause n°160.

(³) ماركو جيركي، المرجع السابق، ص 285.

(⁴) LOI du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures

في اعتقادنا فإنّ توجه المشرّع البلجيكي يميل إلى ترجيح اعتبارات الفعالية، قد يكون هذا الموقف مبرّرا من منظور الشّرعية الإجرائيّة إلى حد ما، كون الأمر بالحفظ في حقيقته لا يعدو أن يكون مجرد إجراء سابق عن الضّبط الرقمي و لا يقع بموجبه الضّبط بمفهوم القانون، إذ أنّ البيانات المستهدفة بموجب هذا الأمر، لا تنتقل حيازتها إلى السّلطة الإجرائيّة بل تبقى تحت سيطرة مزوّد الخدمة، يلزم من خلاله بالحفاظ عليها و عدم حذفها إلى حين إصدار الأمر بالإفصاح و الذي بمقتضاه تضع سلطة التّحقيق يدها على هذه البيانات.

و هذا الموقف الذي تبناه المشرّع البلجيكي مستمد من طبيعة هذه القرارات التي لا تحتمل التّأجيل تحت طائلة فقدانها لفعاليتها إذ لو إعتمد حلا مغايرا بشأنها لأضحت الأدلّة عرضة للضياع، و من الملاحظ هنا أنّ ضرورة فعالية الإجراء تتقدم على ضرورة شرعية هذا الأخير، و هو الموقف الذي أشارت إليه إتفاقية بودابست و استوضحته مذكرتها التفسيرية على أساس أنّ التنازل على هذا الضّمان سيمكّن السّلطات المختصة من التّصرف بسرعة أكبر في حين تتحقّق حماية حقوق المتّهم باقتضاء إصدار إذن قضائي للإفصاح عنها⁽¹⁾.

d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales JORF du 14 janvier 2017 Art. 3. Dispose que " Dans le même Code, il est inséré un article 39ter rédigé comme suit: Art. 39ter. § 1er. Lors de la recherche de crimes et délits et sans préjudice des compétences visées aux articles 39bis, 46bis et 88bis et aux articles XII.17, XII.18, XII.19 et XII.20 du Code de droit économique, tout officier de police judiciaire peut, s'il existe des raisons de croire que des données stockées, traitées ou transmises au moyen d'un système informatique sont particulièrement susceptibles de perte ou de modification, ordonner, par une décision écrite et motivée, à une ou plusieurs personnes physiques ou personnes morales de conserver les données qui sont en leur possession ou sous leur contrôle.

La décision écrite motivée mentionne:.....

En cas d'urgence, la conservation peut être ordonnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue à l'alinéa 2.

§ 2. Les personnes physiques ou personnes morales visées au paragraphe 1er, alinéa 1er, veillent à ce que l'intégrité des données soit garantie et à ce que les données soient conservées de manière sécurisée.

§ 3. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de coopérer, ou qui fait disparaître, détruit ou modifie les données conservées, est punie d'un emprisonnement de six mois à un an ou d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement."

(1) و قد أشارت المذكرة التفسيرية للإتفاقية الأوروبية لمكافحة الجريمة المعلوماتية في فقرتها 174 إلى أنّه "يمكن أن تستثنى الشّروط و الضّمانات المشار إليها في الفقرة 2 من المادة 18 و فقا للقانون الداخلي لكل طرف البيانات أو

و نحن نخالف هذا التوجه بالسّماح للضّبطية القضائية باتخاذ هذه الوسيلة الإجرائيّة دون أي ضمان قضائي، لأنّ هذا التّدبير يبقى من الأعمال القضائية التي تحرص في إذنها على مراعاة الكثير من الضّوابط الإجرائيّة التي تحفظ الحق في الخصوصية كمبدأ الضّرورة و مبدأ التّناسب و شرط التّحديد في البيانات المطلوبة، و درجة ارتباطها بالجريمة الجاري التحقيق بشأنها و فائدتها في إظهار الحقيقة، و مدى كفاية القرائن المتوافرة التي تسمح باتخاذ هذا الإجراء و حماية البيانات الخاضعة للسّرية المهنية، لذا ينبغي عدم جعل الحرّيات الفردية خاضعة للسّلطة التقديرية للضّبطية القضائية نهائياً، فهو يبقى من الإجراءات الاستثنائية القضائية.

ختاماً، فإنّ هذا الإجراء في الغالب يمكن أن يؤدي إلى تحديد منبع و مصب الإتصال و تحديد هوية الفاعل أو على الأقل النّهاية الطّرفية التي تم من خلالها الإرسال، و هو ما يعتبر قرينة قوية تؤسّس لطلب الإذن بتفتيش بيانات أحد طرفي الإرسال أو غيرها حسب ما تكشف عنه ظروف الواقعة، تمهيدا لمباشرة الخطوة التّانية و هي "مرحلة التّفتيش المعلوماتي" أين يصطدم القائم بالتّفتيش بكم هائل من البيانات تختلط فيه البيانات البريئة مع البيانات المجرّمة التي تشكل موضوعاً للدليل مع استحالة معرفة موقع هذه الأخيرة قبل تنفيذ التّفتيش و امتداده إلى عدد كبير منها بما يتجاوز الغاية من التّفتيش كضمان أساسي لحماية الحرّيات الفردية إلى استباحة أسرار الأفراد.

و لعلّ هذه المشكلة تعدّ من المشكلات الكبرى التي شكّلت هاجساً للفقهاء و القضاء، فكيف يمكن استعادة الحدود التقليديّة للتّفتيش في بيئة رقمية تنعدم فيها الحدود المادية؟ ذلك ما نحاول أن نجيب عنه في الفصل الثاني.

المعلومات الإمتيازية و قد يرغب أحد الأطراف في تحديد شروط و سلطات مختصة و ضمانات مختلفة فيما يتعلّق بتقديم أنواع معيّنة من البيانات الحاسوبية أو معلومات عن المشتركين التي تحتفظ بها فئات معيّنة من الأشخاص أو مقدمي الخدمات فعلى سبيل المثال يجوز لأي طرف فيما يتعلّق بعض أنواع البيانات مثال المعلومات عن المنخرطين المتاحة للعموم أن يسمح لعناصر إنفاذ القانون إصدار أمر من هذا القبيل يتطلب في حالات أخرى أن يصدر عن المحكمة و من ناحية أخرى قد يطلب الطّرف في بعض الحالات أو أن يكون مطالباً بموجب ضمانات حقوق الإنسان أن يصدر أمر التّقديم عن السّلطة القضائية فقط بغية التّمكّن من الحصول على أنواع معيّنة من البيانات و قد ترغب الأطراف في حصر الكشف عن هذه البيانات لأغراض تنفيذ القانون في الحالات التي يكون فيها أمر التقديم من أجل الكشف عن هذه المعلومات صادراً عن سلطات قضائية و يوفّر مبدأ التّناسب أيضاً بعض المرونة فيما يتعلّق بتطبيق التّدبير و الذي تلجأ له كثير من الدّول من أجل استبعاد تطبيقه على الحالات البسيطة .

الفصل الثاني

ضوابط التفتيش عن الأدلة المعلوماتية

التفتيش عن الأدلة المعلوماتية إجراء قانوني يمسّ الحرّيات الشخصية لذلك تحرص مختلف التشريعات على إحاطته بقيود و ضمانات أساسية سعياً لتحقيق التوازن بين اعتبارات مصلحة الهيئة الإجتماعية في التّوصل إلى الحقيقة و بين حقوق الأفراد و حرياتهم، و من بين هذه الضّمات التي ينبغي توافرها لإجراء التفتيش عن الأدلة المعلوماتية ما هو موضوعي (مبحث أول)، و منها ما هو شكلي (مبحث ثاني).

المبحث الأول

الضوابط الموضوعية للتفتيش عن الأدلة المعلوماتية

الأصل أنه لا يوجد في القانون حق مطلق، لذا فإن حق الهيئة الإجتماعية في اللجوء إلى التفتيش عن الأدلة المعلوماتية إعمالاً لحقها في الحفاظ على كيان المجتمع و ردع المجرمين، يظل محاطاً بجملة من الشروط التي تقيد استعماله و ترسم حدوده، فلا يجوز لها إعمال هذا الإجراء الخطير إلاّ إذا قام السبب الذي يبرر المساس بالحريّات الفردية (مطلب أول)، مع وجوب قصره على محل معيّن (مطلب ثاني).

المطلب الأول: سبب التفتيش المعلوماتي

لا يمكن إنتهاك الحريّات الفردية إلاّ إذا قام مبرر في القانون لهذا الإنتهاك، و هو وقوع الجريمة سعياً للوصول إلى الدليل بقصد إستظهار الحقيقة (فرع أول)، مع توافر دلائل كافية على وجوده في مكان معيّن (فرع ثاني)، و توجيه الإتهام لشخص بارتكاب هذه الواقعة الجرمية (فرع ثالث).

الفرع الأول: التّحقق الفعلي لجريمة من نوع جنائية أو جنحة

سبب التفتيش هو البحث عن الدليل المعلوماتي و استرجاعه، و هذا السبب لا ينشأ إلاّ بعد وقوع الجريمة، فحق الهيئة الاجتماعية في اتخاذ هذا الإجراء لا ينشأ إلاّ بتحقق الفعل المجرّم، لذا يحظر التفتيش عن الأدلة المعلوماتية لمجرد التحوط لجريمة مستقبلية (أولاً)، بل لا بد أن تبلغ هذه الجريمة من الخطورة ما يسمح بالتعرض للحقوق الفردية و الحريّات الشخصية (ثانياً).

أولاً: الوقوع الفعلي للجريمة

على الرغم من أنّ ضابط الوقوع الفعلي للجريمة يعتبر من الضمانات الجوهرية التي تحول دون الافتئات على الحريّات الفردية دون مبرر يسوغ ذلك، إلاّ أنّ المشرّع الجزائري لم يعتمد هذه القاعدة على إطلاقها، بل أجاز التفتيش عن الأدلة المعلوماتية في سياق التحوط من بعض الجرائم المستقبلية التي تهدد الأمن الوطني، و يتحتّم علينا تبعا لذلك، أن ندفع بهذه القاعدة (أ) و الإستثناءات الواردة عليها إلى دائرة الضوء (ب).

أ- حظر التفتيش المعلوماتي في سياق التحوط لجريمة مستقبلية

نعني بسبب التفتيش المعلوماتي "الواقعة المنشئة للسلطة في التفتيش"، أي الواقعة التي تخول للمحقق الحق في أن يصدر أمراً بالتفتيش⁽¹⁾، لذا فإنه من القواعد الإجرائية المهمة أنّ التحقيق لا يباشر إلا بعد وقوع فعل يعدّ في نظر القانون جريمة، فلا يجوز الأمر بالتفتيش لضبط أدلة في جريمة مستقبلية و لو قامت التّحريات و الدلائل الجدية على أنّها ستقع بالفعل⁽²⁾، معنى ذلك أنّ الإذن بالتفتيش إنّما يصدر لضبط دليل جريمة تحقّق وقوعها من مقارناتها لا لضبط جريمة محتملة، و هو شرط يقتضيه المنطق السليم لأنّ التفتيش من إجراءات التحقيق، الذي يسعى لغاية محدّدة و هي التّوصل إلى حقيقة الواقعة الإجرامية، و من غير المتصوّر القيام بأيّ إجراء من إجراءات التحقيق قبل وقوع الجريمة.

و لما كان سبب التفتيش هو الحصول على الدليل في تحقيق قائم مع قيام القرائن على وجود ذلك الدليل لدى شخص معيّن أو في مسكنه أو أيّ محلّ آخر، فإنّ تلك العلة هي التي تدفع السلطة المختصة إلى إصدار قرارها بالتفتيش و مباشرته، و هذا المعنى تملّيه القواعد العامة في القانون، و لأهمية هذا القيد في حماية الحرّيات الفردية من كلّ تعسف رأى المشرّع ضرورة النصّ عليه صراحة في القانون، حيث تنصّ المادة 44 من قانون الإجراءات الجزائية على أنّه "لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنّهم ساهموا في الجناية أو أنّهم يحوزون أوراقاً أو أشياء متعلّقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلاّ بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الإستظهار بهذا الأمر قبل الدخول إلى المنزل و الشروع في التفتيش"، فعبارة "أنّهم ساهموا في الجريمة"

(1) محمود نجيب حسني، شرح قانون الإجراءات الجنائية، بدون رقم الطبعة، دار النهضة العربية، القاهرة، 2013، ص 594.

(2) قرّرت محكمة النقض المصرية بأنّ "الأصل في إذن التفتيش و تسجيل المحادثات أنّه إجراء من إجراءات التحقيق لا يصحّ إصداره إلاّ لضبط جريمة (جناية أو جنحة) وقعت بالفعل و ترجّحت نسبتها إلى متهم معيّن و أنّ هناك من الدلائل ما يكفي للتّصدي لحرمة مسكنه أو لحرية الشخصية (نقض جلسة 1987/11/11 س 38 ق 153 ص 943)، كما قضت بأنّ "الأصل في القانون أنّ الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يصحّ إصداره إلاّ لضبط جريمة "جناية أو جنحة" واقعة بالفعل و ترجّحت نسبتها إلى متهم معيّن و أنّ هناك من الدلائل ما يكفي للتّصدي لحرمة مسكنه أو لحرية الشخصية" (نقض جلسة 1986/12/11 س 37 ق 200 ص 1059) مشار إليهما لدى: إيهاب عبد المطلب، تفتيش الأشخاص و الأماكن، الطبعة الأولى، المركز القومي للإصدارات القانونية، مصر، 2009، ص 148.

تفيد تحقّق الجريمة بتاريخ سابق عن اللّجوء إلى التفتيش، و هذه القاعدة عامة تنطبق على كافة صور التفتيش دون أن تقتصر على تفتيش المساكن، لأنّ عموم النّص لا يصحّ تخصيصه دون سند.

و يعدّ هذا الشرط بمثابة الشرط المفترض و الشرط الأولي، و مردّ ذلك إلى أنّ الغاية النهائيّة من إصدار إذن التفتيش هي ضبط دليل أو أكثر يؤكد أو ينفي نسبة الجريمة إلى الخاضع للتفتيش، سواء كان لديه في شخصه أو شخص غيره أو في مسكن أو مسكن غيره، فإذا لم تكن هناك جريمة على هذا النّحو فلن تكون هناك حاجة إلى إصداره لانقضاء السبب، و يوصف هذا الشرط بكونه الشرط الأساسي بحكم دوره الهام في إصدار إذن التفتيش و صحته، بمعنى أنّ مفترضات بحث صحة إصدار الإذن و صحة الإجراءات السابقة على صدوره تبدأ من هذا الشرط⁽¹⁾.

فإذا صدر أمر بتفتيش مسكن لأنّ التّحريات دلّت على أنّ الشّخص المقيم فيه سيحوز في اليوم الموالي مواد مخدرة عقد العزم على شرائها أو أنّه سيتقاضى مبلغاً على سبيل الرّشوة فالأمر في الحالتين باطل و يبطل التفتيش ذاته و ما يتولّد عنه من أدلة⁽²⁾، و هكذا يتضح لنا من تحليل مفهوم وقوع الجريمة على النّحو المتقدّم أنّ جوهر هذا الشرط يتمثّل في التأكيد على عدم صحة إجراء التفتيش حتّى و لو كان بموجب إذن قضائي متى كان ذلك بقصد الكشف عن جريمة غير معلوم ارتكابها للسلطة الأمرّة، و من ثمّ يفقد هذا الإجراء الغاية الأساسية لإقراره و التي تتمثّل في اعتباره وسيلة جمع أدلّة الإثبات في المواد الجنائية⁽³⁾.

ب) - الاستثناء الوارد على قاعدة حظر التفتيش المعلوماتي لمنع وقوع الجريمة

قدّمنا أنّ قاعدة وجوب التّحقّق الفعلي للجريمة، كشرط مسبق لنشوء حق الهيئة الإجتماعية في اللّجوء إلى التفتيش المعلوماتي يعتبر بمثابة خط دفاع أولي ضد أي إنحراف أو تسعف قد تقدم عليه هذه الأخيرة، لما ينطوي عليه هذا الإجراء من خطورة المساس بحرمة

(1) حسام الدين محمد أحمد، الإذن بالضبط و التفتيش، بدون رقم الطّبعة، دار النّهضة العربية، مصر، 2003، ص 37.

(2) محمود نجيب حسني، شرح قانون الإجراءات الجنائية، بدون رقم الطّبعة، دار النّهضة العربية، القاهرة، 2013، ص 595.

(3) حسام الدين محمد أحمد، المرجع السابق، ص 37.

النظام المعلوماتي التي تتجاوز بكثير الحرمة المكرّسة ليس فقط للمساكن بل تتعدى حرمة غرفة النوم أيضا، وبالرغم من خذه الحقيقة إلا أنّ المشرّع الجزائري أهدر هذا الضمان الإجرائي الهام بأن أورد عديدا من الاستثناءات على هذه القاعدة الوقائية.

واقع الأمر أنّه بالرّجوع إلى نص المادة 5 من القانون 04/09 الذي يتضمّن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها التي تحيلنا بدورها على المادة 4 من نفس القانون، يتبيّن أنّ المشرّع يسمح باللّجوء إلى التفتيش المعلوماتي و لو لم يتحقّق الوقوع الفعلي للجريمة في حالتين، أولا "للوّاقية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة". و ثانيا "في حالة توافر معلومات عن احتمال إعتداء على منظومة معلوماتية على نحو يهدّد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني"، مما مقتضاه أنّه أجاز التفتيش المعلوماتي لتوقّي خطر جريمة يحتمل وقوعها في المستقبل، و في اعتقادنا فإنّ هذا النصّ مخالف لمبدأين هاميين في القانون، مبدأ إفتراض البراءة و مبدأ وضوح النصّ الجنائي.

1 (مخالفة مبدأ إفتراض البراءة

إنّ التّسامح الملحوظ من طرف المشرّع بخصوص الاستثناءات التي أوردتها على قاعدة حظر التفتيش المعلوماتي لاكتشاف الجريمة و منع وقوعها، يعدّ مساسا خطيرا بضمانات دستورية و يتنافى مع مبدأ إفتراض البراءة، لأنّ الغاية من التفتيش قضائية و هي البحث عن الأدلّة ، مما يستلزم تمييزها عن الأغراض الإدارية أو البوليسية، و من أهمّ الأغراض ذات الطّابع الإداري أو البوليسي التي قد تختلط مع هذه الغاية القضائية، هو البحث عن الجرائم لكشفها و منع وقوعها أو منع تمامها، فصيانة الأمن بمنع وقوع الجريمة غاية جلييلة و غرض نبيل، لكنها ليست غرضا قضائيا و لذلك فمهما يكن من نبيل هذا الهدف و سموه، فإنّه لا يجوز إجراء التفتيش لتحقيقه⁽¹⁾، " فالإحتياط لمنع ارتكاب الجرائم هو عمل من أعمال الضبطية الإدارية و لا يبرر القانون إتخاذه أساسا للإذن بالتفتيش"⁽²⁾.

(1) توفيق محمد الشاوي، المرجع السابق، ص 93.

(2) حكم محكمة جنايات الإسكندرية في 23 مارس 1950، مشار إليه لدى توفيق محمد الشاوي، المرجع السابق، ص 95.

فالأصل أنّ عمل السّلطة القضائية لا يبدأ إلاّ بعد تحقّق الجريمة و ليس قبل ذلك، إذ أنّ وقوع الجريمة هو الذي يشكّل الحد الفاصل بين الإجراءات القضائية بما فيها التفتيش و الإجراءات الإدارية المشابهة لها و التي لا يجوز أن تصل إلى فرض إجراءات مقيدة لحرّيات الأفراد، لذا نرى أنّ التفتيش المعلوماتي لتوقي خطر وقوع جريمة محتملة و يجب إعتباره غير مشروع، فالمشرّع بمقتضى هذا النصّ استبدل المبدأ الطبيعيّ المعبر عنه بمبدأ إفتراض البراءة بقرينة الإدانة *La Présomption De Culpabilité*، لأنّ الغرض من التفتيش في هذه الحالة لم يكن لغاية جمع الأدلّة بل لمنع حدوث جريمة محتمل وقوعها مستقبلا.

و لا معنى لأصل البراءة -الذي يشكّل سياجا لحماية الحرّية الشّخصية في مواجهة كل إجراء تتخذه السّلطة و في أيّ مرحلة من المراحل الإجرائية للإثبات الجنائي- إذا أجزت تفتيش النّظم المعلوماتية لفرد من أفراد الهيئة الإجتماعية لمجرد إحتمال وقوع جريمة في المستقبل. ذلك أنّ أصل البراءة ليس إلاّ تأكيدا للأصل العام و هو حرية المتهم، مما يترتب عليه ضرورة حماية جميع الحقوق و الحرّيات و التي بغيرها يفقد أصل البراءة معناه، فالحرّية لا يمكن أن ترتفع من خلال إنتهاكات للحقوق و الحرّيات التي تكون معها وحدة متكاملة هي كرامة الإنسان⁽¹⁾، بل إنه لا يمكن أصلا الحديث عن هذا الضمان إلاّ بعد وقوع الجريمة و توجيه الاتهام.

غير أنّ المحكمة الأوروبية لحقوق الإنسان قررت شرعية الإجراءات الماسة بالحرّيات الشّخصية التي تتخذ في سبيل الوقابة من الجرائم الخطيرة التي تهدّد حياة الأمة و حصرت ذلك في نطاق الظروف الإستثنائية و قالت المحكمة "إنّ المجتمعات الديمقراطيّة اليوم مهدّدة بأشكال بالغة التعقيد من التّجسس و الإرهاب، و حتّى تتمكّن الدولة من مكافحة هذه التّهديدات بفعالية، و مراقبة العناصر الهدامة التي تعمل على أراضيتها سرا، فإنّ وجود أحكام تشريعية تمنح السلطات المراقبة السّرية للمراسلات و الطرود البريدية و الإتصالات السّلكية و اللاسلكية، في مواجهة وضع استثنائي، أمر ضروري في مجتمع ديمقراطي، و الأمن الوطني و إنفاذ القانون، و منع الجرائم"⁽²⁾.

(1) أحمد فتحي سرور، القانون الجنائي الدّستوري الطّبعة الثّانية، دار الشّروق، مصر، 2002، ص282.

(2) Geneviève Giudicelli-Delage, Les transformations de l'administration de la preuve pénale Perspectives comparées : Allemagne, Belgique, Canada, Espagne, Etats-Unis, France, Italie, Portugal, Royaume-Uni, Archives de politique criminelle, 2004/1 ,n° 26, p 154.

لا جدال في أنّ الظروف الإستثنائية تسمح بوضع قيود على الحرّيات الفردية أوسع نطاقاً مما تتضمنه الإجراءات الجنائية في ظلّ الشرعية الإجرائية في الظروف العادية⁽¹⁾، لكنه عند تقييم ضرورة تدبير معيّن، تشدّد اللّجنة المعنية بحقوق الإنسان في تعليقها العام رقم 27 على المادّة 12 من العهد الدولي الخاص بالحقوق المدنية و السياسية على "عدم إعاقة جوهر الحق من جزاء القيود و يجب ألاّ تُقلّب العلاقة بين الحق و القيد، بين القاعدة و الإستثناء، و ينبغي للقوانين التي تجيز تطبيق القيود أن تستخدم معايير دقيقة، و لا يجوز لها أن تمنح المسؤولين عن تنفيذها حرية غير مقيدة للتصرف حسب تقديراتهم"⁽²⁾، فحتّى في هذه الحالة و جب قيد نطاق أعمال هذه الإجرائية الإستثنائية ضمن حدود الضرورة بموجب قوانين واضحة و محدّدة تجنبا لأيّ تعسّف في تطبيقها، و هو ما يقودنا إلى الضمان التّاني الذي أهدره المشرّع الجزائري.

(2) - مخالفة مبدأ وضوح النصّ الجنائي الإجرائي

لا تتوقف مستلزمات الشرعية الإجرائية أن يكون القانون مصدرا لقواعد الإجراءات الجزائية فحسب، بل أن يكون دقيقاً بما يكفي لتمكين الشّخص المتأثر من تنظيم تصرفاته، مع تبصّر الآثار التي يمكن أن تترتب عن عمل معيّن.

كما يجب أن تضمن الدّولة أنّ يكون أيّ تدخل في الحق في الخصوصية أو العائلة أو السّكن أو المراسلات جائز بموجب قوانين يمكن أن يصل إليها عامة الجمهور، تتضمن أحكاماً تضمن أنّ عمليات جمع البيانات و الوصول إليها و استخدامها مصمّمة لأهداف مشروعة محدّدة، دقيقة بما يكفي و تحدّد بالتفصيل الظروف الدّقيقة التي يمكن السّماح فيها

(1) تنص الفقرة الأولى من المادة الرابعة من العهد الدولي للحقوق المدنية و السياسية: "في حالات الطّوارئ الإستثنائية التي تتهدّد حياة الأمة، والمعلن قيامها رسمياً، يجوز للدّول الأطراف في هذا العهد أن تتخذ، في أضيق الحدود التي ينطلبها الوضع، تدابير لا تتقيّد بالالتزامات المترتبة عليها بمقتضى هذا العهد، شريطة عدم منافاة هذه التدابير للالتزامات الأخرى المترتبة عليها بمقتضى القانون الدولي و عدم إنطوائها على تمييز يكون مبرّره الوحيد هو العرق أو اللّون أو الجنس أو اللّغة أو الدّين أو الأصل الاجتماعي".

(2) مشار إليه لدى تقرير مفوضية الأمم المتحدة السّامية لحقوق الإنسان الحق في الخصوصية في العصر الرّقمي، وثيقة رقم: A/hrc/2737، ص 11، فقرة 25.

بأيّ تدخل من هذا النوع، و إجراءات إصدار الإذن، و إجراءات إستخدام البيانات المجمّعة و تخزينها، و تنصّ على ضمانات فعّالة ضد التّجاوزات⁽¹⁾.

بالعودة إلى نص المادّة 5 من القانون 04/09 فإنّه يبدو جليا مخالفتها لهذه المعايير التي استقرّت عليها سوابق المحكمة الأوروبية لحقوق الإنسان، بل مناقضة لروح الأحكام الدستورية التي ترعى الحق في الخصوصية، فهي تنطوي على غموض و لبس شديدين، إذ نصّت على جواز اللّجوء إلى التفتيش المعلوماتي " للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التّخريب أو الجرائم الماسة بأمن الدولة.. في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدّد النظام العام أو الدّفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني..".

فهذه الصياغة التشريعية تمنح للقائم بالتفتيش سلطات تقديرية واسعة في تفسيره للقاعدة الإجرائية، فاستعمل المشرّع عبارة "النظام العام" و هي أشدّ العبارات غموضا في القانون، حتّى قيل إنّ "النظام العام يستمدّ عظمته من ذلك الغموض الذي يحيط به، فمن مظاهر سموه أنّه ظلّ متعاليا على كل الجهود التي بذلها الفقهاء لتعريفه".

لذا كان الأولى بالمشرّع عند تنظيمه لهذا الإجراء الخطير خاصة في الأحوال التي أجاز فيها اللّجوء إليه في سياق منع وقوع الجرائم، أن يكون حريصا على دقة القاعدة الإجرائية فيحدّد بوضوح الحالات التي يجوز فيها تقييد الحق في الخصوصية بهذا الشكل الخطير، على نحو يغلّق باب التّأويل و التفسير الموسع بالإحالة مباشرة على نصوص المواد المحدّدة في قانون العقوبات، فالنقييد الوارد في المادّة 4 من القانون 04/09 يجرّد فعلا الحق في الخصوصية من معناه، لأنّه بإمكان سلطة التّحقيق بل و حتّى قضاء الحكم تفسير القاعدة الإستثنائية بشيء من التّوسع لتصبح بالفعل قاعدة عامة تبيح اللّجوء إلى هذا الإجراء لمنع وقوع أي جريمة منصوص عليها في القانون، و من هنا يصبح هذا الضمان المتمثّل في القانون "بحد ذاته ظالم و غير إنساني، بل مجرد عزاء تافه لضحاياه"⁽²⁾.

(1) الجمعية العامة للأمم المتحدة، مجلس حقوق الإنسان، تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان الحق في الخصوصية في العصر الرقمي، وثيقة رقم A/hrc/2737، ص 12.

(2) Marsh, Norman S, Commission internationale de juristes, Le principe de la légalité dans une société libre : rapport sur les travaux du Congrès international de juristes tenu à New Delhi (Janvier 1959), p 62.

و إذا كان من حسن حظ الأفراد و حرياتهم أنّ القواعد التقليديّة للتفتيش المادي تعتبر أنّ هذا الإجراء قيد مقررّ على حقوق الأفراد لمصلحة العدالة و القضاء وحده و لا يجوز استعماله إلاّ لمصلحة الإثبات الجنائي الذي لا يشرع في إجراءاته إلاّ بعد وقوع الجريمة و اكتشافها فعلا، فإنّ السّؤال الذي يفرض نفسه هنا كيف يمكن المحافظة على هذا المبدأ الإجرائي العتيد حال اللّجوء إلى التفتيش المعلوماتي في الأحوال التي يقتضي فيها تنفيذه و جوب المرور بالخطوة الأولى و هي مرحلة "التفتيش المادي" لمسكن المتّهم، بحثا عن أجهزة التخزين الرّقمية لإخضاعها للتفتيش المعلوماتي لاحقا؟

هل قاعدة جواز التفتيش المعلوماتي للوقاية من الجرائم وفقا لأحكام المادّة 5 من القانون 04/09، تسمح بتجاوز هذا المبدأ الرّاسخ فتجيز التّعرض لحرمة مساكن الأفراد في سبيل كشف مبلغ اتصالحهم بجريمة لم تقع بعد؟ أم أنّ التفتيش وفقا لهذا الوضع قاصر فقط على التفتيش المعلوماتي الذي يجري خارج حدود مسكن المتّهم أو عن بُعد؟

إنّ النّص القانوني السّالف ذكره لم يجب بشكل صريح على التّساؤل المطروح، و قد جاء فيه "يجوز للسّطات القضائية المختصّة و كذا ضباط الشّركة القضائية في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عليها في المادّة 4 أعلاه الدّخول بغرض التفتيش و لو عن بعد..."، و المستفاد منه أنّ المشرّع إستوجب حال مباشرة التفتيش المعلوماتي وجوب التّقيّد بالضّمّانات الإجرائية التي يخضع لها التفتيش بشكل عام و المحدّدة في قانون الإجراءات الجزائية، مما مقتضاه أنّه لا يجوز الإذن أو الأمر بإجراء التفتيش المعلوماتي لمنع وقوع الجرائم السّابق بيانها إذا ما استلزم تنفيذه إجراء تفتيش مادي لمسكن المتّهم أو غيره، سعيا لحصر نطاق التفتيش في مجال محدود تقتضيه مصلحة المجتمع و لخطورته لم يجزه المشرّع في تفتيش المساكن إلاّ حين وقوع الجريمة و تكشف معالمها.

و بمفهوم المخالفة فإنّه يجوز إجراء التفتيش المعلوماتي في الحالة التي يكون فيه الشّخص محلا للتفتيش المادي الأولي و أيضا في حالة التفتيش المعلوماتي عن بعد، أي في

جاء في هذه المداخلة:

" On a d'autre part objecté que le Principe de la Légalité, entendu comme l'application certaine d'un droit que chacun peut connaitre á l'avance, s'inspire d'un critère trop étroit. Dans un pays ou les lois elles-mêmes sont injustes ou inhumaines, le fait de les connaitre avec certitude et de savoir qu'elles seront appliquées n'apportera qu'une piètre consolation á leurs victimes. "

جميع الحالات الأخرى التي لا يتطلب فيها التفتيش المعلوماتي انتهاك حرمة المسكن، و نحن نعارض مسلك المشرع في هذه المسألة، لأننا نرى أنه لا يوجد أي أساس سواء في قانون الإجراءات الجزائية أو القانون 04/09 أو غيرهما من القوانين، بمقتضاه يعتبر تفتيش المعلومات أو تفتيش الشخص أقل خطورة من تفتيش المسكن، لأن حرمة المسكن في الحقيقة ليست إلا وجهها من أوجه حماية حرمة الأشخاص، و حماية المعلومات ليست سوى مظهرا عاما لحماية هذه الحرمة بالرغم من طغيان "الحق في حرمة المعلومات" على باقي الحقوق بالنظر إلى المجتمع المعاصر الذي يفضل أفراده دفن أسرارهم و تفاصيل حياتهم الشخصية ضمن الأوعية المعلوماتية، لذا يصبح من العبث الحديث عن الحرّيات الفردية بقصرها على حرمة المسكن طالما لم تشمل هذه الحماية حرمة المعلومات.

ففي نظرنا فإن أمن الفرد في نظامه المعلوماتي من أقوى مظاهر الحماية الإجتماعية التي يجب أن تكفل له، خاصة أن الوضع المجتمعي الحالي يكشف توجه أفرادهم و تمسكهم بالمعلوماتية في مختلف مناحي الحياة، لذا ينبغي لتفتيشها اعتماد ذات القواعد و القيود التي تحكم تفتيش المساكن، بل يلزم التّشدد فيها، فكان على المشرع أن يحيط النظام المعلوماتي بالعناية الأوفى باعتباره المستودع الطبيعي الذي يغلب أن يحفظ الإنسان فيه سره.

و يمكن أن نخلص مما تقدم إلى أنّ السبب التشريعي لإقرار حق سلطة التّحقيق في التفتيش المعلوماتي هو الحصول على دليل في جريمة تحقّق وقوعها و إجازة اللّجوء إلى هذه الوسيلة القسرية لمجرد احتمال وقوع الجرائم بدون تحديدها، يعتبر في اعتقادنا نوعا من التّعدي و الإفتئات على حقوق الأفراد و حرمة معلوماتهم و مخالف لمبدأ التناسب و الضّرورة، مما يتطلب مراجعة هذا النصّ الإجرائي في ضوء الإنتقادات الموجهة إليه.

ثانيا: نوع الجريمة

باعتبار أنّ التفتيش المعلوماتي يمثل إنتهاكا خطيرا للحق في الخصوصية، فإنّه كان لزاما أن تتميز الجريمة التي يقدر اللّجوء إليه بخطورة معينة كي يمكن الإستعانة بمثل هذا الإجراء الإستثنائي، بحصر نطاق التفتيش في الجنايات و الجنح، أمّا المخالفات فليس في وقوعها ما يبرّر مباشرة التفتيش لأنّها ليست من الأهمية بالقدر الذي يسمح بالتعرض للحرية

الشخصية أو إنتهاك لمسكن، و هذا الإستبعاد قد يكون صراحة مثل قانون الإجراءات الجنائية المصري⁽¹⁾، و قد يرد النص عليه ضمنا كما هو حاصل في التشريع الفرنسي⁽²⁾.

أما المشرع الجزائري فقد أجاز اللجوء إلى التفتيش المادي في الجرح و الجنايات و هذه النتيجة تثير لدينا تساؤلا فيما إذا كان جواز اللجوء إلى التفتيش المعلوماتي قاصرا فقط على التحقيق في الجرائم المعلوماتية أم يشمل جميع الجرائم بدون استثناء؟

أجاب المشرع الجزائري على هذا التساؤل بشكل مباشر و صريح ضمن المادة الثالثة من القانون رقم 04-09 المتضمن القواعد الخاصة للحماية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها، و التي وردت عامة تحت عنوان "مجال التطبيق"، جاء فيها "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات و الإتصالات يمكن لمقتضيات حماية النظام لعام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجنائية و في هذا القانون، وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية و تجميع و تسجيل محتواها في حينها و القيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية".

و يستمد من هذه النصوص أنّ المشرع لم يحصر مجال أعمال هذا الإجراء ضمن دائرة الجرائم المعلوماتية فحسب، بل أنّ نطاقه يشمل جميع الجرائم تقليدية كانت أم معلوماتية على حد سواء، فالموضع الذي تخيره المشرع للنص على حالات اللجوء إلى التفتيش المعلوماتي جاء عاما في صورة قاطعة، و ذلك على خلاف حالات جواز اللجوء إلى التفتيش المعلوماتي لمنع وقوع الجرائم الذي لا يجوز لسلطة التحقيق اللجوء إليه إلا في حالات استثنائية لم يوفق المشرع في تعدادها ضمن نص المادة الرابعة من نفس القانون.

(1) المادة 91 من قانون الإجراءات الجنائية المصري (معدلة بالقانون رقم 37 لسنة 1972 - الجريدة الرسمية - عدد رقم 39 الصادر في 1972/9/28) تنص تفتيش المنازل عمل من أعمال التحقيق ولا يجوز الإلتجاء إليه إلا بمقتضى أمر من قاضي التحقيق بناء على إتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جنابة أو جنحة أو باشتراكه في ارتكابها أو إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة و لقاضي التحقيق أن يفتش أي مكان و يضبط فيه الأوراق و الأسلحة و كل ما يحتمل أنه استعمال في ارتكاب الجريمة أو نتج عنها أو وقعت عليه و كل ما يفيد في كشف الحقيقة، و في جميع الأحوال يجب أن يكون أمر التفتيش مسببا".

(2) و يسفاد ذلك من خلال نصوص المواد التي خصت قاضي التحقيق بصلاحيه إصدار إذن التفتيش و إختصاص القاضي بحسب هذا القانون بالتحقيق يكون قاصرا بصفة أساسية على الجنايات و أحيانا الجرح.

على أنّ الملاحظ في هذا الصدد أنّ المشرّع أشار ضمن المادة الثانية من هذا القانون إلى المقصود بالجرائم المتّصلة بتكنولوجيات الإعلام و الإتصال - و التي يفترض أن يكون هذا القانون قد إستهدف الوقاية منها و مكافحتها- على أنّها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحدّدة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونيّة"⁽¹⁾، و مؤدى ذلك أنّه يخرج من نطاق التّطبيق الجرائم التي لا يعتمد في ارتكابها على نظم المعلومات و في ذلك تناقض صارخ بين المادة الثانية و المادة الثالثة من نفس القانون.

فعموم نص المادة الثالثة لا يصح تخصيصه بالمادة الثانية و دليلنا في ذلك أنّه يصح الإستناد إلى فئات معينة من الأدلة المعلوماتية لبناء هيكل الإدانة أو البراءة في جرائم تقليدية بحته لم يتم الإستعانة في التّحضير لها أو تنفيذها بالمعلوماتية نهائياً، و أهمّ مثال على ذلك الأدلة المعلوماتية المتعلّقة بالتّحديد الجغرافي لموقع المتّهم بتاريخ ارتكاب الجريمة، تعتبر من بين أهمّ الأدلة المعلوماتية التي لا تتقطع المحاكم في الإعتماد عليها لكشف الحقيقة في الجرائم الأكثر خطورة كالقتل و الحريق و السرقة، دون أن يكون الجاني قد لجأ إلى إستخدام النظام المعلوماتي في تحقيق فعله الجرمي.

و من ثمّ فإنّه لم يعد من سائغ الإبقاء على الفقرة (أ) من المادة الثانية لأنّها تشكّل وجهاً من أوجه التّضخم التشريعي، فليس هناك أيّ فائدة ترجى من هذا التّعريف لأنّ المشرّع ذاته لم يعتمد في ما أرساه من أحكام إجرائية يفترض أن ترتبط بالجريمة المعرّفة فحسب، لذا يتعيّن حذفها توجّهاً من تعارض النصوص القانونية.

الواقع أنّ مثل هذه النتيجة تفضي إلى طرح تساؤل لا ينعقد من مبدأ التّناسب في الحفاظ على الحرّيات الفردية عند التّقيب على الدليل المعلوماتي، فيما إذا كان المشرّع قد ضيق من نطاق تفتيش "بيانات المحتوى" على الجرائم الخطيرة فقط، بحسبان أنّ هذه الفئة من البيانات تكشف عن خبيئة الفرد بشكل مباشر؟

(1) و هو ما يستفاد بشكل واضح من خلال أحكام المرسوم الرئاسي رقم 19-172 مؤرخ في 06 جوان 2019 يحدّد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها و تنظيمها و كفاءات سيرها (جريدة رسمية رقم 37 لسنة 2019) و الذي بمقتضاه ألغي المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 الذي يحدّد تشكيلة و تنظيم و كفاءات سير الهيئة الوطنية للوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها (جريدة رسمية عدد 53 لسنة 2015).

لا مرأى في أنّ جميع فئات البيانات المعلوماتية سواء "بيانات المرور" أو "بيانات المحتوى" أو "بيانات المشتركين" هي بيانات ذات طابع شخصي، غير أنّ درجة ارتباطها بالخصوصية تختلف من فئة لأخرى و تشكل فئة "بيانات المحتوى" الفئة الأكثر التصاقاً بالحق في الخصوصية مقارنة بغيرها من البيانات، بحيث يجب أن يخضع تفتيشها لمتطلبات أكثر صرامة في ضوء متطلبات مبدأ التناسب والضرورة على نحو لا يجوز تفتيش بيانات المحتوى إلا إذا بلغت الجريمة قدراً من الخطورة تبرّر إنتهاك حرمتها، بما يقيم توازناً بين فاعلية العدالة الجنائية و ضمان الحرّية الشخصية.

و يبدو أنّ المشرّع الجزائري لم يراع مبدأ التناسب بين هذه الوسيلة الإجرائية و غايتها إذ يتيح لسلطة التحقيق تفتيش "بيانات المحتوى" أيّا كانت ضالّة الجريمة من حيث درجة خطورتها على الهيئة الإجتماعية، و ليس في القانون ما يعالج هذه المسألة فهي تخضع للقاعدة العامة المنصوص عليها بالمادة 5 من القانون 09-04، و في ذلك ميل واضح نحو اعتبارات الفعالية على حساب الشرعية، و ما يؤسف له أنّ أغلبية الفقه تؤيد هذا التوجه و ترفض أشكال التمييز بين مختلف أنواع الأدلة المعلوماتية بشأن ضمانات التفتيش عنها⁽¹⁾.

(1) تميّز التشريعات الإجرائية في أحيان كثيرة بين جمع محتوى اتصال ما، من جانب، والبيانات المتعلقة بالاتصال، أو البيانات الوصفية، من الجانب الآخر، مع خضوع الحالة الأولى ل ضمانات أقوى من الضمانات التي تخضع لها الحالة الأخيرة. إلا أنّه يجب التخلّي تماماً عن أشكال التمييز هذه، إذ أنّها تعكس فهماً بالياً لطبيعة الاتصالات التي تُجرى الآن و فشلاً في تحديث القوانين بناءً على ذلك. فأشكال التمييز هذه تعود إلى عصر كان يُميّز فيه بين الظرف الذي توضع به الرسالة و محتوى هذا الظرف، في حين أنّه عند النظر إلى الاتصالات الرقمية فإنّ ما يُسمى بالظرف، أو البيانات الوصفية، تتضمن معلومات حساسة و قيّمة و وفيرة جداً. فمثلاً، من الممكن أن تُستمد تلك المعلومات من البيانات الوصفية و أن تُحلّل من أجل الحصول على معلومات عن المعتقدات السياسية أو الدينية للشخص. و في دراسة أجرتها جامعة ستانفورد بيّنت أنّ من الممكن الحصول على معلومات طبية و مالية و قانونية من البيانات الوصفية، بناءً على ذلك، ينبغي إعادة النظر في ذلك التمييز.

يراجع بهذا الخصوص: مجلس حقوق الإنسان، الدورة الثامنة و العشرون التقرير السنوي لمفوض الأمم المتحدة السامي لحقوق الإنسان و تقارير المفوضية السامية و الأمين العام، موجز حلقة نقاش مجلس حقوق الإنسان المتعلقة بالحق في الخصوصية في العصر الرقمي وثيقة رقم A/HRC/28/39 بتاريخ 19 ديسمبر 2014، ص 12، فقرة 28.

الفرع الثاني: إتهام شخص بارتكاب جريمة أو الإشتراك فيها

و هذا الشرط يتصل كذلك بتكليف التفتيش بأنه "عمل تحقيق"، و يقتضي ذلك أن يجري في نطاق تحقيق حتى يتخذ موضعه فيه⁽¹⁾، لهذا يشترط لقيام سبب التفتيش المعلوماتي إلى جانب تحقق وقوع جريمة معينة، أن تتوفر في حق المراد تفتيش نظمه المعلوماتية دلائل كافية تؤدي إلى الإعتقاد بأنه قد أسهم في ارتكاب الجريمة بصفته فاعلا أو شريكا⁽²⁾، و لا يكفي أن توجه التهمة إلى أي شخص معين، بل يجب أن يكون الاتهام جديا و قامت من الدلائل ما يكفي لانتهاك حق الخصوصية لديه⁽³⁾، و هو الشرط مستفاد ضمنا من نص المادة 79 من قانون الإجراءات الجزائية التي وردت في باب "جهات التحقيق"، و معنى ذلك أنه لا يجوز اللجوء إلى التفتيش بشكل عام سواء كان مادي أو معلوماتي إلا في تحقيق مفتوح.

أما التشريع المصري فقد كان يسلك نفس مسلك التشريع الجزائري بصريح نص المادة 91 من قانون الإجراءات الجنائية التي تقرّر بأن "تفتيش المنازل عمل من أعمال التحقيق لا يجوز الإلتجاء إلى التفتيش إلا في تحقيق مفتوح"، مما يعني أنه يجب أن يكون التحقيق قد بدأ و اتخذت بعض إجراءاته قبل الأمر بالتفتيش، و لكن القضاء قد فسّر هذا الشرط تفسيراً ضيقاً من نطاقه⁽⁴⁾، فأجاز لصحة مباشرة إجراءات التفتيش أن يفتح التحقيق و لو بإتخاذ إجراء واحد يسبق الأمر به، ثم لجأ المشرع المصري إلى إلغاء هذا الشرط لاعتبارات عميلة⁽¹⁾.

(1) لقد أحسن المشرع البحريني في صياغة قاعدة تطبيق مجال الإجراءات الجزائية المعلوماتية في المادة 11 من القانون رقم 60 لسنة 2014 حيث نصت: "تسري أحكام هذا الفصل على ما يلي:

(أ) الجرائم المنصوص عليها في الفصل الأول من هذا القانون.

(ب) الجرائم المنصوص عليها في أي قانون آخر إذا ارتكبت باستخدام نظام تقنية المعلومات.

(ج) جمع الأدلة التي تكون في صورة إلكترونية والمتعلقة بأية جريمة."

(2) أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، مجلة البحوث الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، المجلد 29 العدد 58، نوفمبر 2013، ص 98.

(3) علي حسن محمد الطويلة، مرجع سابق، ص 70.

(4) حيث أكدت محكمة النقض المصرية ذلك بقولها "إن قضاء محكمة النقض مستقر على أن تفتيش المنازل إجراء من إجراءات التحقيق لا تأمر به سلطة من سلطاته إلا بمناسبة جريمة ترى أنها وقعت و صححت نسبتها إلى شخص بعينه و أن هنالك من الدلائل ما يكفي لاقتحام مسكنه الذي كفل الدستور حرمة و حرم القانون على رجال السلطة دخوله إلا في أحوال خاصة، و أن تقدير كفاية تلك الدلائل و إن كان من شؤون سلطة التحقيق إلا أنه خاضع لرقابة محكمة الموضوع بحيث إذا رأت أنه لم يكن هناك ما يبرره فإنها لا تأخذ بالدليل المستمد منه باعتبار

و لا يتصور التخلي عن هذا القيد الإجرائي في التشريع الجزائري لكون قضاء التحقيق هو الجهة الوحيدة المخولة بذلك، و هذا لا يمنع من اعتبار الأمر بالتفتيش في حد ذاته فتحاً للتحقيق بغية المسارعة في تنفيذ التفتيش منعا من حذف الدليل المعلوماتي أو تعديله بفعل التراخي في التنفيذ.

الفرع الثالث: توافر الدلائل الكافية

الدلائل الكافية شرط ضروري لاتخاذ أي إجراء يتضمن مساسا بحرمة النظام المعلوماتي أو أي إجراء آخر ينطوي على انتهاك للحريات الفردية، و هي بمثابة شرط وقائي يقي الفرد من الوقوع ضحية إجراء تعسفي، لذلك لا يجوز الإلتجاء إليه إلا إذا وجد ما يبرره، و الذي يبرر انتهاك حرمة النظام المعلوماتي في نظر المشرع هو وجود قرائن جديده على ضرورة التفتيش لصالح الإثبات الجنائي المعلوماتي لتبرير مشروعية التفتيش، فالرابطه الإجرائية التي تنتقر بمجرد الاتهام إنما تعني في حقيقتها وجود طرفين هما: المتهم و النيابة، و لكل منهما حقوق و عليه واجبات، فلا يجوز بالتالي اعتبار المتهم عبدا ذليلا للنيابة تفعل به ما تشاء دون شرط أو قيد، فلا يصح بقاؤها حرة طليقة اتجاهه، بكل ما لديها من سلطات و إنما لا بد من تقييدها في حدود القانون⁽²⁾، و هو ما يؤسس لعدم جواز اتخاذ إجراء جنائي يقيد الحرية الفردية إلا بوجود توافر دلائل كافية من شأنها أن تبرر اتخاذه.

أنه إذا فقد المبرر لإجرائه أصبح عملاً يجرمه القانون فلا يسوغ أن يؤخذ بدليل مستمد منه و إذا كان الشارع قد نص على أن يكون هناك تحقيق مفتوح فإتما قصد بذلك التحقيق الذي تتولاه سلطة التحقيق و لم يشترط الشارع للتحقيق المفتوح الذي يسوغ التفتيش أن يكون قد قطع مرحلة أو استظهر قدراً معيناً من أدلة الإثبات بل ترك ذلك لتقدير سلطة التحقيق لكي لا يكون من وراء غل يدها احتمال فوات الغرض منه مما تتأثر به مصلحة الجماعة، التي تسمو على مصلحة الفرد". الطعن رقم 1265 لسنة 22 مكتب فني 04 صفحة رقم 909.

(¹) وقد جاء في المذكرة الإيضاحية للقانون المصري رقم 43 لسنة 1958 الذي أدخل هذا التعديل أن اشتراط إجراء تحقيق على هذا الوضع قبل أن تجري سلطة التحقيق التفتيش بنفسها، أو تأذن لأحد مأموري الضبط القضائي بإجرائه قد يضرر بالمصلحة العامة التي يجب أن تسمو على مصلحة الفرد، لأنه قد يعطل من سير الإجراءات خصوصاً في الأحوال التي لا تحتمل التأخير، وقد يؤدي طول الإجراءات إلى إذاعة خبر التفتيش قبل إجرائه، و ليس فيه ضمانه جديدة، ما دام تقدير مبررات التفتيش متروك لسلطة التحقيق تحت إشراف المحكمة". مشار إليه لدى: محمود نجيب حسني، المرجع السابق، ص 598.

(²) أشرف محمد عبد القادر سمحان، القواعد الناظمة لسلطة تقدير الدلائل الكافية (الجزء الأول)، مجلة كلية القانونية الكويتية العالمية، الكويت، السنة 4، العدد 1، مارس 2019، ص 287.

و مفهوم كفاية الدلائل، مفهوم غير منضبط فهو يتيح المجال لممارسة الجهة المختصة سلطاتها بموجب قانون الإجراءات الجزائية بشكل تحكمي الأمر الذي يدعو إلى تعسف السلطة، حتى قد ذهب البعض إلى وصف مفهوم الدلائل الكافية بأنه مفهوم غير محدد الأمر الذي يجعله قاصراً عن تحقيق الغاية منها، كما وصف مفهوم الدلائل الكافية بأنه فكرة مرنة تستعصي على التحديد المجرد مقدماً، فهي أمر نسبي تختلف باختلاف الجرائم كما تختلف باختلاف الزمان و المكان، إلا أنه و لما كانت روح القانون و اعتبارات العدالة تتأبي على كل ما هو تحكمي و غير منضبط كان لزاماً البحث في مدى إمكانية وضع معايير موضوعية تضبط قدر الإمكان - مثل هذه السلطة التقديرية⁽¹⁾، لوزن مدى كفاية الأدلة لاتخاذ إجراءات التفتيش المعلوماتي.

عموما يقصد بالدلائل الكافية، العلامات الخارجية أو الشبهات المعقولة، دون ضرورة التعمق في تمحيصها، و تغليب وجوه الرأي فيها، أو هي أمارات معينة تستند إلى العقل، و تبدأ من ظروف أو وقائع يستنتج منها الفعل، توحى للوهلة الأولى بأن جريمة ما قد وقعت، و أنّ شخصاً معيناً هو مرتكبها⁽²⁾، و ليس معنى اشتراط وجود قرائن تبرّر التفتيش المعلوماتي أن تتوافر أدلة قاطعة على وجود ما يفيد التحقيق في المحل المراد تفتيشه بل يكفي لذلك وجود دلائل جدية، فهي قرائن ضعيفة، قد لا تصلح وحدها سببا للإدانة فهي ذلك القدر الضئيل المبني على احتمال معقول تؤيده الظروف التي تكفي للاعتقاد بارتكاب جريمة و لكنها تبرّر اتخاذ بعض الإجراءات الماسة بالحريّة الفردية ضمانا لحسن سير العدالة⁽³⁾.

و من البديهي أنّ السبب يسبق المسبب، فالقرائن المبررة للتفتيش المعلوماتي باعتبارها سببا له يجب أن يكون سابقة عليه، فوجود القرائن المبررة للتفتيش يجب الحكم عليه قبل بدء التفتيش و لا يجوز أن يكون لنتيجة التفتيش النهائية أي أثر في ذلك، فإذا أسفر التفتيش عن عدم وجود أي شيء فلا يكفي ذلك للقول فإّنه قبل إجرائه لم تكن توجد دلائل جدية تبرّر

(1) رمسيس بهنام، الإجراءات الجنائية تأصيلا و تحليلا، الجزء الأول، بدون رقم الطبعة، منشأة المعارف، مصر، 1977، ص 159.

(2) هلاي عبد الله أحمد، "المركز القانوني للمتهم في مرحلة التحقيق الابتدائي - دراسة مقارنة بالفكر الجنائي الإسلامي"، الطبعة الثانية، دار النهضة العربية، مصر، 1988، ص 51.

(3) عبد الحميد الشوربي، إذن التفتيش في ضوء الفقه و القضاء، بدون رقم الطبعة، منشأة المعارف، مصر، 1988، ص 21.

التفتيش، و على العكس من ذلك يكون التفتيش باطلا إذ لم يكن للمحقق وقت إجرائه قد حصل فعلا على قرائن تبرّره، و لا يمنع هذا البطلان أن يسفر التفتيش فعلا عن وجود أشياء تفيد التحقيق، فنتيجة التفتيش لا يجوز أن تتدخل في تقدير وجود الأسباب له أو عدم وجودها⁽¹⁾.

واقع الأمر أنّ المشرّع الجزائري لم يورد نصا صريحا على ضرورة وجود قرائن كافية لمشروعية التفتيش سواء التفتيش المادي أو المعلوماتي، و لكن هذا الشرط مستوحى في اعتقادنا من نص المادة 44 من قانون الإجراءات الجزائية التي قرّرت بأنه "لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنّهم ساهموا في الجناية أو أنّهم يحوزون أوراقا أو أشياء متعلقة بالأفعال الجنائية المرتكبة لإجراء تفتيش...".

إذ تفيد عبارة " يظهر... أنّهم يحوزون" على ضرورة قيام قرائن كافية تتحقّق الاعتقاد المنطقي بوجود ما يفيد إظهار الحقيقة في المكان أو الشيء المراد إخضاعه للتفتيش، و إن كان المشرّع قد اشترط ضرورة توافر أمانة قوية على إخفاء أو حيازة أشياء تفيد في كشف الحقيقة لمشروعية التفتيش في حالة التلبس، فإنّه من البديهي و من باب أولى ضرورة قيام هذا الشرط في الأحوال العادية⁽²⁾.

أمّا التشريع الأمريكي فإنّه أولى اهتماما بالغا لهذا الضابط الإجرائي إذ أصبح عليه طابعا دستوريا، كما يقطع بذلك التعديل الدستوري الرابع بقوله "لا يجوز المساس بحق الأفراد في أن يكونوا آمنين في أشخاصهم و منازلهم و مستنداتهم و مقتنياتهم ضد عمليات التفتيش

(1) توفيق محمد الشاوي، المرجع السابق، ص 199.

(2) أمّا بالنسبة للتشريعات العربية فقد عالجت هذا القيد بموجب نصوص صريحة قاطعة الدلالة و مثال ذلك ما نصّت عليه المادة 75 من قانون رقم (23) لسنة 2004 بإصدار قانون الإجراءات الجنائية القطري (الجريدة الرسمية عدد 12 بتاريخ 2004/08/29) تنص "تفتيش المنازل عمل من أعمال التحقيق، لا يجوز إلا بإذن كتابي من النيابة العامة بناءً على تحريات تكشف أنّ حائز المسكن أو المقيم فيه ارتكب جناية أو جنحة أو إشتراك في ارتكابها أو وجدت قرائن تدل على أنّه حائز لأشياء تتعلّق بالجريمة. و يجوز أن ينصرف الإذن إلى كل مسكن يحوزه المتّهم أو يقيم فيه و لو بصفة غير دائمة. و يكون التفتيش لضبط الأشياء المستعملة في ارتكاب الجريمة أو التي وقعت عليها أو نتجت عنها و كل ما يفيد في كشف الحقيقة. و لعضو النيابة العامة أن يفتش المتّهم. و لا يجوز له تفتيش غير المتّهم أو مسكنه، إلا إذا اتضح من إمارات قوية أنّه حائز لأشياء تفيد في كشف الحقيقة". و المادة 94 من قانون الإجراءات الجنائية المصري "لقاضي التحقيق أن يفتش المتّهم، و له أن يفتش غير المتّهم إذا اتضح من إمارات قوية أنّه يخفي أشياء تفيد في كشف الحقيقة. و يراعى في التفتيش حكم الفقرة الثمانية من المادة 46".

و الضبط غير المعقولة، و لا يجوز إصدار إذن بهذا الخصوص إلا على أساس وجود سبب معقول مدعوم بالقسم أو التوكيد بحيث يصف هذا الإذن بدقة المكان المقصود تفتيشه و الأفراد و الأشياء المراد ضبطها⁽¹⁾.

و قد عبّر عنه بمصطلح السبب الرّاجح أو السبب المعقول Probable Cause و الذي استهدف من خلاله توفير حماية للأفراد ضد التفتيش التعسفي أو ذاك الذي لا يوجد له مبرر، إذ أنّ المشرّع الدستوري قيد صدور الإذن بالتفتيش المعلوماتي بوجود أو ظهور السبب الرّاجح و الذي يدعو للإعتقاد بأنّ مبررات إصدار الإذن موجودة، و مع ذلك لم يتعرّض هذا المشرّع لتفسير و تحديد مفهوم السبب الرّاجح على الرّغم من وضع هذا القيد على سلطة إصدار الإذن بوجود مثل هذا السبب، إلا أنّ التحليل الدقيق لصياغة هذا التعديل يمكن أن يفسّر هذا المصطلح على اعتبار أنّه باسْتِطْرَاط أن يكون له وجود، فإنّ ذلك يعني الإشارة إلى أفعال أو وقائع واضحة و ظاهرة و موثوق بها أو يعول عليها بحيث يتولّد عنها الاعتقاد المنطقي بأنّ الجريمة قد تمّ ارتكابها و هو ما يمثّل الشرط المفترض و الذي يتعيّن أن يتحقّق في المرحلة السابقة عن صدور الإذن⁽²⁾.

و من الأهميّة التّقرير بأن تطلب السبب المعقول لا يلزم أعضاء السّلطة الإجرائية بأن يكونوا من ذوي البصيرة و الإدراك لتحديد شكل الدليل أو الشّيء المجرّم الذي سوف يتواجد في المكان المراد تفتيشه فعلى سبيل المثال لا يحتاج أعضاء الضبطية القضائية إلى سبب معقول ليعتقدوا بأنّ الدليل المقصود بالبحث سوف يكون موجودا في شكل معلومات على الحاسوب، و بالمثل فهم لا يحتاجون إلى معرفة أيّ انتهاك للقانون سوف يكشف عنه الدليل، كما أنّهم في غير حاجة إلى معرفة من الذي يملك الشّيء المطلوب ضبطه و تفتيشه، إذ

(¹) U.S. CONST. amend. IV:

«The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized».

(²) حسام الدين محمد أحمد، المرجع السابق، ص 80.

يتطلب معيار السبب الراجح بساطة من الضبطية القضائية إقامة احتمال معقول يدل على أنّ الشّيء المجرّم أو دليل الجريمة يتواجد في المكان المعين المراد تفتيشه⁽¹⁾.

و من بين أهمّ تحديات السبب المعقول التي تواجه التفتيش المعلوماتي تظهر غالباً عندما يكون الدليل المدعوم بالإفادة الخطية (طلب الإذن) مأخوذاً بكثرة من سجلات حساب معيّن على الأنترنت **internet account** أو بروتوكول **internet protocol IP** أنترنت و المشكلة هنا هي مشكلة عملية بشكل عام، فالحقيقة أنّه إذا كان هناك حساب ما أو عنوان ما قد تمّ استخدامه فإنّه لا تتحدّد بشكل نهائي هوية أو موقع الشّخص المعين الذي استخدمه، و نتيجة لذلك فإنّ الإفادة الخطية المبنية بشكل كبير على حساب أو عنوان بروتوكول أنترنت يجب أن تبرّر الصّلة الكافية بين العنوان و المكان المراد تفتيشه⁽²⁾.

و تقدير الدلائل و مبلغ كفايتها يكون بدءاً للضبطية القضائية على أن يكون تقديره هذا خاضعاً لرقابة سلطة التحقيق، تحت إشراف محكمة الموضوع⁽³⁾، و يترتّب على إغفال هذا الشرط بطلان التفتيش و لو أسفر التفتيش فعلاً عن الدليل المستهدف⁽⁴⁾، فشرط وجود سبب

(1) عمر محمد بن يونس، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي المرشد الفيدرالي الأمريكي لتفتيش و ضبط الحواسيب توصلاً إلى الدليل الإلكتروني في التّحقيقات الجنائية، المرجع السابق، ص ص 234-235.

(2) المرجع نفسه، ص 235.

(3) سامي حسني الحسيني، المرجع السابق، ص 198.

(4) و قد قررت محكمة النقض المصرية في الكثير من قراراتها بطلان التفتيش جزاء مخالفة هذا الشرط و قد جاء في أحد أشهر أحكامها: "لما كان الحكم المطعون فيه قد قضى ببراءة المطعون ضده و بصحة الدّفع ببطلان التفتيش قائلاً في تسيب قضائه ما نصه "و إذ كان ما تضمنه المحضر المحرّر بطلب الإذن بالتفتيش لم يتضمّن من الدلائل و الإمارات ما يقنع المحكمة بجديّة الإستدلالات التي بني عليها أمر التفتيش أو كفايتها لتسويغ إصداره و آية ذلك ما قرره مستصدر الإذن بالتّحقيقات من أنّ التّحرّيات التي قام بها بنفسه أكّدت أنّ المتّهم يتاجر في مادة ماكستون فورت و أنّ المدمنين يتردّدون عليه لتعاطيها في الوقت الذي لم يذكر شيئاً عن ذلك في محضره مكتفياً بإطلاق المادة التي زعم أنّ المتّهم يتاجر فيها و هي المواد المخدرة دون ترخيص أو تحديد و الفرق بين الإتجار في المواد المخدرة و إعطاء حقنة الديكسا فيتامين واضح و بيّن، و لو صحّ ما زعمه الضّابط بشأن تحرياته لأثبتها في محضره و هو الأمر الذي يشكك المحكمة في صحة قيام هذه التّحرّيات و يجردها من صفة الجديّة. و لا يقدر في ذلك أنّ سلطة التّحقيق صاحبة الحق في إصدار الأمر بالتفتيش قد قرّرت جديّة هذه التّحرّيات، إذ أنّ ذلك خاضع لرقابة محكمة الموضوع باعتبارها الرّقابية على قيام المسوّغات التي تراها سلطة التّحقيق مبرّرة لإصدار الأمر بالتفتيش، و من ثمّ فإنّ إذن التفتيش الصّادر بالبناء على هذه التّحرّيات يكون باطلاً). الطّعن رقم 640 لسنة 47 جلسة 06/11/1977 س 28 ع 1 ص 914 ق 19، مشار إليه لدى مجدي محب حافظ، إذن التفتيش دراسة تحليلية تطبيقية في التّشريع

التفتيش مسألة قانونية من اختصاص محكمة العليا الإشراف عليها، أما كفاية السبب أو بعبارة أدق تقدير قيمة القرائن التي إستند إليها المحقق في القول بأن هنا جريمة و أنّ إجراء التفتيش ضروري للتحقيق فيها فهي مسألة من اختصاص محكمة الموضوع وحدها و لا تجوز المجادلة فيها أمام محكمة النقض⁽¹⁾.

في الحقيقة فإنّ هذا الضمان الذي يفترض به أن يشكّل سبباً يقي الأفراد من الوقوع ضحايا لتفتيش معلوماتي يمكن أن يكون تعسفياً، قد عجز القانون و القضاء و الفقه إلى غاية اليوم عن إيجاد معيار ثابت يهتدي به لتحديد مدى تحقّقه لمشروعية التفتيش من عدمه، فبقي خاضعاً للسلطة التقديرية لقاضي التحقيق، دون تحديد دقيق لضوابطه، مما يجعله قاصراً أحياناً عن تحقيق الغاية منه، خاصة في الأحوال التي يتمّ فيها تنفيذ التفتيش و يؤول فيه إلى عدم الجدوى، إذ تصبح الرقابة القضائية اللاحقة بدون فائدة ترجى منها بعد تحقّق الانتهاك الفعلي لحق الفرد في خصوصيته دون وجود مبرر مسبق يدعو إلى إتخاذ هذا التدبير.

غير أنّ القيمة الفعلية لهذا الضابط الإجرائي تتحقّق من جانب آخر و هي ضمان عدم تجاوز الغاية من التفتيش المعلوماتي، فطالما أنّ التفتيش قد أجزى لضرورة التحقيق و جب لزاماً أن يكون محدوداً بحدود الضرورة التي برّرت و هي كشف الحقيقة في جريمة معينة، و استهداف هذه الغاية هو علة مشروعية التفتيش المعلوماتي و هو أهم ضمان تقوم عليه نظرية التفتيش، منعا من امتداد التفتيش المعلوماتي إلى محل آخر يتجاوز حدود سبب التفتيش، و هو ما يحيلنا إلى معالجة الركن الجوهرية الثاني لهذا العمل الإجرائي و هو التحديد الدقيق لمحل التفتيش المعلوماتي.

المطلب الثاني: المحل

محل التفتيش هو المستودع الذي يحفظ فيه الفرد أسراره، و حماية لحرمة لا يوجب القانون أن يكون محل التفتيش محدّداً منعا من التفتيش الاستكشافي فحسب، بل يشترط أيضاً أن يكون هذا المحل مما يجوز تفتيشه، من هذا المنطلق و جب علينا تحديد المقصود بالمحل (فرع أول)، و بيان المتطلبات الكافية لتحديده (فرع ثاني)، و كذا مشروعيته (فرع ثالث).

المصري و التشريعات العربية و التشريع المقارن في ضوء الفقه و أحكام القضاء في مائة عام، بدون رقم الطبعة، دار النهضة العربية، 2001، ص ص 101-102.

(1) توفيق محمد الشاوي، المرجع السابق، 208.

الفرع الأول: المقصود بمحل التفتيش المعلوماتي

يثور التساؤل في ضوء هذا الضابط الإجرائي عن "الشيء" الذي يقتضي لصحة الإذن أن يحدده "محلا للتفتيش"؟ هل يحدّد "أجهزة التخزين الرقمية" المراد ضبطها في مرحلة التفتيش المادي؟ أم "المعلومات" المراد استردادها في مرحلة التفتيش المعلوماتي؟ وإذا كان القانون يشترط لزوم تحديد مكان التفتيش فهل المقصود هنا تحديد "مكان الأجهزة المادية" أم "مكان البيانات من مساحة التخزين الرقمية"؟ والإجابة على ذلك تقتضي التطرق إلى مفهوم محل التفتيش (أولا)، و بيان الإشكاليات التي يثيرها هذا المفهوم في البيئة الرقمية (ثانيا).

أولا: مفهوم محل التفتيش

إنّ القانون إذ أجاز إنتهاك الحرمة لمصلحة التحقيق، فإنما يجيز ذلك بالنسبة لمحل معيّن و محدّد، و تعيين محل التفتيش معناه وجود رابطة محددة بين التفتيش و غايته و بين المحل الذي يراد إجراؤه فيه، فالقرائن التي تدل على أنّ هناك أشياء تفيد التحقيق لا تكفي لتبرير التفتيش إلاّ إذا حدّدت المحل الذي ترجح وجود هذه الأشياء فيه و متى تحدّد هذا المحل جاز تفتيشه⁽¹⁾، و معنى ما تقدم أنّ التفتيش العام يعتبر غير مشروع و يترتب عنه البطلان التفتيش مع استبعاد الدليل المعلوماتي المستمد منه⁽²⁾.

و قد ذهب البعض إلى أنّه إذا لم يؤدّ التفتيش "الخاص" إلى نتيجة ما، استطاع المحقّق أن يأمر بتفتيش عام في جميع منازل حي معيّن أو جهة معيّنة و ظاهر أنّ هذا القول لا يتفق

(1) توفيق محمد الشاوي، المرجع السابق، 287.

(2) و هذا ما تراه محكمة النقض المصرية وفقا لقضائها المتواتر " أن إجراء تفتيش المنازل على ما استقر عليه قضاء محكمة النقض إجراء من إجراءات التحقيق لا تأمر به سلطة من سلطاته إلا لمناسبة جريمة جناية أو جنحة ترى أنّها وقعت و صحت نسبتها إلى شخص معيّن و أنّ هناك من الدلائل ما يكفي لاقتحام مسكنه الذي كفل الدستور حرمة و حرّم القانون على رجال السلطة دخوله إلاّ في أحوال خاصة، فيجب أن يكون تعيين الشخص المراد تفتيشه واضحا و محدّدا له تحديدا نافيا للجهالة وقت صدور الإذن، فإذا جاء الإذن الصادر من النيابة بإجراء التفتيش مجهلا خاليا من أيّة إشارة تحدّد الشخص المراد تفتيشه و البلدة التي يقع فيها منزله بل هو في عبارته العامة المجهلة يصلح لأن يوجّه ضد كل شخص يقيم في أي بلدة تجاور البلدة المذكورة بالإذن ما دام أنّ الأمر متروك للمرشد على ما يراه هو دون أيّ تحديد... فإنّه لا يكون إذنا جديا و يكون التفتيش الذي حصل على مقتضاه قد وقع باطلا لمخالفته الأصول المقررة للتفتيش، و يبطل تبعا الدليل المستمد منه." أنظر: الطعن رقم 1262 لسنة 28 جلسة 1959/11/03، صفحة رقم 852. مشار إليه لدى إيهاب عبد المطلب، موسوعة المخدرات، الطبعة التاسعة، المركز القومي للاصدارات القانونية، 2016، ص 48.

مع المقصود من التفتيش، فالتفتيش إجراء من إجراءات التحقيق و لا يجوز الإلتجاء إليه إلا بناء على تهمة موجهة إلى شخص معين بارتكاب جريمة، أو إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة، و هو ما يعني أنّ التفتيش ينبغي إجراؤه في محل معين، فليست منازل المواطنين جميعا مفتوحة أمام سلطات التحقيق و إنما تلك التي يشتبه في احتوائها على أدلة معينة⁽¹⁾.

و إذا كان لقاضي التحقيق أن يفتش أي مكان من أجل الكشف عن الحقيقة⁽²⁾، فلا يعني هذا أنه يملك إصدار أمر تفتيش عام لدى المواطنين في جهة معينة، إنما المقصود أنه يملك تفتيش أي مكان تتوفر في شأنه القرائن التي تبين احتواءه على أدلة تفيد في كشف الحقيقة، و بهذا المعنى فإن المكان الذي يجري قاضي التحقيق فيه تفتيشه يكون مكانا محددا سواء تعلق بالمتهم أو بغيره و على حد تعبير البعض فإن قاضي التحقيق "يملك تقدير القرائن التي تبرر إجراء التفتيش، لكن لا يعني أن سلطة التقدير مطلقة من كل قيد فهو لا يستطيع أن يذهب إلى حد تعميم الإتهام أو الشبهات على بلدة بأكملها أو حي بأكمله و إلا كان ذلك تعسفا"⁽³⁾، و محل التفتيش مرتبط بالغاية منه، فإذا لم يكن للتفتيش غاية يستهدفها أو أن يستهدف غاية غير ما حدده المشرع فهو مشوب بعيب "التعسف في استعمال سلطة"⁽⁴⁾.

إنّ إعمال هذه القواعد العتيدة لا يطرح أي إشكال في حالة التفتيش عن الأدلة المادية، و هذا صحيح لسببين أساسيين. أولاً، تتناسب هذه القواعد مع حقائق التفتيش عن الأدلة المادية، فعادة ما تتبّع عمليات التفتيش المادية التقليدية آلية التفتيش ثم الإسترجاع، بحيث يمكن تحديد الأدلة المادية عموما واسترجاعها من مكان مادي معين و خلال فترة وجيزة، إذ يسمح الإذن للضبطية القضائية بالدخول إلى الممتلكات المادية (المباني و السكنات) و تحديد موضعها ثم استرجاع الأدلة المحددة في الإذن القضائي، و السبب الثاني الذي تتناسب به هذه القواعد مع عمليات التفتيش عن الأدلة المادية، هي أنها تكفل حصول سلطة التحقيق على هذه الأدلة بطريقة ضيقة نسبيا تقلل من إنتهاك خصوصية المتهم، فهي ترسم حدودا

(1) سامي حسني الحسيني، المرجع السابق، ص 198.

(2) المادة 81 من قانون الإجراءات الجزائية الجزائري.

(3) توفيق محمد الشاوي، المرجع السابق، 208.

(4) محمود نجيب حسني، المرجع السابق، ص 602.

واضحة لعمل الضبطية القضائية عند تنفيذ إذن التفتيش، فشرط التحديد يصف المكان المراد تفتيشه على وجه التخصيص كشقة أو مبنى معين، و يشرح كيفية التنفيذ من خلال وصف الأشياء المراد ضبطها بما لا يسمح بالإطلاع العام بل مقيد بنطاق مستهدف التفتيش و غايته⁽¹⁾.

الواقع أن هذا المفهوم التقليدي لمحل التفتيش يثير تساؤلا محددًا مضمونه ما هو المقصود محل التفتيش المعلوماتي؟ هل وسائط التخزين الرقمية؟ أم البيانات التي تحتويها هذه الدعامات المادية؟ أم فقط جزء من النظام المعلوماتي ممثلًا في بعض الملفات و المجلدات؟

ثانياً) - إشكالية تحديد محل التفتيش المعلوماتي

تعدّ إشكالية تحديد محل التفتيش المعلوماتي من الإشكاليات العملية الهامة، لا تتوقف عند المنظور المزدوج لهذا المحل (أ)، بل تتعدى ذلك إلى إشكالية ارتباط هذا المحل في تحديده بمستهدف التفتيش في مرحلة التفتيش المادي (ب).

أ) - إشكالية المنظور المزدوج لمحل التفتيش المعلوماتي

من المنفق عليه أنّ محل التفتيش هو المكان الذي يجري التفتيش فيه، و لزوم قصره على مكان معين هو من مستلزمات طبيعته الإستثنائية، و هذا المبدأ محل استفسار متزايد حول مدلول محل التفتيش في البيئة الرقمية، باعتبار أنّ التفتيش يجري في مكان ممثل في "البيانات" و الذي لا يختلف بدوره عن مكان تواجد البيانات ذاتها و هي "الأجهزة المادية"⁽²⁾، فأيهما يوجب القانون تحديده كمحل للتفتيش؟ و بعبارة أخرى هل صدور إذن بالتفتيش عن

(1) Orin S. Kerr, Search Warrants in an Era of Digital Evidence, op cit, p 99.

(2) يرى جانب من الفقه الأمريكي أنه يمكن النظر إلى وسائط التخزين من زاويتين داخلية و أخرى خارجية، فوفقاً للمنظور الداخلي لوسيط التخزين الرقمي، فإنّ دعامة التخزين الرقمية (منظومة التخزين المعلوماتية) تمثل مجموعة من البيانات مجمعة ضمن ملفات حاسوبية أو وحدات أصغر كجدول البيانات، و أنّ هذه "الأشياء" مستقلة عن بعضها البعض و بذات الوقت منفصلة عن جهاز التخزين الرقمي، و التي 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 في نظره لا تعدو أن تكون مجرد مجموعات من البيانات، مرتبطة بشكل يجعلها لا تنفصل عن وسيلة التخزين و هي بهذا المعنى ليست "مكاناً" بل "شيئاً". حول إشكالية المنظور المزدوج لمحل التفتيش المعلوماتي مقارنة بالتفتيش عن بقية الأدلة المادية يراجع:

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

دليل معلوماتي معيّن، يجيز توسيع نطاق التفتيش إلى كافة البيانات التي يحتويها جهاز التخزين الرقمي؟ أم يقتصر نطاقه على ملف معيّن وجب تحديده في الإذن القضائي؟

لا يجمع القضاء الأمريكي على موقف موحد إزاء المشكلة محل البحث، حيث يعتمد جانب من الفقه "المنظور المادي" لوسيط التخزين الرقمي و ينادي بوجود التعامل مع وسائط التخزين كدليل مادي بحيث يعتبر القرص الصلب و ما في حكمه مجرد "شيء"، و ليس "مكانا"، أو بعبارة أخرى ينظر إليه في صورة "شيء واحد" على نحو لا يحتوي على أيّ أشياء أخرى ضمنه، شأنه شأن أيّ دليل مادي آخر يتمّ "فحصه" (تحليله) و ليس "تفتيشه"⁽¹⁾، بحيث يجوز التوسع في التفتيش عبر كافة مساحة وسيط التخزين الرقمي باعتبارها تشكّل وحدة واحدة، و من تطبيقات ذلك ما قضت به الدائرة الخامسة الفيدرالية في قضية **United States v. Runyan**، و تردّد ذات التبرير في قضية **United States . Slanina**⁽²⁾.

و قد اعتمد المشرّع الأمريكي المنظور المادي لمحل التفتيش المعلوماتي، و يتجلى ذلك من خلال نص المادة 41 من قانون الإجراءات الجنائية الفيدرالي التي تنظّم أحكام التفتيش المعلوماتي من خلال التعبير عن مقتضياتها وفقا لتصور مادي خالص، و تفترض أنّ عمليات التفتيش تجري في أمكنة "مادية"، و أنّ "الأشخاص" أو "الممتلكات" يتمّ تفتيشها و ضبطها، و عندما تناولت هذه المادة أخيرا وسائط التخزين الرقمي تمّ إتباع نهج مادي أيضا، و أوضحت التعديلات التي دخلت حيّز التنفيذ سنة 2009 أنّ محتويات وسائط التخزين "الملكية" لا تحتاج إلّا إلى وصف "وسائط التخزين الماديّة"، و لم تستلزم وصف و تحديد المعلومات، كما أضافت أنّ المدة الزمنية اللاّزمة لتنفيذ "الإذن" تتعلّق بالوقت اللاّزم لضبط وسائط التخزين أو نسخها، و ليس تفتيشها⁽³⁾.

و هو المسلك الذي سلكه مشروع إتفاقية الأمم المتحدة للتعاون في مكافحة الجريمة الإلكترونيّة بشكل صريح و واضح⁽⁴⁾، و هذا النهج له ما يسوّغه كما سنرى لاحقا عند معالجة

(¹) Ibid, p 117.

(²) عمر محمد بن يونس، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي المرشد الفيدرالي الأمريكي لتفتيش و ضبط الحواسيب توصلا إلى الدليل الإلكتروني في التّحقيقات الجنائية، المرجع السابق، ص 61.

(³) Josh Goldfoot, op cit , p 12.

(⁴) و في هذا الإطار تنص المادة 26 من مشروع اتفاقية الأمم المتحدة للتعاون في مكافحة الجريمة الإلكترونيّة " البحث عن البيانات الحاسوبية المحفوظة أو المعالجة و ضبطها.

متطلبات تحديد محل التفتيش المعلوماتي بين مرحلة التفتيش المادي و مرحلة التفتيش المعلوماتي.

و على عكس هذا المذهب، إتجه جانب آخر من الفقه في محاولة منه لتقليص نطاق امتداد التفتيش المعلوماتي إلى مطالبة القضاء بالتعامل مع ملفات القرص الصلب كمجموعة حاويات مغلقة و منفصلة، يتطلّب فحص كلّ حاوية إذنا مستقلا بتفتيشها. و بعبارة أخرى، ينبغي أن يُنظر إلى الحاسوب على أنّه الحاوية الماديّة مع سلسلة من "الحاويات" الإلكترونيّة الفرعية "Subcontainers"، و هي المجلدات و الملفات التي يقتضي الإطلاع عليها و

1 - تتخذ كلّ دولة طرف ما قد يلزم من تدابير تشريعية و تدابير أخرى لتمكين سلطاتها المختصة من السعي إلى الوصول في إقليم تلك الدولة الطرف إلى ما يلي:

(أ) أجهزة تكنولوجيا المعلومات و الاتصالات و البيانات الحاسوبية المخزّنة فيها.

(ب) وسائط تخزين البيانات الحاسوبية التي ربما خزّنت فيها البيانات الحاسوبية المطلوبة.

2- تتخذ كل دولة طرف ما قد يلزم من تدابير تشريعية و تدابير أخرى تكفل قدرة سلطاتها المختصة على أن تجري على وجه السرعة عملية بحث للوصول إلى جهاز تكنولوجيا المعلومات والاتصالات الآخر إذا كان لدى هذه السلطات، التي تجري بحثاً وفق أحكام الفقرة 1 (أ) من هذه المادة، أسباب تدعو إلى الاعتقاد بأنّ البيانات المطلوبة مخزّنة في جهاز آخر من أجهزة تكنولوجيا المعلومات و الاتصالات الموجودة في إقليم تلك الدولة الطرف.

3 - تتخذ كلّ دولة طرف ما قد يلزم من تدابير تشريعية و تدابير أخرى لتمكين سلطاتها المختصة من حجز البيانات الحاسوبية في الإقليم أو المنطقة الخاضعة لولاية الدولة الطرف، أو من تأمين هذه البيانات بطريقة مماثلة. و تشمل هذه التدابير توفير الصلاحيات التالية:

(أ) حجز جهاز من أجهزة تكنولوجيا المعلومات و الاتصالات المستخدمة لتخزين المعلومات أو تأمينه بشكل آخر.

(ب) إعداد نسخ من هذه البيانات الحاسوبية والاحتفاظ بها.

(ج) الحفاظ على سلامة البيانات الحاسوبية المخزّنة الهامة.

(د) إزالة البيانات المحفوظة أو المعالجة في شكل إلكتروني من أجهزة تكنولوجيا المعلومات و الاتصالات.

4 - تتخذ كلّ دولة طرف تدابير تشريعية و ما قد يلزم من تدابير أخرى لتمكين سلطاتها المختصة من أن تأمر، في إطار الإجراء المنشأ بموجب تشريعاتها المحلية، أي شخص لديه معرفة خاصة بتشغيل نظام المعلومات المذكور، أو شبكة المعلومات و الاتصالات السلكية و اللاسلكية، أو الأجزاء المكوّنة لها، أو التدابير المطبّقة لحماية المعلومات التي تتضمنها، بأن يوفّر المعلومات اللازمة أو المساعدة الضرورية لاتخاذ التدابير المشار إليها في الفقرات من 1 إلى 3 من هذه المادة.

5 - تحدّد الصلاحيات و الإجراءات المشار إليها في هذه المادة وفق أحكام المادتين 21 و 22 من هذه الاتفاقية".

الولوج إليها بشكل منفصل دون أن يمتدّ الإطلاع إلى مجملها، فكلّ فتح منفصل يعدّ بمثابة عملية تفتيش جديدة، تخضع للقيود الدستورية⁽¹⁾.

و من هنا يصبح القانون وفقا لهذا الجانب من الفقه وسيلة "لتنظيم الوصول إلى المعلومات" في "بيئة رقمية" حيث الحواجز الماديّة غالبا ما تكون مفقودة⁽²⁾، و هو الإجتهد القضائي الذي إنتهت إليه الدائرة العاشرة في قضية **United States v. Carey**⁽³⁾.

و الملاحظ أنّ المنظور المادي لمحل التفتيش المعلوماتي هو الذي يلقي التأييد لكن ليس بشكل مطلق إذ أن مختلف الإتفاقيات الدوليّة كاتفاقية بودابست⁽⁴⁾ و الإتفاقية العربية لمكافحة جرائم تقنية المعلومات⁽⁵⁾ اعتمدت كلا النهجين و إن كان الميل واضحا تجاه المنظور

(¹) Thomas K. Clancy, The Fourth Amendment Aspects of Computer Searches and Seizures, Miss. L.J., Vol 75 (2005), p 240.

(²) Orin S. Kerr, Searches and Seizures in a Digital World, Harvard Law Review, Vol 119, Issue 2, (2005), p 535.

(³) United States v. Carey, 172 F.3d 1268, 1275 n.8 (10th Cir. 1999).

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

(⁴) Article 19 alinéa 1 du Convention du Conseil de l'Europe sur la cybercriminalité dispose que : " Perquisition et saisie de données informatiques stockées 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

A. à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées;

et B. à un support du stockage informatique permettant de stocker des données informatiques sur son territoire.

(⁵) المادة 26 من الإتفاقية العربية تنص: تفتيش المعلومات المخزّنة.

1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى :

أ- تقنية معلومات أو جزء منها و المعلومات المخزّنة فيها أو المخزّنة عليها.

ب- بيئة أو وسيط تخزين معلومات تقنية معلومات و الذي قد تكون معلومات التّنية مخزّنة فيه أو عليه.

2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى

تقنية معلومات معيّنة أو جزء منها بما يتوافق مع الفقرة (1-أ) إذا كان هناك اعتقاد بأنّ المعلومات المطلوبة

مخزّنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوقّرة

في التّنية الأولى فيجوز توسيع نطاق التفتيش و الوصول للتّنية الأخرى.

المادي و قد عبّرت عن ذلك بالولوج "لنظام معلومات أو لجزء منه" أو "لدعامة تخزين معلوماتية" و هو مسلك التشريعات العربية (1).

إنّ هذا الموقف الذي يكاد يكون محل إجماع يعبر بشكل واضح ترجيح اعتبارات الفعالية في الوصول إلى الدليل المعلوماتي و لو بالتجاوز على هذا الضمان الإجرائي لأنّ تبني المنظور المادي لمحل التفتيش يجعل هذا القيد غير محدّد و غير معيّن بل شامل، لأنّ وسيط تخزين واحد يمكن أن يشتمل على ملايين من المعلومات المرتبطة بعدد يكاد لا يحصى من أفراد الهيئة الإجتماعية في ظل شيوع إرتباط نظم المعلومات و تبادل المعلومات و الاتصالات، أين تنفي الرابطة بين سبب التفتيش و غايته، بحيث يصبح التفتيش بهذا الشكل مماثلاً لتفتيش مدينة بأسرها.

و لم يشذ المشرّع الجزائري عن الوضع السائد في التشريعات العربية و المقارنة حين حسم موقفه بنص صريح قاطع الدلالة حيث تنص المادة 5 من القانون 04/09 "يجوز للسلطات القضائية المختصة ... الدخول بغرض التفتيش... إلى: أ - منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزّنة فيها، ب- منظومة تخزين معلوماتية"

و يجب في هذا المقام التذكير بأنّ المفهوم القانوني للنظام المعلوماتي لا ينصرف إلى البيانات فقط، إذ عرّفت المذكرة التفسيرية لاتفاقية بودابست النظام المعلوماتي بكونه كلّ آلة

(1) تنص المادة 15 القانون البحريني رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات.

(1) للنيابة العامة أن تصدر أمراً مسبباً بالدخول إلى ما يلي و تفتيشه:

أ) نظام تقنية المعلومات المتصل بالجريمة أو أي جزء منه و أية بيانات لوسيلة تقنية المعلومات مخزّنة فيه.

ب) أي من وسائط تخزين بيانات وسيلة تقنية المعلومات التي من المحتمل أن يكون مخزّناً عليها بيانات متصلة بالجريمة.

(2) إذا قامت لدى النيابة العامة أثناء تنفيذ الأمر المشار إليه في البند (أ) من الفقرة (1) من هذه المادة أمارات قوية بأنّ البيانات المتصلة بالجريمة مخزّنة في نظام تقنية المعلومات آخر أو في جزء منه، و كانت هذه البيانات قابلة لأن يتمّ الدخول إليها من خلال نظام تقنية المعلومات الأول أو متاحة من خلاله على نحو مشروع، فإنّ للنيابة العامة أن تصدر أمراً مسبباً بمدّ الدخول و التفتيش إلى النظام الآخر.

بمفردها أو مع غيرها من الآلات المتّصلة و التي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذاً لبرنامج معيّن بأداء معالجة إلية للبيانات⁽¹⁾.

في حين نجد أنّ التشريع الفرنسي و بحكم مصادقة فرنسا على الإتفاقية الأوروبية لمكافحة الجرائم المعلوماتية فإنّ تشريعاتها الداخلية تؤكد في كثير من مواضعها على إتباع نهج مادي في تحديد محل التفتيش المعلوماتي و يظهر ذلك جليا من خلال نص المادة 57 من قانون الإجراءات الجزائية⁽²⁾، و المادة 11 من القانون رقم 731 لسنة 2016 المؤرخ في 3 جوان 2016 بشأن تعزيز سبل مكافحة الجريمة المنظّمة و الجرائم الإرهابية و تمويلها⁽³⁾.

و نخلص مما سلف بيانه، أنّ لزوم تحديد محل التفتيش كضمانة شكلية تحول دون التوسع في التفتيش ينصرف مدلولها إلى البيانات المخزّنة التي تختلط بها "المعلومات" المجرّمة و ليست "وسائط التخزين" في وضعها المادي، بحيث يمكن في اعتقادنا إستعارة المفهوم المادي للمكان و ترجمته في العالم المعلوماتي في شكل ملف معيّن أو مجلّد، برنامج، أو تطبيق ما، على نحو يشكّل حيّزا محدّدا ضمن مساحة التخزين الرقمي و ذلك إلتزاما بحدود الشرعية و ما توجبه قرينة البراءة، أمّا اعتماد المنظور المادي لمحل التفتيش فهو يشكل عدوانا على الحق في الخصوصية و انتهاكا للحريات، لذا وجب على القضاء أن لا يتردّد في تطبيق القاعدة بكل حزم مهتديا في ذلك بروح الدّستور في حماية الحرّيات الفردية.

(¹) Conseil de l'Europe, Rapport explicatif de la Convention du Conseil de l'Europe sur la cybercriminalité , op cit, Clause n 23.

(²) Art 57-1 alinéa 1 du C.P.P.F Modifié par LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, et loi n° 2016-731 dispose que " « Art. 57-1. - Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial. »

(³) L 'article 11 alinéa 3 de la LOI n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale JORF n°0129 du 4 juin 2016 dispose qu'«il peut être accédé, par un système informatique ou un équipement terminal présent sur les lieux où se déroule la perquisition, à des données stockées dans ledit système ou équipement ou dans un autre système informatique ou équipement terminal, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial. Les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent être copiées surtout support.. »

غير أن الخلاف في الحقيقة لا يتوقف عند تحديد المقصود بمحل التفتيش المعلوماتي من وجهة النظر التي تملئها الشرعية الإجرائية، لأنّ المسألة أكثر تعقيدا و مثارا للجدل فتحديد "البيانات" كمحل للتفتيش المعلوماتي هو معطى يناقض الغاية من هذا الإجراء في مرحلة التفتيش المادي، ذلك أن ارتباط محل التفتيش المعلوماتي بمستهدف التفتيش المادي يعيد طرح إشكالية تحديد المحل مجددا؟

(ب) - إشكالية ارتباط محل التفتيش المعلوماتي بمستهدف التفتيش المادي

من البديهي أن تكون أجهزة التخزين الرقمية أو الأنظمة المعلوماتية "مستهدفا للتفتيش" قبل أن يكون جزءا منها "محلا له"، فينبغي التفتيش عليها قبل تفتيشها، و تثير هذه الحقيقة في معرض دراستنا تساؤلا مشروعا يتعلّق أساسا بما ينبغي للإذن أن يحدده كـ "دليل مادي" يتعيّن التفتيش عنه و ضبطه في مرحلة التفتيش المادي لتفتيشه لاحقا؟ هل يحدّد الأجهزة الماديّة ذاتها؟ أم يحدّد البيانات؟

كما سبق و أن أشرنا، فإنّ التشريع الجزائري لا ينظّم تماما أحكام التفتيش المعلوماتي، إذ بقيت في مجملها خاضعة للقواعد التقليدية التي لا تتواءم مع البيئة الرقمية نهائيا و تطرح العديد من الإشكاليات على نحو يتراجع عنصر الشرعية بشكل كبير جدا، و يأتي القضاء الأمريكي في مقدمة الاجتهادات القضائية في محاولة منه لرسم معالم مشروعية التفتيش الجنائي المعلوماتي، لذ نجد أنّ هذا الأخير قد تعرض لهذا التساؤل في كثير من أحكامه و خلص إلى وجوب التمييز بين الحالة التي تكون فيها الأجهزة الماديّة بحد ذاتها "مجرمة" أو "أدلة عن الجريمة" أو "أداة للجريمة"، و بين الحالة التي تكون فيها هذه الأجهزة مجرد "حاوية للدليل المعلوماتي".

لا تطرح الحالة الأولى بكل الفروض التي تحملها أيّ إشكال يذكر، إذ لا يتطلب القضاء هنا سوى تحديد وسائط التخزين الرقمية كأدلة مادية ينبغي التفتيش عنها و استردادها بدلا عن المعلومات التي تحتويها، أمّا الحالة الثانية و هي الحالة التي تكون فيها أجهزة التخزين الرقمية مجرد حاوية للدليل الجنائي، فإنّ القضاء عالجا بدون تعمق مكثف بالإشارة إلى لزوم التركيز على الملفات المستهدفة و أنّ إغفالها قد يشكّل مخالفة مقتضيات التعديل الدستوري الرابع. و على نقيض موقف القضاء الأمريكي فقد تطرق الفقه الأمريكي إلى هذه

الفرضية بتعمق كبير، ليس بما تستلزم من إجابات بقدر ما تطرح من إشكاليات⁽¹⁾، إذ يرى الفقه أنّ هناك افتراضان:

أما الافتراض الأول:

فهو تحديد أجهزة التخزين الماديّة كأدلة يراد ضبطها، ما يجعل الإذن القضائي في هذه الحالة دقيقاً جداً، حيث يتمّ تنفيذ الإذن بالدخول إلى المكان المطلوب تفتيشه - محل التفتيش المادي- و البحث عن أجهزة التخزين الرقمية و استرجاعها، و هذا الفرض ما يثير إشكالا بالغ التعقيد، ففي الحالة التي يقتصر فيها التخصيص على الأجهزة الماديّة يصبح الإذن القضائي بالتفتيش عاماً، فمن جهة أولى لا يوجد لدى الضبطية القضائية سبب يبرر ضبط جميع أجهزة التخزين الموجودة بالمسكن.

و من جهة أخرى، فإنّ اقتصار التحديد على الأجهزة الماديّة و إن كان دقيقاً من الناحية التقنية في مرحلة التفتيش المادي، بيد أنّه لا يفصح عن أيّ تفصيل بشأن التفتيش المعلوماتي اللاحق، فعندما يقوم خبراء التحليل الحاسوبي الشرعي بالاطلاع على محتويات أجهزة التخزين الرقمية لاسترداد الأدلة المعلوماتية لن يكون هناك ما يوجّه سلوكهم، كون الإذن يجيز الضبط الشامل للأجهزة الماديّة⁽²⁾، فيمتدّ التفتيش ليصل إلى أقصى مدى له من حيث النطاق و هو ما يخالف المعقولة.

أما الافتراض الثاني،

يقوم الافتراض الثاني على لزوم تحديد "البيانات" كأدلة يتعيّن ضبطها، و هذا النهج في الحقيقة لا يحدّد بدقّة ما ستقوم به السّلطة الإجرائية في مرحلة التفتيش المادي، و لكنّه ينجح في تحديد الأدلة التي تسعى إليها سلطة التحقيق في مرحلة التفتيش المعلوماتي، فهو يضع حداً لامتداد التفتيش بأن يصبح الإذن أكثر تحديداً بما يتلائم مع مقتضيات الشرعية غير أنّه يفضي إلى إشكالية جديدة طالما أنّ ذات الإذن يفتقد لشرط التحديد بخصوص كيفية

(¹) لاحظ أنّ هذه الإشكاليات و الفروض التي تواجه سلطة التحقيق عند محاولة تحديد محل التفتيش في الإذن أو الأمر القضائي لم يتطرق إليها التشريع بشكل عام إذ أنّ الفقرة (1) من المادة 5 من القانون 04/09 ليس سوى مجرد نسخ لنفس النصوص الإجرائية الموجودة في الإتفاقيات و التشريعات المقارنة بدون أيّ تعديل.

(²)Orin S. Kerr, Search Warrants in an Era of Digital Evidence, Mississippi Law Journal, Vol 75, Issue 1, (2005), pp 101-102.

تنفيذ مرحلة التفتيش المادي، فإن كان الإذن يجيز التفتيش عن بيانات محدّدة و ضبطها، إلا أنّ التفتيش المعلوماتي يستوجب أولاً ضبط جميع أجهزة التخزين الرقمي التي يمكن العثور عليها في الموقع المادي و إرسالها إلى مخابر التحليل الحاسوبية الشرعية المتخصصة لفحص محتوياتها، فتنفيذ الإذن في هذه الحالة يتمّ بالمخالفة لما يجيزه الإذن نفسه⁽¹⁾.

في اعتقادنا فإنّ هذه الجدليّة تكشف أنّ التّحديد الذي ينصّب على أجهزة التخزين الرقمية كأدلة يراد ضبطها يجعل التفتيش واسع النطاق و أكثر توسّعا و شمولاً و في ذلك ما يناقض مبدأ الشّرية، و في مقابل ذلك فإنّ التّحديد الذي يركّز على "المعطيات المعلوماتية المخزّنة" لا يجيز لسلطة التحقيق القيام بما هو ضروري لاسترداد هذه الأدلّة، فيفشل الإجراء في تحقيق الفعالية، و هو الإشكال الذي وقع فيه التّشريع الجزائري لأنّه لم ينظم مرحلة التفتيش المادي و اكتفى بتنظيم مرحلة التفتيش المعلوماتي من خلال تحديد النّظام المعلوماتي كمحل التفتيش المعلوماتي، لكنه لم يحدّد مستهدف التفتيش المادي⁽²⁾.

عموماً يقترح الفقه لحل هذه الإشكالية و وضع حد لامتداد نطاق التفتيش ضرورة أن يشتمل إذن التفتيش تحديداً للأدلة الماديّة المراد ضبطها في مرحلة التفتيش المادي و تخصيصاً للأدلة التي يتعيّن ضبطها في مرحلة التفتيش المعلوماتي اللاحق⁽³⁾.

و بدورنا نوّيد هذا الرّأي، فتقييد مرحلة التفتيش المادي بأجهزة محدّدة يجوز ضبطها متى قامت الأسباب التي ترجّح احتوائها على أدلة تقيّد في إظهار الحقيقة، مع تضييق نطاق المراجعة (التحليل) في مرحلة التفتيش المعلوماتي من شأنه أن يرسم حدوداً لنطاق التفتيش

(1) Orin S. Kerr, Search Warrants in an Era of Digital Evidence, Loc.Cit.

(2) يلاحظ في هذا الصّدّد أنّ المشرّع في تنظيمه لهذه المسألة اكتفى باقتباس نص الإتفاقية الأوروبية لمكافحة الجرائم المعلوماتية، فالفقرة الأولى من نص المادة 5 من القانون 04/09 منقولة حرفياً من الفقرة 1B من المادة 19 من اتفاقية بودابست :

"Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire: ...b. à un support du stockage informatique permettant de stocker des données informatiques sur son territoire. "

(3) Orin S. Kerr, op cit, p 132.

مما يجب الإشارة إليه في هذا المقام أنّ الفقيه Orin S. Kerr قد تراجع عن هذه التّوصية ضمن أبحاثه الحديثة و دعى إلى جعل مرحلة التفتيش المادي طليقة من غير قيد بشأن شرط تحديد محل التفتيش كما سنرى لاحقاً عند معالجة ضابط تحديد أسلوب تنفيذ التفتيش المعلوماتي.

توخياً من امتداده إلى جميع أجهزة التخزين الرقمية المتواجدة بمسكن المتهم بغض النظر عما إذا كانت ملكيتها ترجع إلى المتهم أو أحد أفراد أسرته المقيمين معه، و إلى جميع محتوياتها في المرحلة الثانية لأن وجود سبب يبرر تفتيش ملف معين لا يبرر تفتيش محتويات الجهاز ككل⁽¹⁾، فكيف يكون مبرراً لتفتيش كافة هذه الأجهزة.

إن عدم تحديد محل التفتيش في المرحلة الثانية يعتبر في نظرنا باطلاً، لأن القانون إذ أجاز تقييد حرية الأفراد بصفة استثنائية فإنه يسمح بذلك بالنسبة لمحل معين على وجه التخصيص و ليس العمومية منعا من التطاول على الحريات الفردية، و إلا فقد الإذن مضمونه و حاد عن الشرعية، و انقلبت العلاقة بين الحرية الفردية كحق و التفتيش كقيد و كلما زاد التخصيص في إذن التفتيش كلما تقلص دور الإستثناء لصالح القاعدة. و الحقيقة التي لا مرأى فيها أن تحديد "فئة من البيانات" كمحل للتفتيش في مرحلة التفتيش المعلوماتي من شأنه أن يعدّ منطلقاً لإرساء حدود واضحة للتفتيش المعلوماتي ينبغي عدم تجاوزها، على أن الأمر ليس على ذلك القدر من السهولة، لأن هذا التوجه يطرح إشكالا عمليا قد يعصف

(1) يعتبر الفشل في تحديد محل التفتيش إشكالية كبيرة و محل نقاش خصيب لدى الفقه الأمريكي الذي ينتقد بشدة النهج المتساهل للقضاء الأمريكي تجاه هذا الضابط الإجرائي و من بين الأمثلة القضائية الحديثة الحكم الصادر في قضية *United States v. Juarez*، تتلخص وقائعها في قيام المتهم بتصوير بعض النساء أثناء تجولهن في نيويورك تصويراً فيه مساس بالحياة الشخصية (موضع العفة)، أين قامت الضبطية القضائية بضبطه لحظة ارتكاب الواقعة الجرمية، و كان الهاتف في وضع تسجيل فيديو أين لجأت إلى قاضي التحقيق و استصدرت إذناً بتفتيش "جميع أرقام الهاتف و الرسائل و الرموز فضلاً عن جميع الصور و تسجيلات الفيديو المخزنة في ذاكرة الهاتف"، و قد كشف التفتيش المعلوماتي عن صور فاحشة للقصر على إثرها تمت متابعة المتهم بهذه الجريمة، و عند طعن هذا الأخير بعدم مشروعية الإذن القضائي لفشله في تحديد المكان المطلوب تفتيشه تم رفض طلبه، و جاء في حكم المحكمة: "إن الإذن القضائي قد حدّد الهاتف كمحل للتفتيش"، و في تعليقه على هذا الحكم يرى الفقه الأمريكي أن هذا المنطق الذي تبنته المحكمة هو أصل الإشكالية، فإذا تم تبني المنظور المادي لمحل التفتيش جاز للسلطة القائمة بتنفيذه تفتيش ملايين المعلومات المخزنة به، بحيث يستبعد سبب التفتيش و غايته كقيد على نطاق التفتيش، و كان الأحرى النظر إلى الهاتف الخلوي على أنه مجموعة حاويات إلكترونية يمكن تقسيمها إلى مناطق مختلفة، ففي هذه القضية يرتبط السبب المحتمل بتسجيل الفيديو فقط لأن المتهم لحظة ضبط هاتفه لم يكن لديه الوقت الكافي لإخفاء الدليل ضمن مكان غير مألوف على الهاتف، و قد اعتبر الفقه أن تحديد محل التفتيش وفقاً لهذا المنظور يعتبر مخالفاً للمعقولة" بمعنى (المشروعية الإجرائية).

حول مجمل هذا الموضوع راجع:

Adam M. Gershowitz, The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches, *Vanderbilt law review*, Vol 69, (2016), p 605.

بهذه النتيجة، و الذي مفاده كيف يمكن التوصل إلى تحديد محل التفتيش تحدياً نافياً للجهالة وسط هذا الكم الهائل من البيانات المختلطة؟

الفرع الثاني: متطلبات التّحديد الكافي لمحل التفتيش المعلوماتي

سبق أن توصلنا إلى أنّ المشروعية الإجرائية توجب تحديد منطقة معينة ضمن البيئة الرقمية كمحل للتفتيش و هذه النتيجة تثير لدينا نقطتين، الأولى تتعلّق بالمعالجة القضائية لمتطلبات التّحديد الكافي لمحل التفتيش (أولاً) و الثانية تتعلّق بمدى كفاية هذه المتطلبات في رسم نطاق التفتيش (ثانياً).

أولاً: المعالجة القضائية لمتطلبات التّحديد الكافي لمحل التفتيش

قدمنا أنّ التشريعات عموماً سواء العربية أو المقارنة لم تعالج هذه الإشكاليات مبقية على القواعد الإجرائية التقليدية للتفتيش و تطبيقها في البيئة المعلوماتية، إلا أنّ القضاء الأمريكي و طيلة أكثر من عقدين من الزمن حاول إرساء قواعد يهتدى بها لتحديد محل التفتيش المعلوماتي عن طريق الفصل في الدفوع التي تقدّم إليه بطلب بطلان الأدلة المعلوماتية المستمدة من إجراء التفتيش الذي لا يستوفي الإذن به تحديداً للمحل المراد تفتيشه وفق ما يقتضيه التعديل الدستوري الرابع.

و لكون المحكمة العليا الفيدرالية لم تحن بعد أمامها الفرصة للتعرض لموضوع متطلبات التّحديد الكافي لمحل التفتيش المعلوماتي و أثر إغفاله على الدليل الجنائي المستمدّ من هذا الإجراء، فإنّ هذا القيد الإجرائي حتّى الآن لا يزال ينظر إليه في إطار المنظور التقليدي، ما فتح المجال للإجتهد القضائي للمحاكم الابتدائية و الدوائر الاستئنافية التي أبدت إنقساماً واضحاً بين متشدّد يرحب باعتبارات الشرعية و يتمسك بالتطبيق الصّارم للقاعدة الدستورية، و بين متساهل يراعي متطلبات الفعالية مدفوعاً بصعوبة الوفاء بمتطلبات التّخصيص الدقيق لهذه البيانات أو الملفات وسط هذا الكم الهائل من البيانات التي تستوعبها الأجهزة الإلكترونية الحديثة.

و يتجه القضاء الأمريكي في غالبته إلى تجنّب التوسّع في تطبيق هذه القاعدة بسبب صعوبة وصف المكان المراد تفتيشه و تعذر تحديد الوصف الدقيق للبيانات التي يحتويها وسيط التخزين، لذا غالباً ما يتمّ وصف محل التفتيش بمصطلحات مرتبطة بالجريمة الجاري التّحقيق فيها، ففي قضية **United States v. Campos** أيّدت الدائرة الفيدرالية التاسعة صحة

التفتيش المعلوماتي بموجب إذن لا يتضمن سوى الإشارة إلى مواد تتصل مباشرة بالصّور الدّاعرة للأطفال القصر، و تأكّد ذات التّبرير في قضية **United States v. Upham**⁽¹⁾.

و هذا التّوجه أيّده الدّائرة العاشرة في قضية **United States v. Reyes** و علّلت قرارها بأنّه "في عصر التّكنولوجيا الحديثة و التّوافر التّجاري لأشكال مختلفة من الأشياء، من غير المتوقّع أن تصف الأذن بدقّة الشّكل الذي ستخذه السّجلات و أنّ ضبط نوع معيّن من العناصر التي تدخل ضمن الأشياء المحدّدة في الإذن لا تشكل تفتيشا عاما غير مسموح به، فالإذن الذي يجيز ضبط وثائق معيّنّة يأذن أيضا بتفتيش حاوية يُحتمل أن تحتوي على تلك الوثائق"⁽²⁾. إذ الضّبطية القضائيّة لا تحتاج إلى إتّباع هذا التّهج في كل قضية لأنّ المراجعة القضائيّة لأذن التفتيش عن الأدلّة المعلوماتيّة ذات طبيعة عقلانية و عملية أكثر من كونها ذات بعد تقني و بناء على ذلك، فإنّ ما يهّم هو جوهر الأدلّة و ليس شكلها⁽³⁾.

غير أنّ الاجتهادات القضائيّة الحديثة تكشف ميلا نحو التّمسك بهذه القاعدة، ففي قرار حديث لها قرّرت المحكمة العليا بولاية نيويورك في قضية **People v. Covlin** بطلان الأدلّة المعلوماتيّة في جريمة توبع فيها المتهم بقتل زوجته، معتبرة أنّ بعض الأذن بالتفتيش

(1) *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999).

في قضية *United States v. Upham* قامت الضّبطية القضائيّة بمراقبة غرفة درشة أين تلقوا صور تتضمّن مواد إباحية للأطفال من خلال جهاز حاسوب تبين في وقت لاحق أنّه ملك لـ *Kathi Morrissey* و يستخدمها صديقها آنذاك *Upham Troy* أجاز الإذن بضبط "جميع البرامج والأجهزة الحاسوبية. . . و أقراص الحاسوب، و محرّكات الأقراص" فضلا عن "جميع الصّور المرئيّة، بأيّ شكل أو وسائط، و المتعلّقة بالأطفال القصر المنخرطين في ممارسة سلوك جنسي، و أجري التفتيش عن مالك الجهاز أين تمّ التّوصّل إلى ضبط الجهاز و عدد من الأقراص المدمجة و قد قرّرت المحكمة مشروعية التفتيش و أيّدت بذلك صحة شرط التّحديد للمواد و الأشياء التي سيجري ضبطها، مشيرة إلى أنّ اللّغة المقيدة " للقاصرين الذين يمارسون سلوكا جنسيا" لم تترك سوى هامش قليل من التّقدير للقائم بتنفيذ الإذن.

United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999).

(2) *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 التّطبيقات القضائيّة و أخرى مذكورة لدى:

H. Marshall Jarrett, et al, op cit, pp 71-72.

(3) H. Marshall Jarrett, et al, op cit, p 75.

الصّادرة في القضية لا تفي بمعايير "التّحديد الكافية" لمحل التفتيش، و أنّ لغة الإذن وردت عامة و سمحت بتفتيش أيّ نوع محتمل من السّجلات أو الوسائط الإلكترونيّة أو أيّ بيان موجود على هاتف المتّهم" (1).

ثانيا: مدى كفاية متطلبات التّحديد الكافي لمحل التفتيش في تضيق نطاقه

في إطار تقييمه للدّور الوقائي للقاعدة محل البحث يطرح الفقه تساؤلات تزيد من عمق الإشكالية الرئيسيّة، و ذلك في معرض نقده لها، فيما إذا كان تحديد البيانات التي يتعيّن ضبطها يمكن أن يكون ضيقا بما فيه الكفاية؟ و هل يمكن فعلا التّوصل إلى تحديد نهائي لمكان تواجد أدلة معلوماتيّة معيّنة (إن وجدت) (2)؟ و بالتّالي الحدّ من امتداد عمليات التفتيش بقصر هذا الإجراء على تلك الأماكن أو التّطبيقات الموجودة على أجهزة التخزين الرّقمية فقط؟ إنّ الإشكالية المثارة في هذا الصّدّد هي إشكالية عملية بحتة، ففي الحالة التي لا ينجح فيها التفتيش الضيق في الوصول إلى الدّليل المعلوماتي المحدّد في إذن التفتيش، فإنّ ذلك لا يحقّق اليقين الجازم بإنعدام الدّليل الجنائي فعلا و عدم وجوده بهذا المحل، بما يوجب حتما التّوسّع في التفتيش باستكشاف كلّ مكان على محرّك الأقراص الصّلبة، أو ذاكرة الجهاز حيث يُحتمل العثور على الأدلّة أو التّحقّق من إنعدامها ضمن هذا المحل (3).

(1) People v Covlin 2018 NY Slip Op 28011 Decided on January 22, 2018 Supreme Court, New York Country.

(2) Orin S. Kerr, op cit, p 100.

(3) Josh Goldfoot, op cit , p 141.

ينتقد الفقيه Josh Goldfoot المفهوم الغامض لمتطلبات هذه القاعدة المنبثقة من منظور "الحاوية الفرعية" التي 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 و من أين تنهي؟ إذا كان المقصود هو تقسيم الملفات داخل مساحة التخزين الرّقمية، فإنّ هذا التّقسيم لا يأخذ صورة واحدة بل يخضع لميشئة كل مستخدم يقسمها كيف يشاء حسب حاجته، فكيف يمكن تحديدها في الإذن، و يزداد الوضع تعقيدا فيما لو أنّ ملفا واحدا يحمل قدرا كبيرا من المعلومات أين تصبح "الملفات" و "الحقائق" مفهومان مختلفان لتصور "الأشياء" الموجودة بوسيط التخزين الرّقمي، علاوة على ذلك فإنّ الدّليل الجنائي المستهدف بالتفتيش لا يكون دائما في شكل ملف داخل مساحة التخزين الظاهرة للمستخدم بل قد يكون في شكل بيانات مخزّنة داخل المساحة الفارغة space slack أو عبارة عن بيانات وصفية.

و في نظرنا فإنّ هذه الحالة تعتبر من بين أبرز مظاهر التّعارض بين الاعتبارات القانونية و الاعتبارات العملية لقاعدة تحديد البيانات او فئة ميعة من الملفات كمحل للتفتيش المعلوماتي، فالتمسك بتطبيقها الجامد يؤدي إلى شلل كلي لعملية التفتيش، و تجاوزها بهذا الشكل يحدث إنتهاكا غير معقول للحريات الفردية.

إزاء هذا التناقض يجمع الفقه على تراجع دور هذه القاعدة في البيئة المعلوماتية بسبب حجم المساحة المراد تفتيشها و كمية البيانات المخزّنة بداخلها، ففي الحيز المادي يحدّد هذا الشرط محل التفتيش بمكان معيّن كالمنزل أو الشقة، غير أنّه في حالات التفتيش المعلوماتي يمكن لشقة واحدة أن تحتوي على عدّة أجهزة للتخزين الإلكتروني، و التي بدورها قد تحتوي على مجموعة من الأدلة المعلوماتية بالإمكان أن تكون مستترة في أيّ مكان على الأقراص الصلبة دون القدرة على تحديد مكان تواجدها مسبقا قبل القيام بعملية التفتيش، بما يستتبع الإطلاع حتما على أيّ مكان على الأجهزة، و هكذا يصبح التفتيش المعلوماتي معادلا لتفتيش مدينة بأسرها بدلا من منزل فردي، فشرط التّحديد في الإذن تقلص دوره في الحد من امتداد عمليات التفتيش المعلوماتي و قد بات ذلك أكثر وضوحا اليوم نظرا للقدرات التخزينية الكبيرة للحواسيب⁽¹⁾.

لذا عادة ما يجيز القضاء الأمريكي للضبطية القضائية القيام بتفتيش كميات هائلة من البيانات للعثور على "إبرة في كومة قش"، فالإفتراض بكون الإذن بالتفتيش من شأنه أن يحدّد بتفصيل كبير ما هي الملفات أو التطبيقات التي يمكن للشرطة تفتيشها سيكون افتراضا خاطئا⁽²⁾، تلك الحقيقة التي سلّمت بها الدائرة الفيدرالية الثانية موضحة "...عندما يسمح الإذن بتفتيش مكان الإقامة، فإنّ الأبعاد المادية للأدلة المطلوبة ستفرض بشكل طبيعي قيودا على المكان الذي يجوز فيه للضابط القيام بالبحث... هذه القيود غائبة إلى حد كبير في المجال الرقمي، حيث أنّ حجم الملف أو خصائصه الظاهرية قد لا تكشف شيئا عن محتواه"⁽³⁾، و

(¹) 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.

(²) Adam M. Gershowitz ,The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches ,Vanderbilt law review, Vol 69, (2016) , p 599.

(³) United States v. Galpin, 720 F.3d 436, 448-49 (2d Cir. 2013).

ذلك هو مبنى الخلاف الذي يوضح عدم مواعمة الحدود التقليدية التي تفرضها قاعدة التّحديد في الإذن القضائي عندما ينظر إليها بمفهوم مادي.

رغم وجهة النّقد الموجّه للقاعدة، فإننا نتحقّق عن المغالاة فيه و المطالبة بالتّخلي عن هذا الضمان في مرحلة التّفنّيش المادي و جعلها طليقة من غير قيد⁽¹⁾، أو اعتماد منظور مادي لمحل التّفنّيش بشكل مطلق⁽²⁾، لأنّ ذلك بمثابة دعوة للتّخلي على هذه الضّمانة الإجرائية، و هو ما من شأنه أن يفتح باب التّوسّع الخطير في إمتداد التّفنّيش و يمنح قاضي التّحقيق سلطة غير محدودة فتتوسّع عبر الملفات البريئة وفقاً لرؤيتها، و من هذا المنطلق لا يقبل تطبيقاً للقواعد العامة أن يجيز الإذن القيام بتفتيش عام لجميع أجهزة التخزين الرقمية التي يُعثر عليها بحوزة المتهم أو بمقر إقامته لأنّ التّفنّيش مشروع في نطاق الغاية منه⁽³⁾.

(1) Orin S. Kerr, Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data, op cit, p 11.

(2) Josh Goldfoot, op cit, p166.

(3) حول القيد الإجرائي المتعلّق بضرورة تحديد محل التّفنّيش المعلوماتي إعتقاداً على المنظور الداخلي لوسائط التخزين الرقمية و أثره على تراجع شرعية الإثبات و إنعكاساته السلبية التي تتعدى المتهم إلى كافة أعضاء الهيئة الإجتماعية كتب القاضي KLEINFELD في رأيه المخالف في قضية *United States v. Micah J. Gourde*، يلي: "هناك الكثير من الأسرار المخبأة في الحواسيب، أغلبها شرعي، بعضها محرّج، و منها ما قد يترك أثراً مأساوياً في تداعياته. قد يحتوي البريد الإلكتروني و الروابط المؤرخة، أنّ شخصاً ما قد طلب علاج لمرض أخفاه حتّى عن أفراد أسرته. أو أنّ طفلاً لأحدهم تلقى نصائح و إرشادات لمشكلة حرجة ليس من شأن أحد أن يعلمها. أو أنّ أمّاً لثلاثة أطفال ترسل صديقاً قديماً من المدرسة الثانوية عبر رسائل بريد إلكتروني مفعمة بالإغراءات. أو أنّ شاباً قديراً في منتصف عمره يتأمّل صوراً مخلة. كما لو أنّ مسؤولاً طُرد من منصبه لأنّ إحدى المدعوات إلى الحفلة وجدت مجلة إباحية عندما دخلت إلى حمام بيته. قد تهدّم حياة الأفراد بسبب محتويات شرعية و لكنها محرّجة وجدت في حواسيبهم. و في كل المناطق الحضرية -باستثناء الكبيرة منها- لا يهتمّ ما إذا كانت هناك أيّ تهم رسمية ترتبت على عثور الشرطة أو أحد الرّوار على هذه المحتويات، بكل الأحوال سيذاع ذلك في الجرائد و كل أنحاء البلاد في غضون أيام. .. و ليست الأسرار هي المشكلة الوحيدة، بل غالباً ما ينجّر الضّبط على جهاز حاسوب مشترك بين أفراد العائلة- مع أنّه غير جائز من الناحية القانونية- لمصادرة كتاب أستاذ، أو رسالة دكتوراه أو شكت على الانتهاء، أو حسابات عمل دائنة و مدينة. لا يستطيع الناس إكمال أعمالهم الشرعية إن احتجزت حواسيبهم عند الشرطة بسبب أنّ أحداً ما اشتبه بملفات إباحية حملها طفل. نعتبر أنّ ممارسة الجنس مع الأطفال شيء فضيع حتّى أنّنا سنعتبر لبرالين إن سمحنا بالتّفنّيش عندما تقوم الحكومة بالتّحقيق في قضايا استغلال الأطفال لأغراض إباحية... خصوصية الأفراد مع حواسيبهم مهمّة جداً حيث لا نسمح بانتهاكها بسبب الإشمئزاز الجنسي..."

United States v. Micah J. Gourde, 440 F.3d 1065 (9th Cir. 2006).

و مراعاة لمبدأ التناسب نرى الإصرار على هذا القيد و على وجه التحديد في المرحلة الثانية، منعا من التوغل في استعمال هذه السلطة، و لو كان في تطبيقها ما يناهض متطلبات الفعالية، لأن الهيئة الإجتماعية-التي تعتبر مصلحتها أساس مشروعية التفتيش - لا يضيرها إفلات مجرم، بقدر ما يهدم أوأصرها تفتيش معلوماتي على درجة من الشمولية و التوسع يكشف عورات أفرادها و ينتهك أسرارهم.

الفرع الثالث: مشروعية محل التفتيش المعلوماتي

الأصل أنه متى توفرت شروط التفتيش أمكن إجراءه في أي محل يحتوي ما يفيد في التوصل إلى وجه الحق في الجريمة، غير أن القانون قد يضيف على بعض المحال حصانة معينة، فلا يصح تفتيشها رغم تحقق ما يوجب إجراء التفتيش، و ترجع الحصانة التي يضيفها القانون على تلك المحال إلى تعلقها بمصلحة معينة، عامة أو فردية، يرى الشارع أنها أولى بالرعاية من مصلحة التحقيق التي تتطلب التفتيش⁽¹⁾، و هو ما يملينا التطرق إلى تحديد بعض هذه الحصانات (أولاً)، و استراتيجية مراجعة ملفات الحاسوبية التي تمتع بهذا الإمتياز (ثانياً).

أولاً: حظر تفتيش المحل المعلوماتي المتمتع بالحصانة

إن أهم الحصانات التي تقف عقبة في وجه ممارسة سلطة التحقيق و تحول دون التمكن من إجراء التفتيش رغم قيام ما يبرره هي تلك التي تتعلق بالهيئات الدبلوماسية (أ)، و الهيئات البرلمانية (ب)، و بحق الدفاع (ج).

أ- الحصانة الدبلوماسية

هناك مبدأ عام متفق عليه في القانون الدولي هو أن البعثات الدبلوماسية و أشخاصها و مساكنها و مراسلاتها تتمتع بامتياز يجعلها بعيدة عن تدخل سلطات الدولة التي توجد بها، و قد كان أساس تلك الحصانة عرف دولي مستقر تؤيده نصوص متفرقة في بعض القوانين الداخلية⁽²⁾، ثم تم تنظيمها بموجب إتفاقية فينا للعلاقات الدبلوماسية لسنة 1961⁽¹⁾. و ليس هنا

(1) سامي حسني الحسيني، المرجع السابق، ص 210.

(2) توفيق محمد الشاوي، المرجع السابق، ص 262.

من مجال للتوسع في دراسة هذه الحصانة و شروطها فذلك من شأن أبحاث القانون الدولي، و الذي يهمننا هو ما تستتبعه الحصانة الدبلوماسية من عدم جواز تفتيش الأنظمة المعلوماتية الخاصة بالبعثات الدبلوماسية.

عموما تتمتع مراسلات الدبلوماسيين بالحصانة فلا يصح ضبطها أو الإطلاع عليها و يسري هذا المبدأ على كافة المراسلات و البيانات المعلوماتية المخزنة المتعلقة بعمل البعثة أو الخاصة بالمبعوثين أنفسهم، و يجب على دولة الإقليم أن تكفل للمبعوثين الدبلوماسيين حرية الإتصال بدولهم أو بغيرها من الدول دون عائق حتى و لو كان هذا الاجراء مفيد في كشف الحقيقة في تحقيق يجري ضد متهم لا يتمتع بالحصانة⁽²⁾، و من ثم لا يجوز تفتيش بياناتهم أيّا كان مكان تخزينها (التخزين المحلي أو السحابي) و أيّا كانت الدّعمة المادّية المستعملة للتخزين (هاتف، لوح رقمي، حاسوب محوّل أو ثابت)⁽³⁾.

و تتسحب هذه الحماية الإجرائية لتشمل الزوج أو الزوجة و الأبناء، و تشمل مقر البعثة الدبلوماسية و ملحقاتها كالحدايق و المخازن و السيارات، بل و تشمل أيضا بعض الأماكن التي يقصدها هؤلاء على سبيل التّأقيت كالفنادق و قصور الضيافة⁽⁴⁾. و على أيّ حال فإنّ حدود هذه الحصانة و شروطها غير متفق عليها بين الدول، لذلك يثور التساؤل عن حكم التفتيش المعلوماتي الذي يقع على النظم المعلوماتية الخاصة بالدبلوماسية، هل يكون صحيحا أو ينبغي الحكم ببطلانه لوروده على محل غير قابل للتفتيش؟

(1) أنظر المواد 22، 23، 27 من اتفاقية فينا للعلاقات الدبلوماسية و التي إنضمت إليها الجزائر بموجب المرسوم الرئاسي رقم 74/64 المؤرخ في 4 مارس 1964 المتضمن المصادقة على هذه الإتفاقية المؤرخة في 18 أفريل 1961.

(2) سامي حسني الحسيني، المرجع السابق، ص 211.

(3) تعددت الآراء في تحديد الأساس القانوني الذي تبنى عليه الحصانة الدبلوماسية، و وجدت في هذا الشأن نظريات ثلاث: نظرية امتداد الإقليم، و نظرية النيابة، و نظرية مقتضيات الوظيفة. و استقرت من بين هذه النظريات، النظرية الأخيرة التي ترى أنّ الحصانة المقررة إنّما هي لضمان قيام المبعوث الدبلوماسي بوظائفه في الدولة الموفد إليها، دون ضغط يقع عليه، حتى يكون مطمئنا في أدائه لعمله.

يراجع بهذا الخصوص: سامي حسني الحسيني، المرجع السابق، ص 211.

(4) حسام الدين محمد أحمد، المرجع السابق، ص ص 136 - 137.

يمكن القول أنّ التفتيش يكون صحيحاً إذا أمرت به أو أقرته السلطات العليا في الدولة، لأسباب ترجع إلى المحافظة على سيادتها و أمنها الداخلي أو الخارجي أو لاعتبارات دولية كعامل دولة أخرى بالمثل، و لا يترتب على إنتهاك حصانة الممثل الدبلوماسي في هذه الأحوال إلاّ المسؤولية الدولية إذا وجدت، و ممّا يؤكّد هذا الحل أنّ هذه الحصانة لا يوجد بشأنها نص صريح في التشريع الداخلي⁽¹⁾.

ب) - الحصانة البرلمانية

يتمتع أعضاء المجالس البرلمانية بحصانة عما يبدونه من أفكار و آراء و أقوال أثناء ممارسة عملهم النيابي سواء داخل المجلس أو في لجانه، و يترتب على عدم جواز تحريك الدعوى الجنائية أو رفعها على العضو أيّ تكليف هذه الحصانة بمثابة قيد إجرائي⁽²⁾، فالحصانة البرلمانية بنوعها الموضوعي و الإجرائي إستثناء من القانون العام⁽³⁾، اقتضته ضرورة جعلت السلطة التشريعية بمنأى من اعتداء السلطة التنفيذية و الهيئات و ذوي النفوذ عليها.

غير أنّ هذا الإستثناء لم يشرّع كامتياز لصالح العضو بقدر ما هو ضمانه للوظيفة التي يشغلها ليؤديها في اطمئنان و دون خشية من أحد، إذ يخشى أن تتخذ السلطة التنفيذية إجراءات كيدية ضدّهم لما يبدونه من آراء داخل المجلس أو بسبب مواقفهم المعارضة للسلطة التنفيذية التي تملك سلطة الإتهام⁽⁴⁾. و هذه الحصانة تجد لها تنظيماً دقيقاً في الدستور، إعلاء لشأن مهام النائب و من هنا فإنّه لا مرية أنّ تفتيش الأنظمة المعلوماتية لهذه الشريحة من الأفراد غير جائز لأنّه يستلزم حتماً متابعة النائب و توجيه الإتهام له كما سبق و أن نظرنا

(1) توفيق محمد الشاوي، المرجع السابق، ص 263.

(2) حسام الدين محمد أحمد، المرجع السابق، ص 138.

(3) و ما يهمننا في هذا البحث هو النوع الثاني من الحصانة و هي الحصانة الإجرائية و يطلق عليها الفقه المناعة البرلمانية، أو الحصانة ضد الإجراءات الجنائية، أو الحرمة البرلمانية، و المصطلح الأخير محل نقد من قبل الفقه، لأنّ هذا المفهوم يوحي بأنّ المتمتع به لا يمكن أبداً متابعتة جزائياً في حين أنّ ذلك غير صحيح. حول مجمل هذا الموضوع: أحمد بومدين، الحصانة البرلمانية، رسالة دكتوراه، كلية الحقوق جامعة أبي بكر بقايد تلمسان، الجزائر، 2015، ص 45 و ما بعدها.

(4) الطّبطبائي عادل، الحدود الدستورية بين السلّطتين التشريعية و القضائية "دراسة مقارنة"، الطبعة الأولى، مجلس النّشر العلمي، جامعة الكويت، الكويت، 2000، ص 265.

إليه⁽¹⁾، و هو ما يستغرقه الحظر من المتابعة الجزائية بشكل عام إلا في حالة إقدام النائب على التنازل شخصيا على هذا الامتياز القانوني، أو بإذن من المجلس الشعبي الوطني أو مجلس الأمة الذي يقرّر رفع الحصانة عنه بأغلبية أعضائه⁽²⁾، و أيضا في حالة التلبس بارتكاب الجريمة⁽³⁾.

مع ذلك ينبغي تفسير هذه القواعد الدستورية تفسيراً ضيقاً لأنها قواعد استثنائية، فالحصانة ضد الإجراءات الجنائية تقتصر من حيث الأشخاص الذين يتمتعون بها على أعضاء البرلمان، فهي ضمان شخصية مقصورة على أعضاء البرلمان فلا تمتد إلى سواهم من الوزراء، أولاد العضو أو زوجه أو أقاربه أو أتباعه أو شركائه في الجريمة⁽⁴⁾، و لهذا يمكن القول بأنّ هذا النوع من الحصانة يقتصر على الشخص الذي توافرت فيه صفة العضوية، بل و يشترط توافر هذه الصفة وقت إتخاذ الإجراء و ليس بوقت ارتكاب الجريمة، و يكمن الفرق في ذلك أنه إذا زالت الصفة فإنه يجوز تحريك الدعوى ضده حتى و لو كان وقت ارتكاب الجريمة متمتعا بها⁽⁴⁾، و كذا العكس فإذا بدأت الإجراءات الجنائية قبل إنتخاب الشخص عضوا في مجلس النواب يتعين لاستمرارها استئذان المجلس⁽⁵⁾.

(¹) تنص المادة 126 من الدستور الجزائري: "الحصانة البرلمانية مُعترف بها للنواب و لأعضاء مجلس الأمة مدة نيابتهم ومهمتهم البرلمانية. و لا يمكن أن يتابعوا أو يوقفوا. و على العموم لا يمكن أن ترفع عليهم أية دعوى مدنية أو جزائية أو يسلبت عليهم أي ضغط بسبب ما عبّروا عنه من آراء أو ما تلقّظوا به من كلام، أو بسبب تصويتهم خلال ممارسة مهامهم البرلمانية".

(²) و هي الحالة التي عالجتها المادة 127 من الدستور الجزائري: "لا يجوز الشروع في متابعة أيّ نائب أو عضو مجلس الأمة بسبب جنابة أو جنحة إلا بتنازل صريح منه، أو بإذن، حسب الحالة، من المجلس الشعبي الوطني أو مجلس الأمة الذي يقرّر رفع الحصانة عنه بأغلبية أعضائه".

(³) و هو الإستثناء المقرر بالمادة 128 من الدستور الجزائري: "في حالة تلبس أحد النواب أو أحد أعضاء مجلس الأمة بجنحة أو جنابة، يمكن توقيفه، و يخطر بذلك مكتب المجلس الشعبي الوطني، أو مكتب مجلس الأمة، حسب الحالة، فورا يمكن المكتب المختر أن يطلب إيقاف المتابعة و إطلاق سراح النائب أو عضو مجلس الأمة، على أن يعمل فيما بعد بأحكام المادة 127 أعلاه".

(⁴) أحمد علي عبود الخفاجي، الحصانة البرلمانية: دراسة تطبيقية في ظل دستور العراق لسنة 2005 م، الطبعة الأولى، المركز العربي للنشر و التوزيع، مصر، 2018، ص 142.

(⁵) و متى كانت الدعوى صحيحة على المتهم قبل إنتخابه عضوا في البرلمان و كانت المحكمة تجهل أنّ المتهم إنتخب بعد ذلك، فإنّ إذن البرلمان في استمرار السير في الإجراءات بعد أن تتبّعت المحكمة يمنع من القول ببطلان الإجراءات التي تمت ضد المتهم إثر إنتخابه و لا يصح تشبيه هذه الحالة مع جميع الوجوه بحالة الإجراءات التي تبدأ

غير أنّ مثل هذا النوع من الحصانة يضع إشكالية مشروعية التفتيش المعلوماتي في إطار عدّة افتراضات أهمّها مدى مشروعية التفتيش المادي لمسكن النائب بحثاً عن أجهزة التخزين الرقمية في إطار التحقيق في جريمة بعد إتهام أحد أفراد أسرة النائب المقيم معه في ذات المسكن؟

في هذا الفرض فإنّ التفتيش المعلوماتي يستوجب تفتيش منزل النائب للعثور على أجهزة التخزين الرقمية التي يربح أنّها تحتوي على الأدلة المستهدفة، و نعتقد أنّ التفسير الضيق للنص الدستوري يجعل الحصانة البرلمانية قاصرة على شخص النائب فلا تتعداه إلى أفراد أسرته و لو وقع التفتيش في منزله⁽¹⁾، فحصانة النائب مقررة لمصلحة الأمة في تمثيلها و تلك العلة في رأينا تنتفي حال مباشرة إجراءات تفتيش في مواجهة متهم مقيم مع النائب، هذا فيما يتعلق بمرحلة التفتيش المادي أمّا مرحلة التفتيش المعلوماتي لأنظمة معلوماتية وجدت بمنزل النائب فهي تخضع لضمانات خاصة كما سنرى لاحقاً.

ضد عضو في البرلمان بغير إذن المجلس إذ أنّ حكم كل من الحالتين لا يتفق تماماً مع حكم الآخر سواء من جهة طبيعته أو جهة علته. راجع: سامي حسني الحسيني، المرجع السابق، ص 215.

(1) ذهب الفقه في مصر إلى أنّ الحصانة البرلمانية تمتدّ إلى منزل النائب، فلا يجوز تفتيشه لأنّ ذلك التفتيش فيه إعتداء على حرية النائب و استقلاله أمّا الفقه الفرنسي، فقد ذهب البعض إلى جواز تفتيش منزل النائب، حيث يمكن إجراء التفتيش دون حاجة إلى حضور النائب ذاته، تمسكاً بالتفسير الضيق للنصوص، و ذهب البعض الآخر إلى عدم جواز تفتيش المنزل قبل الحصول على إذن البرلمان، لأنّ التفتيش ينبغي مباشرته في حضور المتهم كما أنّه يعتبر عائقاً لحرية النائب من حيث هو إجراء يتضمّن إكراهها يحول دون النائب و بين ممارسته لأعمال نيابته و الذي يبدو أنّه لا يجوز تفتيش منزل النائب أثناء انعقاد البرلمان، في غير أحوال التلبس، إلّا إذا إذن بذلك المجلس المختصّ فالنصوص صريحة في عدم إجازة إتخاذ أية إجراءات جنائية ضد النائب قبل صدور الإذن من البرلمان ثم إنّ تفتيش المنزل فضلاً عما فيه من إعتداء على حرية النائب، تنتفي به الحكمة من تقرير مبدأ الحصانة، إذ يجعل النائب نهياً للقلق لا يأمن ما قد تتخذه السلطة التنفيذية قبله من إجراءات كيدية تستهدف الضغط عليه أو النيل منه و تؤدي شعور عائلته التي ينبغي أن يتوفّر الإطمئنان في دارها و ليس من شك في أنّ كل ذلك يؤثر على نفسية النائب و يقف حائلاً بينه و بين أداء واجبه في أمانة و حياد لذا يرى أغلب الفقه أنّه لا يجوز تفتيش منزل النائب أثناءه دون إذن من المجلس التابع له، إلّا في حالة التلبس بالجريمة. راجع: توفيق محمد الشاوي، المرجع السابق، ص 274-275، سامي حسني الحسيني، المرجع السابق، ص ص 216-217.

(ج) - حق الدفاع:

إذا كانت مصلحة المجتمع تقتضي الكشف عن الحقيقة و ضبط الأدلة المتعلقة بالجريمة مما يبرر الإعتداء على حق السر و إجراء تفتيش الأشخاص و المساكن، فإنّ المصلحة العامة لا يمكن حمايتها إلا إذا كان حقّ المتّهم في الدفاع عن نفسه بمنأى عن أيّ اعتداء، فحرية الدفاع عنصر من عناصر العدالة ذاتها و هي ما توجب ضرورة تمكين المتّهم من إثبات براءته إن استطاع حتّى لا يدان بريء لمجرد التسرع في الإتهام دون أن يكفل له المجتمع دفاعا حرا و من ثمّ فحقّ الدفاع يتعلّق بمصلحة الحقيقة⁽¹⁾. و لا شك في أنّ هذا الضمان جاء لحماية حقّ الدفاع و مهنة القائم به، و أنّ المحامي ملتزم بعدم إفشاء كل ما يتعلّق بسرّ مهنته و يقتضي إحترام هذا السرّ أن لا يجيز القانون الإطلاع عليه عن طريق التفتيش⁽²⁾.

يستتبع هذا الحظر عدم جواز تفتيش جميع الأوراق و المستندات الموجودة لدى المحامي عن المتّهم سواء كان موكلا من قبله أو منتدبا من قبل المحكمة و يسري هذا الحظر بالقطع منذ ثبوت صفته أنّه محام عن المتّهم حتّى و لو كانت الدّعوى لا تزال في مرحلة التّحقيق الإبتدائي و لم يوجّه الإتهام بعد للمتّهم⁽³⁾، و ذلك تحت طائلة البطلان ما لم يثبت مشاركة المحامي في هذا الفعل الجرمي⁽⁴⁾، و لو إنصبّ التفتيش على مجرد استشارات⁽⁵⁾، أو بريد إلكتروني يتعلّق بقضية أخرى غير تلك التي لأجلها صدر الإذن بالتفتيش⁽⁶⁾ بل حتّى و لو لم يثر نقيب المحامين اعتراضا بهذا الشأن نهائيا⁽⁷⁾.

(1) سامي حسني الحسيني، المرجع السابق، ص 2018.

(2) Derrida Fernand. Perquisitions et saisies chez les avocats, avoués et notaires, Revue de science criminelle et de droit pénal comparé, 1953, n° 2, p. 230

(3) حسام الدّين محمد أحمد، المرجع السابق، ص 141.

(4) Cass. Crim 27 juin 2001, n° 01-81.865, Bull. Crim.2001, n° 163.

(5) Cass. Com., 9 mars 1999, n° 96-16.559, Bull. Crim 1999, n° 54.

(6) Cass. Crim, 3 décembre 2006 N°: 06-82196, Bull. Crim 2006, n° 313.

(7) Cass. Crim, 25 juin 2013, pourvoi n° 12-88.021, Bull. Crim. 2013, n° 155.

في قرار حديث لها خطت محكمة النقض الفرنسية خطوات كبيرة نحو المحافظة على شرعية الإثبات المعلوماتي حيث اعتبرت أنّ الإنتهاك الإجرائي لحرية الدفاع إنّما يقع بمجرد ضبط مراسلات إلكترونية بين المتّهم و محاميه، دون اشتراط إدراك محتوى هذه المراسلة⁽¹⁾، و يشمل هذا الحظر تفتيش الشّخص و المنزل و المكتب و جميع المراسلات، كما يسري على الأحاديث الخاصة بين المتّهم و محاميه، لكن هذا الحظر محدود بغايته و هو حماية حق الدفاع، فلا يسري على ما يتلقاه من مراسلات من غير المتّهم بوصفه صديقا لا محاميا و تقدير ما يتعلّق بحقّ الدفاع يتوقّف على حقيقة الواقع لا على ما يثيره المحامي⁽²⁾.

و إذا كان المحامي متّهما بالضّلع في ارتكاب واقعة جرمية جاز تفتيش المعلومات المخزّنة بالأجهزة المتواجدة بمكتبه أو مسكنه على هذا الأساس، أمّا إذا أفضى التفتيش قبل المحامي إلى الضّبط العرضي لبعض المعلومات المتعلقة بدفاع موكله فإنّ مآل الضّبط هو البطلان الجزئي في حدود المعلومات المتعلقة بهذا الحق.

و هكذا يخضع تفتيش مكتب المحامي أو أنظمتها المعلوماتية إلى إجراءات خاصة بحيث يجب أن يتضمّن الإذن بالتفتيش تحديدا دقيقا لمبررات و موضوع التفتيش⁽³⁾، فلا يجوز تفتيش مكتب المحامي إلّا من قبل قاضي التحقيق المختصّ بحضور النقيب أو مندوبه أو بعد إخطارهما قانونا، و حضور النقيب عملية التفتيش عبّرت عنه المحكمة الأوروبية لحقوق

(1) يراجع بهذا الخصوص ، Cass. Crim., 24 avril 2013, n 12-80331, Bull. Crim 2013, n° 102 ، و قد جاء في هذا القرار:

" Attendu que, pour refuser de se prononcer sur le contenu des documents listés en pièce n° 8 par la société Medtronic et refuser d'annuler la saisie de la pièce n° 7 dont il admet qu'elle relève véritablement de la correspondance entre avocat et client, le premier président énonce que l'Autorité ne s'oppose pas à la restitution de ce document protégé et que la simple copie réalisée par celle-ci ne saurait constituer une atteinte disproportionnée au regard des intérêts en présence, la pertinence de la saisie ne pouvant s'apprécier que par la prise de connaissance de son contenu ; Mais attendu qu'en statuant ainsi, alors qu'il lui appartenait de rechercher si les pièces et supports informatiques dont la saisie était contestée par la société étaient ou non couverts par le secret professionnel entre un avocat et son client, et sans annuler la saisie de correspondances dont il a constaté qu'elles relevaient de la protection de ce secret et alors enfin que la violation dudit secret intervient dès que le document est saisi par les enquêteurs, le premier président a méconnu les textes susvisés et le principe ci-dessus rappelés "

(2) أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، المرجع السابق، ص 776.

(3) Cass. Crim 9 février 2016, 15-85.063, Bull. Crim 2016, n° 34

الإنسان بكونه "ضمان إجرائي خاص"⁽¹⁾، لذا نجد أغلب التشريعات قد نصّت على هذا الضابط الإجرائي سواء في قانون المحاماة⁽²⁾، أو بموجب قانون الإجراءات الجزائية⁽³⁾.

على أنّ ذلك لا يعني أنّ نقيب المحامين أو من يمثّله يعتبر طرفاً في تلك الإجراءات المتخذة بل يعتبر بمثابة حارس لحماية حق الدفاع⁽⁴⁾، و له الحق في بسط رقابته على عملية التفتيش قبل أيّ عملية ضبط محتمل و له أن يعترض على ضبط أي وثيقة عندما تكون هذه الأخيرة متعلّقة بجريمة غير تلك المذكورة في إذن التفتيش⁽⁵⁾، إلا أنّ القضاء الفرنسي لم يرتّب البطلان في حالة ما إذا تمّ ضبط وثائق مختلطة بمستندات رقمية تتمتع بالإمّياز بل أقرت ردها مع اعتبار باقي الإجراءات صحيحة⁽⁶⁾.

(1) CEDH, 21 janv. 2010, Da Silva c/ France, req. n° 43757/05.

(2) تنص للمادة 22 من القانون رقم 07/13 المؤرخ في 29 أكتوبر 2013 المتضمّن تنظيم مهنة المحاماة الصّادر بالجريدة الرّسمية المؤرخة في 30 أكتوبر 2013 عدد 55. "لا يمكن انتهاك حرمة مكتب المحامي. لا يتمّ أيّ تفتيش أو حجز في مكتب المحامي إلاّ من قبل القاضي المختص بحضور النقيب أو مندوبه أو بعد إخطارهما قانوناً.

تعد باطلّة الإجراءات المخالفة للأحكام المنصوص عليها في هذه المادة".

(3) Article 56-1 du CPPF dispose que ; " Les perquisitions dans le cabinet d'un avocat ou à son domicile ne peuvent être effectuées que par un magistrat et en présence du bâtonnier ou de son délégué, à la suite d'une décision écrite et motivée prise par ce magistrat, qui indique la nature de l'infraction ou des infractions sur lesquelles portent les investigations, les raisons justifiant la perquisition et l'objet de celle-ci. Le contenu de cette décision est porté dès le début de la perquisition à la connaissance du bâtonnier ou de son délégué par le magistrat. Celui-ci et le bâtonnier ou son délégué ont seuls le droit de consulter ou de prendre connaissance des documents ou des objets se trouvant sur les lieux préalablement à leur éventuelle saisie. Aucune saisie ne peut concerner des documents ou des objets relatifs à d'autres infractions que celles mentionnées dans la décision précitée. Les dispositions du présent alinéa sont édictées à peine de nullité."

(4) Cass. crim 8 janvier 2013, 12-90.063, Non publié au bulletin «Attendu que le bâtonnier de l'ordre des avocats n'est pas, au sens de l'article R. 49-21 du code de procédure pénale, une partie lorsqu'il exerce les prérogatives qui lui sont données par l'article 56-1 dudit code à l'occasion d'une perquisition dans un cabinet d'avocat, dès lors qu'il agit dans le cadre d'une mission d'auxiliaire de justice chargée de la protection des droits de la défense»

(5) Cass. Crim 25 juin 2013, 12-88.021, Bull. Crim 2013, n° 155 «le Bâtonnier ou son délégué est présent et exerce tout au long de la perquisition son contrôle avant toute éventuelle saisie d'un document en exprimant son opposition à la saisie lorsque celle-ci peut concerner d'autres infractions que celle mentionnée dans la décision»

(6) Cass. Crim 25 juin 2013, 12-88.021 , Bull. Crim 2013, n° 155 .

و يثار في هذا الصدد سؤال مفاده هل هذا القيد يسري على "التفتيش المعلوماتي عن بعد" بخصوص الأنظمة المعلوماتية التابعة لهؤلاء الأشخاص طالما أنّ التفتيش في هذه الأحوال لا يستوجب تفتيش مكتب المحامي أو منزله؟

رغم التعديلات الحديثة التي طالت قانون المحاماة، إلا أنّ المشرّع لم يلتفت إلى هذه المسألة بل أبقى الحصانة على مكتب المحاماة بمفهوم تقليدي، على الرغم أنّ هذا المفهوم بدأ يتراجع بالتوجه نحو الرقمنة، فالمشرّع نصّ على أنه "لا يتمّ أيّ تفتيش أو حجز في مكتب المحامي إلاّ من قبل القاضي المختصّ بحضور النقيب أو مندوبه أو بعد إخطارهما قانوناً"، و إن كانت عبارات النص واضحة فإنّ ذلك لا يجيز تفسير النص تفسيراً ضيقاً في حدود ظاهر عباراته، لأنّ ذلك يناقض غاية المشرّع التي ترمي إلى حماية حرّية الدفاع و حظر الإطلاع على أيّ مستند يتعلّق بهذا الحق أيّا كانت طبيعته و أيّا كان مكان تواجده، فالحماية المقرّرة في القانون إنّما تستهدف حماية حق الدفاع و ليس حصانة المكتب.

و في هذا الصدد ذكرت المحكمة الدستورية البلجيكية "لا تهدف السرية المهنية التي يلتزم بها المحامون و الأطباء إلى منح أيّ امتياز خاص بهم، و لكنّها تهدف في المقام الأوّل إلى حماية الحق الأساسي في احترام الحياة الخاصة للشخص الذي يثق بهم، و أحياناً فيما يتعلّق بما هو أكثر حميمية...، عندما يتمّ تفتيش هذه الأنظمة المعلوماتية فإنّ الأحكام المتعلقة بالتفتيش المادي الذي يحصل في المقرات المهنية للمحامين أو الأطباء قابلة للتطبيق و تسمح بضمان السرية المهنية، و مع ذلك فإنّ حالات التفتيش المنصوص عليها في المادة 39 مكرّر من قانون الإجراءات الجنائية، تتجاوز هذه الفرضية الدقيقة و يمكن تنفيذها خارج فرضية التفتيش ضمن المقرات المهنية"⁽¹⁾.

لذا نرى وجوب النص صراحة على حظر التفتيش الذي ينصّب على الأنظمة المعلوماتية للمحامين، فضلاً عن ذلك فإنّه ينبغي ضمان التبليغ الرسمي المسبق لنقيب المحامين بإذن قاضي التحقيق حال مباشرته إجراءات "التفتيش عن بعد" لكفالة حضوره هذه

(¹) l'arrêt n° 174/2018 du 6 décembre 2018 Numéro du rôle : 6711, paragraphe B 25, B26, disponible sur adresse <https://www.const-court.be/public/f/2018/2018-174f.pdf> (consulté le 19-12-2019).

العملية و لو لم يتم الإنتقال إلى مكتب المحامي أو منزله، لأنّ هذا القيد الإجرائي راجع إلى طبيعة حق الدفاع بحد ذاته، فهو "ينبع من القانون الطبيعي و روح القانون"⁽¹⁾.

ثانيا: استراتيجية مراجعة ملفات الحاسوبية في المحل المتمتع بالحصانة

إنّ أهمّ إشكالية تطرح بصدد بحث المحافظة على شرط مشروعية محل التفتيش، يتعلّق باختلاط الملفات ذات الإمتياز القانوني بغيرها من البيانات الحاسوبية المخزّنة، و المبدأ الذي أرسته محكمة النقض الفرنسية الرّامي إلى كفالة حماية هذه المعلومات أثناء الضّبط و قبل التفتيش أمر صعب للغاية بحكم العدد الهائل من البيانات التي قد تختلط بها.

و نجد أنّ المرشد الفيدرالي الأمريكي لتفتيش و ضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التّحقيقات الجنائية، أشار إلى كيفية التّعامل مع هذه البيانات خلال مرحلة ما بعد الضّبط، عندما تقوم سلطة التّحقيق بضبط حاسوب يحتوي على ملفات ذات امتيازات قانونية، يجب على طرف ثالث موثوق به فحص الحاسوب لتحديد الملفات التي تحتوي على مواد ذات الامتياز. و بعد مراجعة الملفات، سيقدّم الطّرف الثالث الملفات التي تتمتع بهذه الصّفة إلى جهة الإدعاء، و تختلف الممارسات المفضّلة لتحديد من سيقوم بتصفّح الملفات اختلافا كبيرا بين مختلف المحاكم.

و عموما توجد ثلاثة خيارات:

أولاً: يجوز للمحكمة نفسها أن تعيد النّظر في الملفات الموجودة في سرية.

ثانياً: يجوز للقاضي الذي يتولى الرّئاسة تعيين طرف ثالث محايد يعرف باسم "خبير خاص" و يعهد إليه مهمة مراجعة الملفات.

ثالثاً: تشكيل فريق من ممثلي الإدعاء أو أجهزة إنفاذ القانون الذين لا يعملون في القضية "فريقاً للتّصفية" للمساعدة في تنفيذ عملية البحث و مراجعة الملفات، و يقوم هذا الفريق بإعداد جدار يفصل بين الأدلّة وفريق المدعيين العموميين، الأمر الذي لا يسمح إلاّ بمرور الملفات التي ليست ذات إمتياز المميّزة من خلال هذا السّور⁽²⁾.

(¹) Derrida Fernand. Op cit, p 223.

(²) H. Marshall Jarrett, et al, op cit, p 110.

و بالنظر إلى أنّ الحاسوب يمكنه تخزين ملايين الملفات فإنّ القضاة نادرا ما يقومون بمراجعة ملفات الحاسوب بسرية في مكتب القاضي و عوضا عن ذلك الإختيار التّمودجي بين استخدام فريق ذو إمتياز أو طرف خاص فإنّ معظم المدعين العموميين يفضلون استخدام فريق في حالة موافقة المحكمة على ذلك و يمكن للفريق ذو الإمتياز القيام بفحص ملفات الحاسوب المضبوطة بسرعة في حين فإنّ تعيين أساتذة خصوصيون غالبا ما يستغرقون سنوات عديدة لإتمام العملية و من ناحية أخرى فقد أعربت بعض المحاكم عن عدم إرتياحها عن الفريق ذي الإمتياز⁽¹⁾.

في حين نجد أنّ محكمة النّقض الفرنسية قد استقرّت لمعالجة هذه الإشكالية على لزوم أن يلتزم قاضي الحرّيات و الحبس بتعيين خبير مختص في تقنية المعلومات يكلف بالقيام بعملية فرز للملفات و تحديد تلك التي تدخل في نطاق الإذن القضائي و استبعاد غيرها من نطاق الإسترداد⁽²⁾.

المبحث الثاني

الضوابط الشكلية للتفتيش عن الأدلة المعلوماتية

حرص المشرّع على حماية الحق في الخصوصية إزاء التفتيش الجنائي بنوعين من الضّمّانات الوقائية، تكون عضدا للضّمّانات الموضوعية في سبيل حفظ الحرّيات الفردية يتطلب الضّمّان الأول لزوم استصدار إذن قضائي مسبّب تجنبا لوقوع أيّ إنتهاك غير مبرّر (مطلب أول)، و يستوجب الضّمّان الثاني تنفيذ التفتيش بطريقة معقولة إبتغاء قصر نطاق هذا الإنتهاك في أضيق الحدود (مطلب ثاني).

⁽¹⁾ H. Marshall Jarrett, et al, Loc.Cit.

⁽²⁾ Cass. crim 25 juin 2013, 12-88.021 , Bull. crim 2013, n° 155 « Attendu qu'il résulte de l'arrêt attaqué et des pièces de la procédure que lors de la perquisition au cabinet de M. X..., ont été saisis deux ordinateurs et un disque dur ; que le juge des libertés et de la détention, après avoir considéré que la restitution des matériels serait de nature à faire obstacle à la manifestation de la vérité, a décidé que l'ouverture des scellés et la lecture des documents seraient effectuées par le magistrat instructeur, assisté de l'expert qu'il aurait commis préalablement, et en présence du bâtonnier ou de son délégué, en ajoutant que ne pourront être exploités que les documents en relation directe avec les faits objet de l'information en cours et que devront en être exclus les correspondances ou courriels entre M. X... et ses avocats concernant sa défense dans les procédures civiles lancées contre lui relatives aux mêmes faits »

المطلب الأول: الإذن بالتفتيش المعلوماتي

يمثل الإشراف القضائي على الإجراءات الجزائية أهمّ ضمان للحماية التي قررها القانون للحق في الخصوصية بما يتّوفر عليه القضاء من صفات الإستقلال إذ هو القادر على ضمان هذه الحرية في مواجهة أيّ خطر يهدّدها، تلك الرقابة التي يمارسها من خلال اشتراط إذن قضائي (فرع أول) صادر عن سلطة مختصة (فرع ثاني) ينفذ ضمن نطاق زمني محدد (فرع ثالث).

الفرع الأول: لزوم استصدار إذن مسبب بالتفتيش المعلوماتي

لا يمكن الحديث عن الشرعية الإجرائية بغير إشراف قضائي يضمن عدم تعسف السلطة و إنحرافها عن الغاية المتوخاة من الإجراء الجنائي، فيقتضي لمشروعية التفتيش لزوم صدور إذن مسبق يستهدف النظام المعلوماتي على وجه التحديد (أولاً)، و أن يتوقّر في إذن التفتيش مقوماته الشكلية (فقرة).

أولاً: التنظيم التشريعي و القضائي لشرط الإذن بالتفتيش المعلوماتي

نظراً للطبيعة الفريدة للأدلة المعلوماتية التي تمتاز بسهولة تدميرها و حذفها، فإننا نجد أنّ التشريعات تتّجه إلى فرض شرط يعدّ ركن جوهرى لصحة التفتيش، إذ لا يكفي صدور إذن عام لصحة التفتيش المعلومات، بل وجب التّصيص على النظام المعلوماتي ضمن الإذن (أ)، باستثناء بعض الحالات التي يستغى فيها عن الإذن المسبق (ب).

أ- ضرورة استصدار إذن بالتفتيش يستهدف النظام المعلوماتي على وجه التّصيص.

الإذن بالتفتيش تفويض يصدر من سلطة التحقيق المختصة إلى أحد مأموري الضبط القضائي، مخولاً إيّاه إجراء التفتيش الذي تختص به تلك السلطة، إذ تسري على الإذن بالتفتيش أحكام النّدب للتحقيق بوجه عام⁽¹⁾، و قد حرص المشرّع على حماية خصوصية المساكن من خلال إضفاء الطابع الدستوري على هذا الضابط الإجرائي، بحيث تنصّ المادة 47 من الدستور "تضمن الدولة عدم إنتهاك حرمة المسكن، فلا تفتيش إلاّ بمقتضى القانون، و في إطار إحترامه، و لا تفتيش إلاّ بأمر مكتوب صادر عن السلطة القضائية المختصة"، ثم

(1) سامي حسني الحسيني، المرجع السابق، ص 100.

تمسك المشرع مجدداً بهذا القيد ضمن المادة 44 من قانون الإجراءات الجزائية، بحيث أكد أنه "لا يجوز إجراء التفتيش إلا بعد الحصول على إذن مكتوب من السلطة القضائية المختصة".

و يعتبر الإذن القضائي المسبق بمثابة قاعدة وقائية تسعى إلى تجنب وقوع أي انتهاك غير مبرر على هذا الحق، غير أن هذا القيد لم يرد إلا بالنسبة لتفتيش المساكن على وجه التحديد، و سكت المشرع عن إجراءات التفتيش في محلات أخرى كتفتيش الشخص و سيارته، فهل يفيد ذلك أن التفتيش المنصّب على نظم المعلومات ينأى عن هذا الضابط الإجرائي؟ أو بعبارة أخرى هل صدور إذن بتفتيش المنزل أو السيارة أو الشخص ذاته يجيز ضمنا إمتداد التفتيش إلى الأجهزة الحاسوبية الموجودة بالمحل المأذون بتفتيشه؟

نصت المادة الثانية من التوصية الأوروبية بشأن الإجراءات الجزائية المتعلقة بتكنولوجيا المعلومات على أنه "يجب أن تسمح قوانين الإجراءات الجزائية لسلطات التحقيق بتفتيش نظم الحاسوب و ضبط البيانات ذات الأوضاع المقررة في نظم التفتيش و الضبط التقليدية"⁽¹⁾، و في مقابل ذلك نجد أن المشرع البلجيكي كان سابقا إلى إصدار القانون المؤرخ في 2000/11/28 بشأن تعديل قانون التحقيق الجنائي مضيفا المادة (88ter) التي تضمن إختصاص قاضي التحقيق بإصدار إذن بتفتيش نظم المعلومات **systeme informatique** على وجه التخصيص.

الحقيقة أن بين الأمرين آثار مختلفة تترتب، فإذا اعتبرنا أن الحاسوب جزء من المكان الذي يتم تفتيشه فإن ذلك يترتب عليه أن مجرد إصدار أمر تفتيش لهذا المكان فإن هذا الأمر يشمل تفتيش الحاسوب المذكور، أما إذا اعتبرنا أن التفتيش لكي يتم على الأنظمة المعلوماتية فإنه يجب أن يتم تضمين الأنظمة المعلوماتية في إذن التفتيش تخصيصا إلى جوار الصيغة العامة التي يتضمنها إذن التفتيش لكون الحاسوب متميزا عن المحتويات العادية لمنزل المتهم

(1) Recommandation n° R(95)13 du Comité des Ministres aux Etats membres relative aux problèmes de procédure pénale liés à la technologie de l'information. (Adoptée par le Comité des Ministres le 11 septembre 1995, lors de la 543e réunion des Délégués des Ministres) " Les lois de procédure pénale devraient permettre aux autorités chargées de l'enquête de perquisitionner dans les systèmes informatiques et d'y saisir des données, dans des conditions similaires à celles utilisées dans le cadre des pouvoirs traditionnels de perquisition et de saisie. La personne en charge du système devrait être informée que le système a fait l'objet d'une perquisition et de la nature des données saisies. Les recours juridiques prévus par la législation en général contre la perquisition et la saisie devraient être également applicables en cas de perquisition d'un système informatique et de saisie des données qui y sont contenues."

بل و حتى للمتَّهم ذاته إذا كان يحمل حاسوباً مصغراً عبر ساعته أو جهاز النِّقال الخاص به... إلخ، فإنَّه في هذه الحالة يجب أن يكون أذن التفتيش مشمولاً بتحديد معيّن لجهاز الحاسوب، بحيث لا يكفي في هذه الحالة الصّيغة العامة و إنّما يجب أن يتضمّن في أذن التفتيش تحديداً دقيقاً للحاسوب المراد تفتيشه و عدد الأجهزة المراد تفتيشها و أيضاً مراعاة الجريمة التي صدر أذن التفتيش بناءً عليها بحيث لا يكون هناك شمول أو عمومية في هذا الإطار مما يعني لزوم مراعاة تطبيق مبدأ الغاية من التفتيش بشكل كامل⁽¹⁾.

من المسلّم به جدلاً في الوقت الحالي أنّ النّظام المعلوماتي واقع في دائرة الخصوصية⁽²⁾، بحكم ما يتضمّنه من بيانات خاصة⁽³⁾، لذا فإنَّه فلا يجوز تفتيشه إلاّ بموجب إذن قضائي مسبق يحدّد فئات معيَّنة من الملفات على أنّها "الأشياء" التي يتعيّن "ضبطها" من

(1) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، المرجع السابق، ص 854.

(2) Le considérant 24 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques précise que : « L'équipement terminal de l'utilisateur d'un réseau de communications électroniques ainsi que toute information stockée sur cet équipement relèvent de la vie privée de l'utilisateur, qui doit être protégée au titre de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ».

(3) يرجع كل من الفقه و القضاء الأسباب الدّاعية إلى إضفاء حماية إجرائية للبيانات أكثر من الحماية التي تتمتع بها المساكن لعدة جوانب و مظاهر تتميز بها أجهزة الحاسوب و ما في حكمها، أولاً أجهزة الحاسوب هي عبارة عن مستودعا لعالم غير محدود من المعلومات، بعضها يتعلّق بأخص شؤون الفرد و أكثرها إتصافاً به ثانياً: تحتوي هذه الأجهزة على معلومات يتم توليدها تلقائياً، و كثيرا ما يكون ذلك دون علم المستخدم فمعظم متصفحات الويب مثلا مبرمجة للإحتفاظ تلقائياً بالمعلومات عن المواقع التي زارها المستخدم من أجل مساعدة المستخدم على تتبّع خطواته الإلكترونيّة، هذه المعلومات يمكن أيضا أن تمكّن المحقّقين من "الإطلاع على التفاصيل الدّقيقة عن مصالح المستخدم وعاداته و هويته، مستعينة بسجل أنشأه المستخدم دون قصد. ثالثاً، يحتفظ الحاسوب بالملفات و البيانات حتى بعد أن يعتقد المستخدم أنّه قام بحذفها، فعندما يتمّ حذف الملف فإنّ محتوى الملف يمكن إسترداده ذلك أنّ المساحة التي كان يشغلها الملف تظلّ متاحة كما كانت قبل الحذف، إذا لم يتمّ نظام التّشغيل بإعادة استخدام هذه المساحة لملف آخر سيظلّ الملف المحدّد للحذف متاحاً لاستعادته، و بهذا يمكن استرداد كمّية كبيرة من البيانات من المساحة الفارغة slack space على القرص الصّلب، فالحذف يعني إخفاءه من مجال الرّؤية الخاصة بالمستخدم رابعاً، نادراً ما تكون الحواسيب كيانات مستقلة بذاتها و عند الإتصال بالأنترنت تصبح بمثابة بوابات إلى كمية غير محدودة تقريباً من المعلومات التي يتمّ مشاركتها بين مختلف المستخدمين و يتمّ تخزينها في أيّ مكان في العالم.

يراجع بهذا الخصوص :

Chan Gerald, op cit, pp 438-439.

وسائط التخزين⁽¹⁾، لذا تولى القضاء الأمريكي عن سوابقه القضائية التي أرست قياساً بين تفتيش الحاويات التقليدية و أجهزة التخزين الرقمية منذ عقدين⁽²⁾. وهذا ما أكدته الدائرة الفيدرالية التاسعة في قضية **United States v. Payton** حيث قرّرت "يجب عدم النظر إلى الحواسيب باعتبارها مجرد حاوية، وأن صدور إذن بتفتيش مكان ما يسمح بتفتيشها طالما كان من الممكن وجود الأدلة المطلوبة بداخلها دون أن يصدر إذن صريح يجيز تفتيش الأجهزة الحاسوبية"⁽³⁾.

(¹) Josh Goldfoot, op cit, p 120.

(²) United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008).

جاء في القرار الصادر عن الدائرة الفيدرالية التاسعة في قضية **United States v. Giberson** ما يلي: "يمكن أن تكون الحواسيب مستودعات للوثائق والسجلات مثل حقائب السفر وغيرها و لم تتح لنا الفرصة بعد لتحديد ما إذا كانت الحواسيب استثناء من المبدأ العام الذي مفاده أن الإذن الذي يجيز ضبط وثائق معينة يأذن أيضاً بتفتيش حاوية يحتمل أن تحتوي على تلك الوثائق. ونرى أنه في هذه الحالة، حيث توجد قرائن على أن الوثائق التي يستهدفها الإذن القضائي يمكن العثور عليها على حاسوب المتهم، فإن الضباط لم يتجاوزوا نطاق الإذن بضبط الحاسوب... لقد كان من المعقول في هذه الحالة أن تعتقد الضبطية القضائية أن الوثائق المحددة في الإذن قد توجد على جهاز الكمبيوتر الخاص به. و بدلاً من ذلك، يدفع المتهم بأن القياس بين الحاسوب و "الحاويات" الأخرى غير مناسب لأن الحواسيب تتمتع بحماية أكبر على نحو لا يمكن تفتيشها إلا عند التنصيص عليها في الإذن... على الرغم من أن المتهم يقدم العديد من الأسس المنطقية لمعالجة أجهزة الحاسوب بشكل مختلف عن وسائل التخزين كخزائن الملفات و حقائب السفر... القول بأن أجهزة الحاسوب قادرة على تخزين كميات هائلة من المعلومات اللامادية، المخزنة رقمياً، على نحو يوجب تمييزها عن باقي حاويات التخزين العادية، فإن كمية المعلومات، أو الشكل الذي يتم تخزينه بها، لا صلة لها في إطار التعديل الدستوري الرابع... ليس هناك سبب يجيز تفتيش غرفة كاملة من خزائن ملفات أو مكتبة كاملة و لا يسمح بتفتيش حاسوب، و من شأن إستثناء الذي يدعيه المتهم أن يثير إشكاليات فيما يتعلق بتفتيش الأجهزة ذات القدرات التخزينية المماثلة. إذا لم نسمح بتفتيش أجهزة الحاسوب، فماذا عن محرك أقراص أو جهاز تخزين خارجي آخر؟ لا يقدم استثناء المتهم أي إجابات على هذه الأسئلة و بالمثل فإن محاولة الحد من عمليات التفتيش إستناداً إلى شكل المعلومات المخزنة ستكون تعسفية، الاستثناء المثار يثير أسئلة أكثر من الأجوبة... و هنا، فإن المبدأ الوحيد الذي يمكننا أن نستقر عليه هو المبدأ الذي سبق أن وضعته هذه المحكمة: أنه لتفتيش حاوية يجب أن يكون من المعقول توقع العثور على الأشياء المذكورة في إذن التفتيش. إذا كان من المعقول الاعتقاد بأن جهاز الحاسوب يحتوي على العناصر المذكورة في الإذن، يجوز للضباط تفتيشه...".

United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008).

(³) United States v. Payton, F.3d , 2009 WL 2151348 (9th Cir. July 21, 2009).

و في هذه القضية صدر إذن بتفتيش منزل المتهم Payton بحثاً عن مواد مخدرة و أية سجلات أخرى تشير إلى الإتجار بالمخدرات، غير أن عملية التفتيش امتدت إلى تفتيش الحاسوب بحجة أن السجلات أو الدفاتر التي تشير

حقيقة الأمر أنّ هذا الضمان الإجرائي قد تعرض له المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات حيث نصّت التوصية الحادية عشر منه بأن "كلّ إجراء يتخذ بواسطة سلطة رسمية و يمسّ بالحقوق الأساسية للمتّهم - ومنها الإجراءات التي تتخذها الضبّطية القضائية- يجب أن تكون مسموح بها عن طريق القاضي أو خاضعة لرقابته⁽¹⁾، لذا نجد أنّ التشريعات قد أولت أهمية بالغة لهذا القيد بالنصّ عليه صراحة، لأنّه يعتبر من الضمانات الجوهرية لحماية حق الخصوصية⁽²⁾.

وبالرجوع إلى القانون رقم 04/09 و البحث في مدى التقييد بهذا الضابط من عدمه عند القيام بإجراء التفتيش الإلكتروني، فإنّنا نجد أنّ المادة 05 من هذا القانون المنظمة لهذا النوع من التفتيش لا تنص صراحة على وجوب إستصدار ضباط الشرطة القضائية إذنا مسبقا بتفتيش المنظومات المعلوماتية كما هو الشأن بالنسبة لمراقبة الاتصالات الإلكترونية، و بالتالي فإنّه يفهم ضمنا من هذا النصّ القانوني أنّ المشرّع أبقى على المبادئ التقليدية التي تنظم هذه المسألة و التي تجد سندها في القاعدة التقليدية التي مؤداها أنّ ما يحمله الأفراد من أمتعة لا تخضع للضمانات و القواعد المقررة لتفتيش المساكن.

و بناء على ذلك فحرمة الأنظمة المعلوماتية مستمدة من إتصالها بشخص صاحبها أو حائزها و من ثمّ يسري على تفتيشها أحكام تفتيش الأشخاص طالما هي في حيازة صاحبها أو برضائه، أمّا إذا كانت هذه الأجهزة داخل أحد ملحقات المسكن فهي تأخذ حكم المكان

إلى تجارة المخدرات يعتقد أنّ تكون موجودة على الحاسوب و طعن المتّهم بأنّ إذن التفتيش لم يأذن صراحة بتفتيش حاسوبه و أنّ نطاق التفتيش للبحث عن المواد المخدرة و الملفات أو السجلات أو الدفاتر التي تشير إلى تجارتها لا يمتدّ إلى تفتيش الحاسوب، و قد قبلت الدائرة الفيدرالية التاسعة طعنه أنّ تفتيش جهاز الحاسوب دون إذن صريح بذلك يعدّ انتهاكا للتعديل الدستوري الرابع حيث لم يكن هناك أيّ شيء موجود في موقع التفتيش يشير إلى أنّ السجلات التي تقع ضمن نطاق الإذن بالتفتيش يمكن العثور عليها عبر الولوج إلى الحاسوب، و قرّرت أنّه لا يجب النّظر إلى الحاسوب باعتبارها مجرد حاوية و أنّ صدور إذن تفتيش مكان ما يسمح بتفتيشها، و استلزمت أن يصدر إذنا يحدّد أنّ المراد من التفتيش هو الأجهزة الحاسوبية على وجه التّحديد.

United States v. Payton, F.3d, 2009 WL 2151348 (9th Cir. July 21, 2009).

(¹) XVIème Congrès International de Droit Pénal , op cit, p 37.

(²) كالتّشريع الفرنسي(المادة 56، 97 من قانون الاجراءات الجزائية)، و التّشريع المصري (المادة 6 من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات) و التّشريع البحريني (المادة 15 من القانون رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات).

المسكون فلا بد من استصدار إذن قضائي مسبب قبل التفتيش، و هو موقف ما يمثل في نظرنا خروجاً على أصول الشريعة الإجرائية التي تقتض البراءة في المتهم و تخضع الإجراءات وجوباً لإشراف القضاء⁽¹⁾، و لا يمكن القول بخلاف ذلك بإعمال القياس بين حرمة المسكن و حرمة النظام المعلوماتي لأن حرمة المسكن وردت على سبيل الاستثناء و الاستثناء لا يقاس عليه⁽²⁾.

و لأنه من غير المعقول أن يكون التفتيش دون إذن قضائي يجيز أكثر مما يبيحه التفتيش المأذون به، كون خصوصية النظام المعلوماتي تتجاوز خصوصية المسكن كما سبق و أن توصلنا إليه، و حجتنا في ذلك هو موقف المشرع الدستوري الذي استدرج حديثاً هذا القصور و حسم الخلاف نهائياً ضمن التعديل الدستوري لسنة 2016، حيث حرص - في

(1) غالبية الفقه يسلّمون جدلاً باشتراك هذا القيد الإجرائي وفقاً للتشريع الجزائري و إن لم يتم النص عليه صراحة من منطلق الحرمة التي تتمتع بها النظام المعلوماتي و مع ذلك فإن هذا التوجه الفقهي لا يقدم تفسيراً منطقياً يدعم موقفه، انظر على سبيل المثال: إبراهيمي جمال، المرجع السابق، ص 39. بن طالب ليندا، الدليل الإلكتروني و دوره في الإثبات الجنائي دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تيزي وزو، 2019، ص 65.

(2) حيث أنه يتبين من المادة 44 من قانون الإجراءات الجزائية أن المشرع العادي قد فرّق في الحكم بين تفتيش الأشخاص و السيارات و غيرها من المحال القابلة للتفتيش و تفتيش المساكن، فيما يتعلّق بضرورة أن يتم التفتيش في الحالة الأخيرة بأمر قضائي ممن له سلطة التحقيق كضمانة أساسية لحصول التفتيش تحت إشراف مسبق من القضاء. فقد استنتجت هذه المادة عدا المسكن من هذه الضمانة، و لا يمكن تفسير سكوت المشرع على أنه لا يفرّق بين الحالتين (المساكن و النظم المعلوماتية) بدليل أن المشرع و بنص المادة 4 من القانون 04/09 و عند معالجة ضوابط المراقبة الإلكترونية لم يسقط هذه الضمانة بل اشترطها بنص واضح الدلالة، و إن لم يفعل ذلك بشأن التفتيش فإنه يكون قد عبّر صراحة على عدم اشتراط إذن قضائي مسبق يحدّد النظام المعلوماتي كمحل للتفتيش المعلوماتي، بل يستمدّ حرمة من المكان الذي يوجد به. و لا يغيّر من ذلك ما جاء بالمادة 5 من القانون 09/04 بقولها "يجوز تمديد التفتيش بسرعة إلى هذه المنظومة بعد إعلام السلطة القضائية المختصة مسبقاً بذلك"، فهذه العبارة لا تعني اشتراط الإذن المسبق للتفتيش المعلوماتي لأنّ الإعلام لا يحل محل الإذن القضائي و لا يحمل مقوماته، فضلاً على ذلك فإنّ امتداد التفتيش يعتبر أخطر من التفتيش المحدّد مسبقاً لأنه يأخذ حكم التفتيش العام و الإستكشافي لعدد كبير من أعضاء الهيئة الإجتماعية و ليس قاصراً على شخص المتهم كما هو حاصل في التفتيش المعلوماتي الأولي، كما أنه لا يخضع لأيّ ضمان إجرائي كما سنرى لاحقاً، و رغم خطورته على الحرّيات الفردية إلا المشرع أن لم يستوجب الإذن القضائي بل إكتفى بضرورة إعلام السلطة القضائية، فلو اشترط المشرع العادي الإذن القضائي لكان الأولى به النص عليه عند الحديث عن إمتداد التفتيش و ليس التفتيش الأولي، و صونا لحرمة النظام المعلوماتي التي تنبثق من الحرّية الشخصية التي تتعلّق بكيان الفرد و حياته الخاصة و أسراره و يجب التأكيد على عدم جواز تفتيشه ما لم يصدر أمر قضائي مسبق و محدّد يستهدف النظام المعلوماتي على وجه التحديد.

سبيل حماية الحرّيات العامة- على كفالة حرمة الحياة الخاصة للأفراد فأكدت المادة 47 المستحدثة بموجب هذا التعديل الدستوري على أنه "لا يجوز انتهاك حرمة حياة المواطن الخاصة، و حرمة شرفه، و يحميها القانون، سرية المراسلات و الاتصالات الخاصة بكل أشكالها مضمونة، لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السّلطة القضائية و يعاقب القانون على انتهاك هذا الحكم"، مما مؤداه أنّ هذا النصّ الدستوري يستلزم لمشروعية أيّ إجراء ينتهك الحق في الخصوصية-بغض النظر عن تكييفه القانوني- ضرورة صدور أمر قضائي مسبق و مسبب يجيزه.

على أنه ينبغي الحذر عند تفسير هذا النصّ الدستوري، فالدستور اكتفى في الفقرة الأولى في تقرير هذه الحماية بإيراد ذلك في عبارات عامة (لا يجوز انتهاك حرمة حياة المواطن الخاصة)، ثم خصّص بالحماية ما يتفرّع عن هذا الحق في الفقرة الثانية (سرية المراسلات و الاتصالات الخاصة بكل أشكالها مضمونة)، إلّا أنه لم يفرّق بين ما يتفرّع عن هذا الحق بخصوص ضمان الإشراف القضائي المسبق على كل إجراء ينتهك التوقع المعقول للحق في الخصوصية كما يقطع بذلك عموم نص الفقرة الثالثة (لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السّلطة القضائية)، و قد جاءت هذه الفقرة عامة مطلقة لم يرد عليها ما يخصّها أو يقيدّها.

و هذا ما جرّنا إلى القول بأنّ المادة 5 من القانون 04/09 التي تخوّل للضبطية القضائية الحق في التفتيش المعلوماتي دون لزوم استصدار إذن قضائي يستهدف النظام المعلوماتي على وجه التحديد، قد أصبح مخالفاً للدستور الذي يحظر إتخاذ أيّ إجراء ينتهك الحياة الخاصة للفرد دون إذن قضائي سابق، و لكون التعديل الدستوري كان لاحقاً عن سن هذا النصّ القانوني، فإنّ مؤدى ذلك صيرورة نص المادة 5 منسوخ ضمناً (ملغى) بقوة الدستور، و بطبيعة الحال فإنّ هذا الإلغاء لا يخرج عن حدود التعارض، و ذلك طبقاً للمبدأ العام الذي يقرّر أنّ اللاحق ينسخ السابق إذا كان مساوياً له في الدرجة أو أعلى منه دون الحاجة إلى النص صراحة على هذا النسخ، و إن كنّا نرى الأولى بالنص صراحة على هذا الضمان الإجرائي.

كما أنه ينبغي الإشارة إلى أنّ المادة 46 من الدستور تستغرق المادة الموالية لها، فالمادة 46 وردت عامة تفرض الإذن القضائي المسبق كشرط لإتيان أيّ إجراء ينطوي على تهديد للحياة الخاصة للأفراد بينما، وردت المادة 47 من الدستور كاستثناء بحيث خصّصت

المنزل دون غيره من هذا الضمان الإجرائي، لذا يجب حذفها منعاً من التوسع في تأويل النصوص بما يناقض بعضها بعضاً.

(ب) - حالات التفتيش المعلوماتي بدون إذن قضائي

تتعدد حالات التفتيش المعلوماتي بدون إذن قضائي في مختلف التشريعات سواء كان ذلك لظروف طارئة (1) أو في أحوال القبض على الأشخاص (2).

(1) - التفتيش بدون إذن قضائي لظروف طارئة

تعدّ الظروف الطارئة استثناءً على تطلب إذن مسبق بالتفتيش، لذا يجوز الإستغناء على هذا القيد الإجرائي متى تحققت حالة من حالات الظروف الطارئة، إذا كانت الأدلة معرضة لخطر التدمير الوشيك، أو أن يكون هناك تهديد للجمهور أو ما يعرض الضبطية القضائية للخطر، أو بصدد حالات المطاردة الشديدة، أو لمنع هروب المشتبه به قبل أن تتمكن الضبطية القضائية من الحصول على إذن بالتفتيش، و تعدّ الحالة الأولى أهمّ حالة بشأن الأدلة المعلوماتية و هي الخشية من تدمير الأدلة ، و لتقدير مدى توافر الظروف الطارئة يجب النظر إلى درجة الخطورة في ضوء مقدار الوقت اللازم للحصول على إذن التفتيش⁽¹⁾.

و لتقدير ما إذا كانت الظروف الطارئة لها وجود، فإنه يجب على الضبطية القضائية الأخذ بعين الاعتبار خمسة أوضاع (1: درجة الوضع الطارئ، 2) مقدار المدّة الزمنية اللازمة للحصول على إذن التفتيش، 3) ما إذا كان الدليل على وشك الإختفاء أو التدمير، 4) إمكانية حدوث خطر في الموقع، 5) ما إذا كان الحائزون للمواد المجرّمة على علم بكون الضبطية في طريقها إليهم، 6) قابلية المواد للتدمير الفوري⁽²⁾.

(1) H. Marshall Jarrett, et al, op cit, pp 27-28.

(2) H. Marshall Jarrett, et al, op cit, p 28 : " In determining whether exigent circumstances exist, agents should consider:

1. the degree of urgency involved,
2. the amount of time necessary to obtain a warrant,
3. whether the evidence is about to be removed or destroyed, (4) the possibility of danger at the site,
4. whether those in possession of the contraband know that the police are on their trail,
5. the ready destructibility of the contraband. »

غالباً ما تقوم و تتحقق الظروف الطارئة في حالة التفتيش عن الأدلة المعلوماتية، لأنّ البيانات المحوسبة قابلة بطبيعتها للتلف، ذلك أنّ الأوامر الموجهة للحاسوب يمكنها أن تؤدي إلى تدمير البيانات في ثوان معدودات، كما يمكن للرطوبة و الحرارة و المجالات المغناطيسية التي تنشأ على سبيل المثال بواسطة تمرير مغناطيس قوي على القرص أن تفضي إلى هذه النتيجة⁽¹⁾، و هكذا لاحظ القضاء "أنّه تمّ التوصل إلى الظروف قد بررت تنزيل البيانات من حاسوب في روسيا بدون إذن قضائي، لوجود سبب وجيه للإعتقاد بأنّ الحاسوب الروسي يحتوي على أدلة متعلّقة بالجريمة، حيث يوجد سبب معقول للتخوف من أن يؤدي التأخير إلى تدمير الأدلة أو فقدانها، و حيث قام الضابط القضائي بنسخ البيانات فقط ثم حصل بعد ذلك على إذن بالتفتيش⁽²⁾.

و من الأهمية بمكان الإشارة إلى أنّ التفتيش المعلوماتي بدون إذن قضائي لا بد أن يكون مقيداً بشكل صارم بالضروريات التي تبرّر الشروع في التفتيش، و هي أنّ الظروف الطارئة التي تدعم و تبرّر ضبط الحاسوب بدون إذن قضائي، قد لا تكفي لتبرير التفتيش المعلوماتي اللائق، و بالتالي فإنّ الحاجة إلى ضبط حاوية لمنع تدمير الأدلة لا تسمح بالضرورة للضبطية القضائية باتخاذ خطوات أخرى دون إذن قضائي⁽³⁾.

(¹) و هذا ما تم تقريره في قضية Miguel Valder، و تتلخص وقائع الدعوى في أنّ ضابط الشرطة قام بالقبض على المتهم وفقاً لأمر بالقبض عليه لتورطه في جريمة الإتجار بالمخدرات، و في هذا الوقت قام ضابط الشرطة بتفتيش الهاتف المحمول للمتهم، و اطّلع على دفتر العناوين التي اتصل بها الهاتف، و دفع المتهم بضرورة بطلان الأدلة المستمدة من تفتيش هاتفه لأنّها كانت بدون إذن تفتيش، كتب القاضي تقريراً للردّ على هذا الدّفع في ضوء القاعدة الفيدرالية (3)(b)59 من قواعد الإجراءات الجنائية، و جاء في التقرير أنّ الضابط شهد أنّه قام بالتفتيش بدون إذن لأنّه كان قلقاً من أنّ المعلومات الموجودة في ذاكرة الهاتف يمكن أن تمحى عن بعد، و أنّه باستعراض ذاكرة الاتصال بالهاتف عرف أنّ المتهم كان على اتصال بشركائه في الجريمة، و بفحص الهاتف فقد ثبت أنّ الهاتف كان بالفعل مجهّزاً لحذف كل محتويات الاتصال مما يجعل من قلق الضابط حول إتلاف الأدلة قلقاً مشروعاً.

هذه التطبيقات القضائية مذكور لدى: محمود عبد الغني فريد جاد المولى، المرجع السابق، ص 171 و ما بعدها.

(2) United States v. Gorshkov, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001), citing

H. Marshall Jarrett, et al, op cit, p 29.

(³) H. Marshall Jarrett, et al, p 30.

و بذلك يكون القضاء الأمريكي قد أرسى قاعدة عامة مبناها أنّ الظروف الاستثنائية التي تسمح بالضبط المادي لأجهزة التخزين الرقمية بدون إذن قضائي، لا تسمح بالتفتيش بدون إذن، لأنّ الضرورة مقدّرة بقدرها و هي منع تدمير الدليل فقط.

على أنّ السؤال الذي يفرض نفسه هنا يتعلّق مضمونه ببحث مدى اعتماد المشرّع الجزائري لهذه القاعدة؟

لا يوجد في القانون الجزائري رقم 09-04 المتضمّن القواعد الخاصة للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها أو قانون الإجراءات الجزائية إشارة صريحة إلى هذه القاعدة، غير أنّه في نظرنا متى توفّر الاعتقاد بوجود حالة من حالات الطوارئ المذكورة أعلاه جاز لضابط الشرطة القضائية القيام بالضبط المادي لأجهزة التخزين الرقمية دون تجاوز هذا الحد من الإجراءات و ذلك لسببين رئيسيين، يرجع الأول إلى طبيعة الأدلة المعلوماتية التي تمتاز بسهولة محوها و تدميرها أو على الأقل تعديلها، و من جهة ثانية فإنّ الضبط المادي لا يشكّل تقييدا كبيرا للحريّة الشخصية، إذ يظهر بشكل جلي تحقّق مبدأ التناسب في هذه الحالة، على أنّه ينبغي على الضبطية القضائية اللجوء فورا لتبليغ النيابة العامة بالإجراء المتخذ، لاستصدار إذن يسمح بالتفتيش المعلوماتي طبقا لنص المادة 46 من الدستور.

و بالإمكان إستنباط هذه القاعدة من المادة 42 من قانون الإجراءات الجزائية المتعلقة بإجراءات جمع الأدلة في حالة التلبس و التي تنصّ " يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس أن يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية و يتخذ جميع التحريات اللاّزمة و عليه أن يسهر على المحافظة على الآثار التي يخشى أن تختفي و أن يضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة..."، و بطبيعة الحال فإنّ الضبط في هذه الأحوال يقتصر فقط على الأجهزة المادّية الواقعة خارج المساكن، لأنّه في غير هذه الأحوال فإنّ الإذن القضائي لدخول المساكن يقع واجبا تحت طائلة البطلان إلّزاما بنص المادة 47 من الدستور و المادة 44 من قانون الإجراءات الجزائية.

(2) - التفتيش بناء على القبض على الأشخاص

لم ينظم قانون الإجراءات الجزائية تفتيش الأشخاص المشتبه فيهم أو المتهمين، إلا أنّ الفقه يرى أنّ تفتيش الشّخص يكون في حالتين إمّا أن يكون تفتيشاً مكمّلاً لتفتيش المسكن، و تلك الحالة التي سبق مناقشتها، و توصلنا إلى عدم جواز إمتداد تفتيش المسكن إلى النّظام المعلوماتي، أمّا الحالة الثّانية فهي تتعلّق بتفتيش الشّخص في حالة القبض عليه تطبيقاً للمادة 4/51 من قانون الإجراءات الجزائية، أو تنفيذاً لأمر قضائي بالقبض تطبيقاً لحكم المادة 120 من نفس القانون، فيجوز القيام بتفتيش المقبوض عليه و هو تفتيش مقترن بالقبض في حالة التلبس بالجناية أو الجنحة أو تنفيذاً لأمر بالقبض صادر عن قاضي التّحقيق⁽¹⁾.

و علة هذه القاعدة أنّه ما دام يجوز التّعرض لحرية الشّخص بالقبض عليه فيجوز تفتيشه، فتفتيش الشّخص أقلّ خطورة من القبض عليه أو أنّ القبض على المتّهم يتضمّن اعتداء على حرّيته الشّخصية بما يجاوز التّفتيش فإذا أهدرت حرّية الشّخص بالقبض عليه فإنّ ذلك يستتبع التّسليم بحق الضّبطية القضاية في تفتيشه⁽²⁾، و هذه القاعدة العامّة التي تضمّنتها مختلف التّشريعات و التي مفادها جواز تفتيش الشّخص في حالة القبض عليه، هل تسري أيضاً على النّظام المعلوماتي الذي يكون بحوزة المقبوض عليه لحظة القبض؟

من الأمثلة النّمودجية للقوانين التي نصّت على جواز تفتيش النّظم المعلوماتية بناء على القبض على الأشخاص، قانون سوء إستخدام الحاسب الآلي في إنجلترا، فالجرائم المدرجة في القسمين الثّاني و الثّالث من قانون سوء إستخدام الحاسب الآلي يعاقب عليها عند الإدانة بعقوبة السّجن لمدة خمسة سنوات حد أقصى، و ذلك يعني أنّ هذه النّوعية من الجرائم تستدعي القبض على المتّهم طبقاً لقانون الشّرطة و الإثبات الجنائي لسنة 1984، و بالتّالي لرجل الشّرطة القبض على المتّهم دون حاجة لاستصدار إذن قضائي بالقبض كما أنّ له تفتيش محل إقامة المتّهم بحثاً على أدلة ذات قيمة تتعلّق بالجريمة المعلوماتية التي تمّ القبض عليه بسببها⁽³⁾.

(1) عبد الله اوهابيه، شرح قانون الإجراءات الجزائية الجزائريّ التّحري و التّحقيق، الطّبعة الثّانية، دار هومة، الجزائر، 2011، ص ص 277-278.

(2) هلاي عبد الله أحمد، المرجع السابق، ص 154.

(3) نفس المرجع السابق، ص 156.

و يتجه غالبية الفقه إلى القول بانطباق هذه القاعدة على التفتيش المعلوماتي قياساً على تفتيش الأشخاص، لأنّ البرامج و المعلومات و لئن كان لها حرمة فإنّ حرمتها مستمدة من حرمة الشّخص الذي يحوزها فإنّ جاز تفتيشه جاز تفتيشها، و من ثمة فإنّه يجوز للضّبطية القضائية عند التّلبس إجراء التفتيش المعلوماتي⁽¹⁾، لأنّ التفتيش في حالة التّلبس لا يشمل جسم الشّخص فحسب، بل كذلك ما يحمله من متاع، و بالتّالي تندرج أجهزة التخزين الرّقمية تحت مسمى المتاع، و هو مذهب تبناه القضاء المصري⁽²⁾.

أمّا المشرّع الفرنسي فقد استوجب هذا الضّمان الإجرائي حتّى في حالة التّلبس بموجب المادّة 56 من قانون الإجراءات الجزائية، بل إنّ المجلس الدّستوري الفرنسي شدّد هذا الضّمان حتّى في حالة الطّروف الاستثنائية، أين قرّر وجوب حصول السّلطة الإدارية مسبقاً على إذن من القاضي الإداري الإستعجالي للقيام بهذا الإجراء⁽³⁾، و قد تواترت أحكام القضاء الأمريكي على اعتماد هذه القاعدة و تطبيقها لمدة تزيد عن عقدين من الزّمن إلى غاية صدور القرار التّاريخي للمحكمة العليا الفيدرالية في قضية Riley v. California⁽⁴⁾.

(1) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، المرجع السّابق، ص 860، هلاي عبد الله أحمد، المرجع السّابق، ص 156، محمود محود محمود جابر، المرجع السّابق، ص 193.

(2) قرار محكمة النقض المصرية في الطّعن رقم 15854، لسنة 84 قضائية، بتاريخ 2015/02/23.

(3) Décision n° 2016-536, QPC du 19 février 2016" 12. En dernier lieu, l'exploitation des données saisies nécessite l'autorisation préalable du juge des référés du tribunal administratif, saisi à cette fin par l'autorité administrative à l'issue de la perquisition. Cette autorisation ne peut porter que sur des éléments présentant un lien avec la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne justifiant la perquisition. Dans l'attente de la décision du juge, les données sont placées sous la responsabilité du chef du service ayant procédé à la perquisition et nul ne peut y avoir accès."

(4) و من بين أهم الحجج التي ساقتها المحكمة العليا الفيدرالية لتبرير حكمها باشتراط الإذن القضائي المسبق لإجراء التفتيش المعلوماتي في حالة القبض على الأشخاص و ذلك في معرض ردها عن ادعاءات النيابة العامة نذكر أهم النقاط الواردة به: "لا يمكن استخدام البيانات الرقمية المخزنة على الهاتف الخليوي في حد ذاته كسلاح لإيذاء الضابط القائم بالقبض أو لتفعيل هروب الشّخص المقبوض عليه، يمكن للضّبطية القضائية فحص الجوانب المادّية للهاتف للتأكد من أنّها لن تستخدم كسلاح و القضاء على أي تهديدات جسدية محتملة..." "تثير الحكومة مخاوف بشأن تدمير الأدلة المعلوماتية، بحجة أنّه حتّى إذا كان الهاتف الخليوي آمناً من الناحية المادّية، فإنّ المعلومات المخزنة الهاتف المحمول لا تزال عرضة للمحو عن بعد أو عن طريق تشفير البيانات... يحدث المسح عن بعد عندما يتلقى الهاتف، متصلاً بشبكة لاسلكية، إشارة بمحو البيانات المخزنة، و يمكن أن يحدث المحو أيضاً عندما يرسل طرف ثالث إشارة عن بعد أو عندما يكون الهاتف مبرمج مسبقاً لحذف البيانات عند دخول أو مغادرة مناطق جغرافية

و في هذا القرار الصادر بالإجماع، أوضحت المحكمة أنّ الضبطية القضائية لا يمكنها بدون إذن قضائي مسبق إجراء التفتيش المعلوماتي على الهاتف الموجود بحوزة الشخص عقب القبض عليه، لأنّ الهاتف لا يمكن أن يشكل سلاحاً يهدّد سلامة الضبطية القضائية، كما أنّ احتمال إتلاف الأدلة عن طريق المسح عن بُعد أو تشفير البيانات لم يظهر أنّه شائع و يمكن التصدي له بتعطيل الهواتف، علاوة على ذلك، فإنّ القدرة التخزينية الهائلة التي تتمتع بها الهواتف المحمولة الحديثة تشتمل على مخاوف تتعلق بالخصوصية بحكم خصوصية المعلومات التي يمكن الوصول إليها عبر الهواتف، و قد لقي هذا الحكم التاريخي تأييداً فقهيًا كبيراً.

معينة، و فيما يتعلّق بالمسح عن بعد، فإنّ الشاغل الرئيسي للحكومة ينصرف إلى تصرفات أطراف ثالثة غير موجودة في مكان القبض، و تشفير البيانات هو أبعد من ذلك... و على أي حال، ففيما يتعلّق "بالحذف عن بعد"، فإنّ هناك وسائل محدّدة للتصدي لهذا التهديد، بحيث يمكن تجنب "الحذف عن بعد" عن طريق قطع إتصال الهاتف بالشبكة بطريقتان بسيطتان أولاً، يمكن للضبطية إيقاف تشغيل الهاتف أو إزالة البطارية. ثانياً، إذا كانوا يشعرون بالقلق إزاء التشفير أو غيرها من المشاكل المحتملة، فإنّه يمكن أن ترك الهاتف يعمل وضعه في العلبة التي تعزل الهاتف من موجات الراديو. و تسمى هذه الأجهزة عادة "أكياس فارادي"... تختلف الهواتف الخلوية من حيث الكم و النوع عن الأشياء الأخرى التي يمكن الاحتفاظ بها على الشخص المعتقل. مصطلح "الهاتف المحمول" هو في حد ذاته اختزال مظلّل. فكثير من هذه الأجهزة هي في الواقع عبارة عن حواسيب الصغيرة، لها القدرة على استخدامها كهاتف. و يمكن بسهولة تسميتها بالكاميرات، و مشغلات الفيديو، و النّقويمات، و مسجّلات الشريط، و المكتبات، و مذكرات، و الألبومات، و أجهزة التلفزيون، و الخرائط، أو الصّحف... إنّ سعة التخزين للهواتف المحمولة لها عدة عواقب مترابطة على الخصوصية. أولاً، يجمع الهاتف الخلوي في مكان واحد العديد من الأنواع المتميّزة من المعلومات - عنوان، مذكرة، وصفة طبية، كشف حساب مصرفي، فيديو - يكشف أكثر من ذلك بكثير في تركيبة من أيّ سجل آخر. ثانياً، يمكن إعادة بناء مجموع الحياة الخاصة للفرد من خلال الصّورة تحمّل تواريخ و مواقع و أوصاف معينة؛ و هو ما أمكن أن ينطبق على صور مخبأة في محفظة. ثالثاً، يمكن للبيانات الموجودة على الهاتف أن تعود لتاريخ سابق عن شراء الهاتف... "تعترف الحكومة بأنّ التفتيش عقب القبض قد لا يمتد ليشمل الملفات التي يتم الوصول إليها عن بعد - أي البحث في الملفات المخزّنة في السّحابة، في حين مثل هذا التفتيش سيكون بمثابة العثور على مفتاح في جيب المقبوض عليه يسمح للضبطية بفتح منزله و تفتيشه لأنّ الضبطية القضائية التي تجري تفتيش الهاتف لن تكون على علم فيما إذا كانت المعلومات التي تتطلّع عليها مخزّنة محلياً وقت الضبط أو تم تنزيلها من السّحابة".

انظر الحكم (2014) 134 S. Ct. 2473, 2493-94 Riley v. California، مذكور و معلق عليه لدى:

Lamparello, Adam, Riley v. California: A Pyrrhic Victory for Privacy Rights?, Journal of Law, Technology and Policy, Vol 3, (2015), pp 1-16.

و في تعليقه على هذا الحكم يرى الفقه الأمريكي أن هذا المبدأ الذي أرسته المحكمة العليا يعتبر بمثابة "إعادة للتوازن" الذي إختل بتطبيق القواعد التقليدية على البيئة المعلوماتية و أدى إلى نتائج غير معقولة، ذلك أن حقائق عمليات التفتيش المعلوماتي تختلف اختلافاً كبيراً عن حقائق عمليات التفتيش المادي التي تتطلب قواعد جديدة، إذ تستدعي الحقائق التي فرضتها البيئة المعلوماتية قواعد جديداً لاستعادة وظيفة القانون القديم⁽¹⁾، سعياً لإيجاد معيار تحقيق التوازن بين عنصر الفعالية و الشرعية في التفتيش عن الأدلة المعلوماتية.

واقع الأمر أنه رغم التعديلات العربية الحديثة فيما يتعلّق بإجراءات التفتيش المعلوماتي إلا أنها لا تزال في غيبة من التعرض لهذه المسألة، و بطبيعة الحال فإن الإبقاء على تطبيق القواعد التقليدية فيه إهدار كبير للحريات الفردية، لذا نرى أن النظام المعلوماتي يتمتع بحرمة خاصة، فلا يجوز فحص أجهزة التخزين الرقمية أو الإطلاع عليها إلا بمقتضى إذن قضائي مسبب يحدّد يستهدف الأنظمة المعلوماتية على وجه التخصيص، إذ أن هذا الإجراء من طبيعة خطيرة فضلا عن مساسه بالحياة الخاصة للمتهم، فهو ينتهك أيضا حق الغير الذي لا تربطه أي رابطة بالجريمة، فوجب توافر ضمانات إضافية بالحصول علي إذن من جهة محايدة. زيادة على ذلك فإن التشريع الإجرائي لما خول للضبطية القضائية في أحوال التلبس سلطة التفتيش فهي سلطة استثنائية لا يجوز التوسع فيها أو القياس عليها لأن ما ثبت على خلاف الأصل من مساس بالحريات لا يقاس عليه و يجب أن يفسر في أضيق نطاق، فالمشروعية الإجرائية تحظر إتخاذ أي إجراء جنائي يمس الحريات الفردية إلا بناء على نص صريح يجيزه، مما مقتضاه أنه لا يجوز للضبطية القضائية في أحوال التلبس إجراء التفتيش المعلوماتي للدعمات المادية التي توجد بحوزة المقبوض عليه، و كلّ ما يجوز لها هو إتخاذ إجراءات الضبط منعا من تدمير الأدلة و محافظة على سلامتها من العبث و التعديل، ريثما يتم الحصول على إذن قضائي يجيز التفتيش، و لذلك حرص الدستور على التأكيد على عدم إنتهاك حرمة الحياة الخاصة للفرد بتفتيش نظامه المعلوماتي ما لم يصدر أمر قضائي مسبب دون أن يستثنى من ذلك حال التلبس بالجريمة.

(1) 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), p 10.

و بهذا الصدد ينبغي أن نشير إلى اعتقاد يتمسك به بعض الفقه من كون أن الدساتير و التشريعات عموما تجيز تفتيش الشخص دون إذن قضائي في حالة التلبس مما يجوز معه من باب أولى تفتيش نظامه المعلوماتي في حالة التلبس بما قد يفيد في كشف الحقيقة باعتبار أن الحرية الشخصية أسمى من حرمة المسكن و أي حرمة أخرى، و بطبيعة الحال فإن هذا المعتقد السائد يعكس فهما خاطئا لحرمة النظام المعلوماتي و ما ينطوي عليه من أسرار و عورات لا يمكن مقارنتها نهائيا بحرمة المسكن أو حرمة الشخص ذاته، لذا وجب على القضاء في الفترة الحالية تطبيق النص الدستوري و إهمال القواعد العادية لتعارضها مع الدستور إلى حين تعديلها.

ثانيا: المقومات الشكلية للإذن القضائي

الإذن و قد استقر تعريفه على أنه وثيقة مكتوبة فإن الشكل يمثل أهمية كبرى حيث يعدّ وعاء يحتوى على كافة الشروط الموضوعية و الشكلية الأخرى، سواء تعلق الأمر ببيانات شكلية عامة (أ)، أو عنصر التسيب كبيان خاص (ب).

(أ) - بيانات إذن التفتيش المعلوماتي

إنّ التفتيش بطبيعته إجراء ينطوي على مساس بحق الفرد في حياته الخاصة لذا وجب أن يكون إذن التفتيش محددا بشكل دقيق⁽¹⁾، فالبيانات الواجب إدراجها في الإذن بالتفتيش تجد مبررات ضرورتها في تحديد الصلاحيات المخولة للسلطة المنتدبة عند تنفيذ التفتيش فلا يسوغ لها تجاوزها، فضابط التحديد يسمح للمتهم بممارسة رقابة بنفسه حال إجراء التفتيش و رقابة لاحقة حول طريقة تنفيذه و المحل الذي شمله⁽²⁾.

لذا يجب أن يكون الإذن بالتفتيش مكتوبا و مؤرخا و موقعا عليه ممن أصدره و يجب أن يكون صريحا في الدلالة على التفويض في مباشرة التفتيش، و ينبغي أن يتضمن من البيانات ما يحدّد نوع الجريمة التي يهدف إلى التوصل إلى دليل بشأنها، و أخيرا فإنه يجب

(¹) Cour eur. D.H., Société colas Est et autres / France, 16 avril 2002, n° 37971/97 .

(²) Cour eur. D.H., Van Rossem colas / Belgique, 09 décembre 2004, n° 41872/98.

تحديد محل التفتيش، و أن يبين في الإذن الفترة الزمنية التي يقدر بقاءه ساري المفعول خلالها لمباشرة الإجراء⁽¹⁾.

و التزاماً بأقصى مدى من الشرعية يجب أن يحدّد الإذن محل التفتيش في مرحلتيه (المادي و المعلوماتي) و مستهدفه أيضاً منعا من تجاوز الغاية منه⁽²⁾، ففي قضية **United States v. Hunter** حيث تمّ تفتيش منزل المشتبه به بناء على إذن أجاز ضبط "أجهزة الحاسوب... أجهزة التخزين الإلكترونية... و جميع نظم البرمجيات الحاسوبية،" دون تقديم أيّ معلومات مفصلة حول أيّ جريمة محدّدة، رأت المحكمة أنّ الإذن كان يفتقر إلى الحد الكافي من التّحديد، و كان أقرب إلى الأذن العامة التي سعى التّعديل الرّابع لمنعها، و قد انتقدت المحكمة اللّغة التي صيغ بها الإذن معتبرة إياها مجرد "فقرة عامة"، و رأت أنّ الإذن يجب أن يحدّد البند أو الملف الذي يحتويه الحاسوب و المراد ضبطه، و يحدّد القيود المفروضة على أيّ تفتيش لاحق⁽³⁾.

ب) - تسبب الإذن القضائي بالتفتيش المعلوماتي

يعتبر التّسبب ضماناً بتوافر العناصر الواقعية التي توافر بها سبب التفتيش بالمعنى الذي حدّدناه فيما تقدم، فهو على هذا النّحو يضمن جدية اتخاذ الإجراء و يحول دون الإعتداء على حرمة الحياة الخاصة للأفراد دون موجب أو اقتضاء⁽⁴⁾، و قد استقرّ القضاء المصري على أنّ هذا الشرط وجوبي في الأمر بتفتيش المسكن دون تفتيش الأشخاص⁽⁵⁾، و يجري التّساؤل في ضوء ذلك فيما إذا كان إذن التفتيش المعلوماتي يخضع لهذا الضّمان؟

(1) سامي حسني الحسيني، المرجع السابق، ص ص 109-134.

(2) إنّ مسألة شكل الإذن و بياناته لا تخرج في عمومها عن أحكام القواعد التّقليدية، و هي لا تثير في معرض دراستنا إشكالا يستحقّ الوقوف عنده، و بحكم أنّ الدّراسات الفقهيّة قد أسهبت في معالجتها فلا موجب للاستفاضة في تناولها، و لمزيد من التّفصيل حول هذا الموضوع يراجع: سامي حسن الحسيني، المرجع السابق، ص ص 100-147، توفيق توفيق محمد الشّاوي، المرجع السابق، ص ص 325-348.

(3) *United States v. Hunter*, 13 F. Supp. 2d 574, 584 (D. Vt. 1998).

(4) أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، المرجع السابق، ص 780.

(5) أنظر الطّعن رقم 1515 لسنة 45 جلسة 12/01/1976 س 27 ص 61 ق 11، جاء في هذا القرار "لما كانت المادة 44 من الدّستور و المادة 91 من قانون الإجراءات الجنائية بعد تعديلها بالقانون رقم 37 لسنة 1972 يوجبان تسبب الأمر القضائي بالتفتيش إلّا إذا كان منصباً على تفتيش المساكن و كان الثّابت من مطالعة الحكم المطعون

إنّ المشرّع الدستوري - توفيقاً بين حق الفرد في الحرّية الشخصيّة و في حرمة مسكنه و حياته الخاصة و بين حق المجتمع في عقاب الجاني - قد أجاز إتخاذ إجراءات جمع أدلّة إثبات الجريمة و نسبتها إليه بعد أن أخضعها لضمان إجرائي معيّن لا يجوز إهداره، يتمثّل في وجوب الحصول مسبقاً على إذن قضائي معلّل، إذ لا قيمة للإذن القضائي ما لم يكون مسبباً. فنص الدستور على هذا الضابط الإجرائي كقاعدة عامة تحكم كل إجراء ينطوي على مساس بحرمة الحياة الخاصة للفرد، و لأنّ "الحرّية الشخصيّة حق طبيعي و هي مصونة لا تمس"⁽¹⁾ ردّد المشرّع هذا الضمان ضمن نص المادّة الأولى من قانون الإجراءات الجزائية⁽²⁾.

ترجع العلة من فرض تسيّب الإذن القضائي إلى حماية الحرّيات الفرديّة، فيتحقّق الضمان القضائي ببسط المحكمة رقابتها على صحة الإذن و قيام مسوّغات التفتيش، لذا نرى أنّ أهمّ مقومات إذن التفتيش هو التسيّب، بأن يكون مبنياً على عدد من القرائن و الدلائل التي ترجّح أنّ النّظام المعلوماتي المراد تفتيشه يحتوي على ما يفيد في كشف الحقيقة،⁽³⁾.

الفرع الثّاني: الإختصاص بتنفيذ إذن التفتيش

متى استوفي الإذن بالتفتيش شروطه الشكلية و الموضوعية، كان لفاضي التحقيق المتخص أن يصدره، سواء تحدّد الإختصاص بمكان وقوع الجريمة أو بمكان إقامة المتهم أو القبض عليه، إلّا أنّه أثناء التنفيذ تتصادف هذه السّلطة أو من تتدبه بعقبات مبنها أنّ البيانات التي يستهدفها التفتيش مخزّنة في نظام معلوماتي آخر يمكن الوصول إليه من النّظام

فيه أنّ التفتيش قد اقتصر على شخص المطعون ضده كما ثبت من المفردات المنظّمة أنّ الإذن الصّادر بالتفتيش كان قاصراً على تفتيش شخص المتهم المذكور دون مسكنه فإنّ الحكم المطعون فيه إذ انتهى إلى بطلان ذلك الإذن بدعوى عدم تسيبته و رتبّ على ذلك القضاء ببراءة المطعون ضده يكون قد أخطأ في تطبيق القانون بما يوجب نقضه" مشار إليه لدى: محمد علي سويلم ، المرجع السّابق، ص 515.

(1) المادة 41 من الدّستور المصري.

(2) المادة 1 من قانون الإجراءات الجزائية المعدّلة بموجب المادة القانون رقم 17-07 المؤرخ في 27 مارس 2017 المعدّل و المتمم لقانون الإجراءات الجزائية.

(3) و قد قطع المشرّع المصري في هذه المسألة صراحة بموجب المادة 06 من القانون رقم 175 لسنة 2018 حيث نصّت لجهة التّحقيق المختصّة .. أن تصدر أمراً مسبباً... للبحث و التفتيش و الدّخول و التّفاذ إلى برامج الحاسب و قواعد البيانات و غيرها من الأجهزة و النّظم المعلوماتيّة"، و هو موقف المرشح البحريني الذي تجسده المادة 15 من القانون رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات.

المعلوماتية المقرّر تفتيشه، و هذا النّظام المعلوماتي قد يتواجد داخل الإقليم الوطني (أولاً)، أو خارجه (ثانياً).

أولاً: امتداد الإختصاص بالتفتيش داخل إقليم الدّولة

يعتبر امتداد التفتيش داخل إقليم الدّولة من الإجراءات الاستثنائية الخطيرة، فبينما تتطلّب فعالية التفتيش سرعة امتداده إلى ما يتجاوز النّظام المأذون تفتيشه (أ)، تفرض الشّرعية الإجرائية إحاطته بضمانات تحول دون صيرورته عامًا طليقاً من أيّ قيد (ب) (1).

(أ) - ارتباط فعالية التفتيش المعلوماتي بسرعة امتداد نطاقه

أدى تطوّر التّقنيات الرّقمية من حيث مبدأ الإقليمية، إلى التّمييز بين الوسيط المادي لتخزين المعلومات و الوسيط الّذي يمكن الحصول من خلاله على نفس المعلومات، إذ بات شائعاً تخزين البيانات على خوادم موجودة في غرفة مخصّصة، أو في مبنى آخر أو لدى جهة خارجية، على نحو يسمح للمستخدم بناء على شاشة و لوحة مفاتيح استخدام هذه البيانات و تعديلها، دون أن يكون لديه حق الوصول المادي إلى وسيط التّخزين الفعلي (2). و من هنا يثير مفهوم "المكان" محل التفتيش تحدّيًا قانونيًا عندما تكون البيانات موزّعة عبر شبكة حاسوبية، أي أنّ التفتيش قد يكون عن حاسوب في مكتب ما في أحد الأماكن، و لكن البيانات قد تكون مخزّنة في حاسوب في مكان مادي آخر على الرّغم من وجوده إفتراضياً أمام المستخدم و القائم بالتحقيق (3).

(1) ينبغي الإشارة الى أن إختصاص قاضي التحقيق بالتفتيش في جرائم المخدرات و الجريمة المنظمة و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و جرائم تبييض الأموال و الإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف هو إختصاص يمتد عبر امتداد التراب الوطني بموجب المادة 47 من قانون الاجراءات الجزائية و تلك مسألة ليست محلاً لدراستنا لأنّها لا تثير إشكاليات تستوجب التعرض إليها، في حين فإن امتداد الإختصاص في غير هذه الجرائم هو الّذي يطرح مسائل آية في التعقيد هي موضوع اهتمامنا.

(2) Alexandre Rousselet-Magri Les perquisitions « informatiques » à l'épreuve du principe de souveraineté, dans un contexte de mondialisation du stockage de données Étude comparée en droit français et états-unien Revue de science criminelle et de droit pénal comparé, Dalloz, 2017/4 (N° 4),p 659.

(3) الأمم المتحدة، تدابير لمكافحة الجريمة المتصلة بالحواسيب، مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة و العدالة الجنائية المنعقد بيناكوك، في الفترة 18-25 أبريل 2005، و وثيقة رقم A/conf.203/14، ص 20.

بالنسبة للإثبات الجنائي المعلوماتي، فإنّ متطلبات الفعالية تستلزم الوصول إلى المعلومات أكثر من الوصول إلى الخادم ذاته، تماما كما هو الحال بالنسبة للمستخدم الذي يتمكّن من الإطلاع على صندوق البريد الإلكتروني، عن طريق حاسوبه، أي معرفة المحتوى الذي يمكن تخزينه على بُعد آلاف الكيلومترات، على خوادم يحتمل أن تكون موجودة خارج إقليم الدولة التي يتواجد بها هذا الأخير، بل قد يكون تخزين هذا المحتوى في نفس الوقت على العديد من الخوادم التي تتوزّع عبر العديد من البلدان دون علم المستخدم⁽¹⁾.

الأصل أنّ تطبيق القواعد التقليدية المتعلقة بالتفتيش لا تسمح بامتداد التفتيش المعلوماتي ليطال معطيات معلوماتية مخزّنة في مكان آخر غير (المحل) المحدّد في الإذن القضائي تحت طائلة بطلان التفتيش و ما يسفر عنه، بما يمكن أن يضيّع فرصة إثبات الجريمة، الأمر الذي حدا بالمشرّع في بعض الدول إلى تشريع ما يمكن أن يطلق عليه "التفتيش عن بعد" إلى الأنظمة المعلوماتية المتواجدة داخل الإقليم.

و قد كانت اللجنة الأوروبية للمشكلات الجنائية التابعة للمجلس الأوروبي سبّاقة إلى تبني فكرة ذاتية إجراءات التفتيش و أوصت بجواز أن يمتدّ تفتيش النظام الحاسوبي إلى الشبكة المتّصل بها، طالما كانت تلك الشبكة تقع داخل إقليم الدولة، فتنصّ التوصية رقم 13 لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتّصلة بتقنية المعلومات على أنّه "السلطة التحقيق عند تنفيذ تفتيش المعلومات -وفقا لضوابط معينة- أن تقوم بمدّ مجال تفتيش كمبيوتر معين يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة ما دامت مرتبطة بشبكة واحدة و أن تضبط البيانات المتواجدة فيها، ما دام أنّه من الضروري التّدخل الفوري للقيام بذلك"⁽²⁾.

(1) Alexandre Rousselet-Magri, op cit ,p 659.

(2) Conseil de l'Europe, Recommandation N° R (95) 13 DU Comite des ministers aux etats member relatives aux problem de procedure penale lies a la technologie de l information (adoptée par le Comité des Ministres le 11 septembre 1995,lors de la 543e reunion des Délégués des Ministres).p 2. Les lois de procédure pénale devraient permettre aux autorités chargées de l'enquête de perquisitionner dans les systèmes informatiques et d'y saisir des données, dans des conditions similaires à celles utilisées dans le cadre des pouvoirs traditionnels de perquisition et de saisie. La personne en charge du système devrait être informée que le système a fait l'objet d'une perquisition et de la nature des données saisies. Les recours juridiques prévus par la législation en général contre la perquisition et la saisie devraient être également applicables en cas de perquisition d'un système informatique et de saisie des données qui y sont continues.

و سعياً لتجاوز هذه المعضلة حرصت مختلف الإتفاقيات الدولية على أن تتخذ كل دولة طرف ما قد يلزم من تدابير تشريعية و تدابير أخرى تكفل قدرة سلطاتها المختصة على أن تجري على وجه السرعة عملية تفتيش للوصول إلى جهاز تكنولوجيا المعلومات و الاتصالات الأخرى إذا كان لدى هذه السلطات، أسباب تدعو إلى الاعتقاد بأن البيانات المطلوبة مخزنة في جهاز آخر من أجهزة تكنولوجيا المعلومات و الإتصالات الموجودة في إقليم تلك الدولة الطرف⁽¹⁾، و من الطبيعي أن تحرص الدول التي صادقت على هذه الإتفاقيات على تعديل تشريعاتها بما يتسق مع هذا النص الإجرائي.

من الأمثلة النموذجية للقوانين التي نصت على جواز امتداد لتفتيش المعلوماتي إلى جميع الأنظمة المعلوماتية المرتبطة بالنظم الأصلي و المتواجدة داخل الإقليم، التشريع البلجيكي⁽²⁾ و التشريع الفرنسي، حيث نصت المادة (17) من القانون رقم 239 لسنة 2003 المسمى قانون الأمن الداخلي الفرنسي على أنه: "الضباط الضبط القضائي أو لمن يعملون تحت مسؤوليتهم من مأموري الضبط القضائي، القيام أثناء تفتيش يجرونه وفقاً لأحكام هذا القانون بالدخول من خلال نظام حاسوبي موجود في الأماكن التي يجري فيها التفتيش، إلى معطيات تهم التحقيق مخزنة في هذا النظام أو في نظام حاسوبي آخر، مادام أن هذه المعطيات متاح الدخول إليها من النظام الرئيسي أو من نظام مرتبط بالنظام الرئيسي"، و هو موقف الفقه الألماني في تفسيره للقسم 104 من قانون الإجراءات الجزائية الألماني⁽³⁾.

الحقيقة أن هذا النهج إتبعته أغلب التشريعات العربية سواء بشكل ضمني كالتشريع المصري⁽⁴⁾ أو بشكل صريح كالتشريع البحريني⁽¹⁾ و اللبناني⁽²⁾ و السوري⁽³⁾ و كان التشريع

(1) أنظر المادة 19 من الإتفاقية الأوروبية لمكافحة الجرائم المعلوماتية و المادة 31-3-3 - أ من اتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني و حماية البيانات ذات الطابع الشخصي، كذلك المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المادة 26 من مشروع اتفاقية الأمم المتحدة للتعاون في مكافحة الجريمة الإلكترونية.

(2) أنظر المادة 88 مكرر من قانون تحقيق الجنايات البلجيكي.

(3) Manfred Mohrenschlager, Computer Crime and Other Crime Against Information Technology in Germany, Revue international de droit pénale, Editions ERES, Paris, 1993, p 351.

(4) تنص المادة 6 من القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات "الجهة التحقيق المختصة - بحسب الأحوال- أن تصدر أمراً مسبباً، لمأموري الضبط القضائي المختصين... ضبط أو سحب أو جمع أو التّحفظ على البيانات و المعلومات أو أنظمة المعلومات، و تتبعها في أيّ مكان أو نظام أو برنامج أو

الجزائري من بين هذه التشريعات التي تبنت مشروعية امتداد التفتيش المعلوماتي و ذلك بموجب الفقرة الثانية من المادة 5 من القانون 04/09 باعتبار أن متطلبات فعالية التفتيش في غالب الأحيان تستوجب السماح بامتداد التفتيش و لو تجاوز الإختصاص الإقليمي لسلطة التحقيق أو من تندبه.

و هي ضرورة إستشعرها المشرع الجزائري تلافياً لأي صعوبة قد تعترض تطبيق القواعد التقليدية في هذا الوسط، لأنّ فعالية هذا الإجراء مرتبطة بالسرعة، إذ يعدّ هذا الإجراء بمثابة إعادة للتوازن بين قدرة الجاني على العبث بالأدلة المعلوماتية في زمن متناه القصر و بين قدرة السلطة الإجرائية على تمديد تفتيشها إلى النظام المعلوماتي الذي يعتقد أنه يحتوي على عناصر الإثبات، غير أنّ هذا الإجراء يثير العديد من التحديات في ما يتعلّق بمبدأ الشرعية الإجرائية لذا وجب قيده بمجموعة من الضمانات التي تحقّق التوازن بين هذه المتطلبات المتعارضة.

دعامة إلكترونية أو حاسب تكون موجودة فيه، و يتم تسليم أدلتها الرقمية للجهة مصدرة الأمر على ألا يؤثر ذلك على استمرارية النظم و تقديم الخدمة إن كان لها مقتضى. 2- البحث و التفتيش و الدخول و النفاذ إلى برامج الحاسب و قواعد البيانات و غيرها من الأجهزة و النظم المعلوماتية تحقيقاً لغرض الضبط...

(1) تنص المادة 15 من القانون البحريني رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات: "

1) للنيابة العامة أن تصدر أمراً مسبباً بالدخول إلى ما يلي و تفتيشه:

أ) نظام تقنية المعلومات المتصل بالجريمة أو أي جزء منه و أية بيانات لوسيلة تقنية المعلومات مخزنة فيه.

ب) أي من وسائط تخزين بيانات وسيلة تقنية المعلومات التي من المحتمل أن يكون مخزناً عليها بيانات متصلة بالجريمة.

2) إذا قامت لدى النيابة العامة أثناء تنفيذ الأمر المشار إليه في البند (أ) من الفقرة (1) من هذه المادة أمارات قوية بأنّ البيانات المتصلة بالجريمة مخزنة في نظام تقنية المعلومات آخر أو في جزء منه، و كانت هذه البيانات قابلة لأن يتمّ الدخول إليها من خلال نظام تقنية المعلومات الأول أو متاحة من خلاله على نحو مشروع، فإنّ للنيابة العامة أن تصدر أمراً مسبباً بمدّ الدخول و التفتيش إلى النظام الآخر."

(2) المادة 124 القانون اللبناني رقم 81 لسنة 2018 و المتعلّق بالمعاملات الإلكترونية و البيانات ذات الطابع الشخصي."

(3) المادة 26 من قرار وزارة الاتصال السورية رقم 2012/290 المتضمّن التعليمات التوضيحية و التنفيذية لقانون تنظيم التواصل على الشبكة و مكافحة الجريمة المعلوماتية الصادر بتاريخ 07 ماي 2012.

(ب) - ضمانات امتداد التفتيش المعلوماتي داخل الإقليم

بالإضافة إلى الضمانات العامة سواء التقليدية أو الحديثة التي يخضع لها التفتيش المعلوماتي فإن امتداده يخضع إلى ضمانات إضافية، فلا يجوز السماح به إلا إذا كان النظام المعلوماتي المطلوب تفتيشه مرتبطاً بالنظام الأولي المأذون بتفتيشه، مع ضرورة توافر الإشراف القضائي في حالة التمديد بموجب إذن إضافي.

(1) - إرتباط محل التفتيش الأولي بنظام معلوماتي آخر

هناك إجماع بين الاتفاقيات الدولية و التشريعات الداخلية على ضرورة قيام هذا الضابط الموضوعي لجواز إمتداد التفتيش إلى غيره من النظم المترتبة به، متى قامت الأسباب المبررة لهذا الإجراء، و قد أكدت ذلك المادة 5 فقرة 3 من القانون 04/09 حيث جاء فيها " إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و أنّ هذه المعطيات يمكن الدخول إليها إنطلاقاً من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية بذلك"⁽¹⁾.

و مفاد هذا النص أنّ عملية امتداد التفتيش المعلوماتي تظهر ضرورتها أثناء تنفيذ عملية تنفيذ التفتيش الأولي، مما مقتضاه أنّه إذا تبين لسلطة التحقيق أثناء إجراء التفتيش المعلوماتي أنّ البيانات المفيدة في إظهار الحقيقة مخزنة ضمن نظام معلوماتي آخر غير أنّه ليس من الممكن تقنيا الولوج إليه إنطلاقاً من النظام المعلوماتي المأذون بتفتيشه، فإنّه لا يجوز لها القيام بإجراء التفتيش وفق هذا المنظور لأنّه لا يعتبر امتداد للتفتيش الأولي بل عملية تفتيش مستقلة تماماً.

و قد جاء ذلك واضحاً ضمن نص المادة 57 من قانون الإجراءات الجزائية الفرنسي التي تنص " لضباط الضبط القضائي... الدخول من خلال نظام حاسوبي موجود في الأماكن التي يجري فيها التفتيش، إلى معطيات تهم التحقيق مخزنة في هذا النظام أو في نظام

(¹) و هو ما تنص عليه المادة 26 فقرة 02 مشروع اتفاقية الأمم المتحدة للتعاون في مكافحة الجريمة الإلكترونية التي جاء فيها "تتخذ كل دولة طرف ما قد يلزم من تدابير تشريعية و تدابير أخرى تكفل قدرة سلطاتها المختصة على أن تجري على وجه السرعة عملية بحث للوصول إلى جهاز تكنولوجيا المعلومات و الاتصالات الآخر إذا كان لدى هذه السلطات، التي تجري بحثاً وفق أحكام الفقرة 1 (أ) من هذه المادة، أسباب تدعو إلى الاعتقاد بأنّ البيانات المطلوبة مخزنة في جهاز آخر من أجهزة تكنولوجيا المعلومات و الاتصالات الموجودة في إقليم تلك الدولة الطرف".

حاسوبي آخر ... " معنى ذلك حظر توسيع التفتيش إلا كان ذلك ممكنا من خلال النظام المعلوماتي الموجود بالجهاز الذي يجري تفتيشه في العالم المادي " *sur les lieux où se déroule la perquisition à des données*.

و هذا الإستثناء الذي أورده المشرع يثير تساؤلا آخر يتعلّق بالفرضية التي يتمّ فيها إجراء التفتيش المعلوماتي عن بعد إنطلاقا من مقر السلطة الإجرائية الأصلية أو المنتدبة عبر الشبكات دون ضرورة المرور بالمرحلة المادية، هل يجوز في هذه الحالة تمديد الإختصاص بالتفتيش؟

إنّ جواز إمتداد التفتيش المعلوماتي في التشريع الجزائري هو قاعدة و ليس استثناء، بحكم التطور الحديث و انتشار خدمات الإتصال أين أصبح تشابك النظم و ارتباطها أمر واقع و يندر وجود نظام تخزين معلوماتي غير مرتبط بغيره من النظم، و مع ذلك فإنّ حكم المادة 5 عام و مطلق و أجاز امتداد المعلوماتي و لو تمّ عن بعد و بشكل سري، على أنّ هذا الإتجاه و إن كان يحقق نتائج فورية إلا أنّه لا يمكن تصور إنتهاك أكثر توسعا و تطفلا على الحياة الخاصة أكثر مما يضيفي إليه هذا الإجراء.

و الملاحظ أنّ أغلب التشريعات العربية لم تنص نهائيا على التفتيش عن بعد بل نصّت فقط على إمتداد التفتيش الذي يجري إنطلاقا من النظام المعلوماتي الأولي (الجهاز المادي الخاص بالمتهم) أمّا التشريع الفرنسي و بعد تردّد طويل اكتفى بالنص على جواز التّفاذ عن بعد إلى نظام المعلومات ليس فقط من نظام معلومات موجود في أماكن البحث المادي، و لكن أيضا من خلال نظم المعلومات الموجودة في مقر وحدة الشرطة أو الدرك و لكنه لم ينص نهائيا على جواز امتداده في هذه الأحوال⁽¹⁾، لأنّه بالفعل إجراء يجرد الحق في الخصوصية من معناه نهائيا، فهو يتمّ في غياب المتهم و بشكل سري دون وجود أيّ نطاق يرسم حدوده ، لذا وجب قصر التفتيش عن بعد على التّحقيق في الجرائم الخطيرة فقط، لأنّ هذا الإجراء قد يخرج عن نطاق التفتيش إلى المراقبة فيتمّ الإطلاع على رسائل إلكترونية لم يقدّم صاحب النظام بفتحها أو أن ينصبّ التفتيش على بيانات مولدة بتاريخ لاحق عن صدور

(¹) Article 1-57- du ccp" Ils peuvent également, dans les conditions de perquisition prévues au présent code, accéder par un système informatique implanté dans les locaux d'un service ou d'une unité de police ou de gendarmerie à des données intéressant l'enquête en cours et stockées dans un autre système informatique, si ces données sont accessibles à partir du système initial.

الإذن بالتفتيش، و لعل السؤال الذي يظل مطروحا هل يجوز امتداد التفتيش إلى نظام معلوماتي آخر بعد عملية الامتداد الأولى؟

الملاحظ في هذا الصدد أنّ التقرير التفسيري لاتفاقية بودابست قد أشار بكل وضوح إلى أنّ المادة 19 فقرة 02 من هذه الاتفاقية⁽¹⁾، لا تقرّر نماذج معيّنة للإذن بالتفتيش و لا لكيفية تطبيق عملية توسيع نطاق التفتيش⁽²⁾، غير أنّها لم تنص على جواز هذا الإجراء شأنها شأن باقي الإتفاقيات، مما يجعل المشرّع الجزائري مطالب بإرساء ضمانات خاصة بهذا الإجراء كتبليغ المتّهم و إعلامه بنطاق التفتيش و تحديد البيانات التي تمّ نسخها و تلك التي تمّ الإطلاع عليها و تمكينه بنسخة من محضر مفصل بكل ذلك لأجل ممارسة طرق الطعن المقرّرة قانونا.

(2) - تجديد الإذن القضائي بامتداد التفتيش المعلوماتي

يثور التساؤل هنا، في حالة ما إذا تمّ الولوج إلى النظام المعلوماتي المحدّد ضمن إذن التفتيش و لم يتم العثور على البيانات ذات القيمة الإثباتية فهل يجوز تمديد التفتيش إلى نظام معلوماتي آخر دون أن يستوجب توسيع التفتيش إذنا قضائيا ثانيا أم يكفي الإذن الأول لمشروعية هذا الإمتداد؟

أجاب المشرّع الجزائري بشكل مباشر على هذا التساؤل، إذ تنص المادة 5 في فقرتها الثّانية من القانون 04/09 "إذا كانت هناك أسباب تدعو للإعتقاد بأنّ المعطيات المبحوث عنها مخزّنة في منظومة معلوماتية أخرى و أنّ هذه المعطيات يمكن الدّخول إليها إنطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السّلطة القضائية بذلك". و معنى ذلك أنّ المشرّع خوّل السّلطات المكلفة بالتحقيق إمكانية توسيع التفتيش أو الولوج بطريقة مشابهة ليشمل نظاما معلوماتيا آخر أو جزء منه، إذا قامت

(¹) L'article 19 de la Convention de Budapest admet ce type de procédure en prévoyant que « lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, (...) et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système ».

(²) Rapport explicatif de la Convention du Conseil de l'Europe sur la cybercriminalité, Clause n°194.

مبررات تدعو للاعتقاد بأن البيانات المطلوبة مخزنة في هذا النظام المعلوماتي، دون اشتراط إذن قضائي بذلك بل يكفي مجرد إعلام السلطة القضائية، أي غياب الإشراف القضائي على إجراء امتداد التفتيش و هو ما يمنح بلا ريب سلطة تقديرية مفرطة لرجال الضبط القضائي لأن هذه السلطة غير محددة بنهائية طرفية معينة⁽¹⁾، على نحو يمكن أن يمتد التفتيش إلى العديد من الأنظمة المعلوماتية في ظل شيوع ارتباطها بفعل الشبكية العنكبوتية لاسيما إذا علمنا أن سلطة التحقيق عادة ما تلجأ في تنفيذ التفتيش إلى التدب.

مؤدى هذا القيد الذي جاء في عبارة "إعلام السلطة القضائية"، لا يفيد وجوب الحصول على إذن منها أو توضيح الأسباب الداعية إلى توسيع نطاق التفتيش، و في اعتقادنا فإن هذا النص قد أهدر كافة الضوابط الإجرائية للتفتيش المعلوماتي التي سبق أن تناولناها، فتوسيع نطاق التفتيش داخل منظومة التخزين (الجهاز) و تجاوزه إلى نظام تخزين آخر يعتبر بمثابة عملية تفتيش جديدة كلياً و ليست امتداد للعملية الأولى، لأن عملية التفتيش الأولى إنتهت بعدم الجدوى بعد تفتيش المحل المأذون تفتيشه.

و نظرا لخطورة هذا الإجراء نجد المشرع البلجيكي حاول إحاطته بالعديد من الضمانات من خلال تعديلات عديدة أدخلها على التشريع الإجرائي منذ سن القانون 28 نوفمبر 2000 المتعلق بالإجرام الإلكتروني إلى غاية اليوم، حيث نجد أن الفقرة 3 من المادة 02 من القانون البلجيكي الصادر بتاريخ 25 ديسمبر 2016 المتعلق بتحسين أساليب التفتيش و بعض تدابير التحقيق المتعلقة بالإنترنت و الاتصالات الإلكترونية و إنشاء قاعدة بيانات للبصمات الصوتية و المعدلة للمادة 39 مكرّر من قانون التحقيق الجنائي تجيز امتداد التفتيش المعلوماتي إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان التفتيش الأصلي بناء على إذن وكيل الجمهورية و ذلك وفقا لما يلي⁽²⁾: "إذا كان ضروريا لكشف الحقيقة بشأن

(1) Monika Zwolinska , Sécurité et libertés fondamentales des communications électroniques en droit français, européen et international , thèse doctorat, Université Nice Sophia Antipolis, France, 2015. p 387.

(2) Loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales JORF du 14 janvier 2017 Art. 2§

3. Dispose que "

الجريمة محل البحث، إذا كانت الإجراءات الأخرى غير مناسبة أو وجدت مخاطر تتعلق بضياح عناصر الإثبات".

لذا نرى أنّ الضرورة التي تبرّر امتداد التفتيش هي الوصول إلى الأدلة قبل فقدها، و هي تعتبر حالة من الحالات الطارئة التي سبق معالجتها و التي تجيز في نظرنا للضبطية القضائية إمكانية إتخاذ التدابير التي تحول دون تدمير الدليل فقط دون إتخاذ خطوات التفتيش، فيجوز لها توسيع الضبط المعلوماتي عن طريق التّنزيل أو النّسخ أو عن طريق المنع من الوصول إلى المعلومات طبقاً لنص المادة 07 من نفس القانون ريثما يبسط القضاء رقابته على مسوغات إمتداد التفتيش من عدمه، و هو ما يتحقّق معه مبدأ الشّريعة في أقصى مدى له، لذا نوصي بتعديل النص وفق هذا المنظور.

و نلمس هذا التّوجه بشكل كبير جداً لدى القضاء البلجيكي، حيث قرّرت المحكمة الدستورية البلجيكية في قرارها رقم 20018/174 الصادر بتاريخ 6 ديسمبر 2018 ، عدم دستورية الفقرة 3 من المادة 39 مكرر من قانون التّحقيقات الجنائية، تأسياً على أنّها أجازت لوكيل الجمهورية تمديد التفتيش إلى نظام حاسوبي أو جزء منه في مكان آخر غير المكان الذي تمّ فيه إجراء التفتيش الأولي، حيث رأت المحكمة الدستورية أنّ هذا التّدبير ينطوي على عمليات تفتيش جديدة، لذا وجب خضوعه لإذن من قاضي التّحقيق، بسبب خطورة التّدخل في الحق في الخصوصية الذي يستتبعه هذا الإنتهاك، لذا لا يجوز التّصريح بهذا التّدبير إلا في ظل نفس الشّروط التي تسمح بها الشّروط المتعلقة بعمليات التفتيش⁽¹⁾، فأخضعت عملية امتداد التفتيش لنفس ضوابط عملية التفتيش الأصلية.

Le procureur du Roi peut étendre la recherche dans un système informatique ou une partie de celui-ci, entamée sur la base du paragraphe 2, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée:

- si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche; et

- si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.

(1) و من بين أهمّ ما جاء في قرار المحكمة الدستورية البلجيكية "يسمح إمتداد التفتيش للمحقّقين بالوصول ليس فقط إلى جميع البيانات المسجّلة أو المخزّنة على الجهاز الذي يمثل نقطة إنطلاق عملية التفتيش المعلوماتي، و لكن أيضاً لجميع البيانات المخزّنة على أنظمة الحاسوب المتصلة به ، و كذلك لجميع الإتصالات التي يحتفظ بها المستخدم مع أطراف أخرى بما في ذلك الرّسائل الجديدة المستلمة أو في عملية الاستقبال التي لم يطلّع عليها المستخدم بعد... و في السّياق الحالي، عندما يتمّ تمديد التفتيش المعلوماتي إلى أنظمة حاسوبية واقعة في أماكن

و تنفيذاً لهذا القرار تم تعديل المادة التي تقرر عدم دستوريتها بمقتضى المادة 11 من قانون 5 ماي 2019 الذي يتضمن أحكاماً مختلفة في المسائل الجنائية و في مسائل العبادة، و تعديل القانون المؤرخ 28 ماي 2002 المتعلق بالقتل الرحيم و قانون العقوبات الإجتماعي⁽¹⁾، و في ضوء هذه الرؤية نجد أن المشرع الجزائري مطالب بالحدو حذو المشرع البلجيكي فيما فرضه من ضمانات لامتداد التفتيش المعلوماتي داخل نطاق إقليم الدولة.

ثانياً) - امتداد الاختصاص بالتفتيش خارج إقليم الدولة

لا مرية أنّ مبررات توسيع التفتيش سواء داخل إقليم الدولة أو خارجه تكمن في سرعة الوصول إلى الدليل المعلوماتي قبل تعرّضه للحذف، إلا أنّ إتخاذ إجراء قسري خارج إقليم الدولة يصطدم بمبدأ الإقليمية و ينطوي على إنتهاك لسيادة الدول التي يجري التفتيش على

أخرى يبدو من الضروري إستصدار العديد من أذون التفتيش و الضبط و من الواضح أنّ مثل هذا النهج يثير المخاوف المتعلقة بخطر فقدان الأدلة إذا لم يكن امتداد التفتيش متزامن مع التفتيش الأولي، كما أنّه في كثير من الحالات، لن يكون من الممكن التوصل مسبقاً لتحديد دقيق للأماكن التي جري فيها التفتيش المعلوماتي أو تحديد الملفات المستهدفة أو حتّى الموقع الجغرافي للأنظمة الحاسوبية، و انطلاقاً مما قرره مجلس الدولة في قراره رقم 1966/54 فإن قاضي التحقيق هو قاض مستقل يتكفل بإجراء تحقيق موضوعي، سواء في مواجهة الضحية أو المتهم في حين فإنّ المدعي العام يعتبر طرفاً في المحاكمة الجزائية و يتضح أنّ هذا النص يسمح بتمديد عملية التفتيش بأمر من المدعي العام، دون تدخل من قاضي التحقيق، ما يجعل هذا الإجراء محاط بضمانات أقل للمتهم الذي يكون نظامه الحاسوبي موضوع تفتيش، و فتح لرسائل البريد، و اعتراض الاتصالات الهاتفية و الإلكترونية و الإستماع إليها".

L'arrêt n° 174/2018 du 6 décembre 2018 Numéro du rôle : 6711, disponible sur adresse <https://www.const-court.be/public/f/2018/2018-174f.pdf> (.Consulté le 04-04-2020.)

(¹) LOI du 5 MAI 2019 portant des dispositions diverses en matière pénale et en matière de cultes, et modifiant la loi du 28 mai 2002 relative à l'euthanasie et le Code pénal social, JORF du 24 mai 2019, Art11. Dispose que " Art. 11. L'article 88 ter du même Code, abrogé par la loi du 25 décembre 2016 et rétabli par l'arrêt n°174/2018 du 6 décembre 2018 de la Cour Constitutionnelle, est remplacé par ce qui suit: "Art. 88 ter. Le juge d'instruction peut étendre la recherche dans un système informatique ou une partie de celui-ci, entamée sur la base de l'article 39bis, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée: - si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche; -et si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus. "

أراضيها، لذا تباينت التشريعات بخصوص مشروعية هذا الامتداد بين مؤيد (أ) و معارض (ب).

(أ) - الإتجاه المؤيد لمشروعية امتداد التفتيش المعلوماتي العابر الحدود

يتيح إجراء امتداد التفتيش الوصول إلى نظام حاسوبي موجود خارج المساكن التي تم تفتيشها لجمع البيانات ذات الصلة بالتحقيق، بيد أن مسألة الأساس القانوني للتفتيش عن البيانات "عن بعد" تنشأ تحديدا بخصوص البيانات التي يمكن الوصول إليها من مكان تواجد الشخص الخاضع للتفتيش أثناء تخزينها في موقع آخر موجود خارج الإقليم الوطني، و قد أثرت هذه الإشكالية ضمن أعمال المؤتمر الدولي الخامس عشر للجمعية الدولية للقانون الجنائي، حيث عرض الفقيه Ulrich Sieber في تقريره المقدم للمؤتمر، قيام مرتكبي الجرائم و تهربا من إمكانية الخضوع للتفتيش إلى تخزين بياناتهم ضمن أنظمة تقنية خارج إقليم الدولة، عن طريق إدراجها في شبكة الاتصالات البعيدة بغرض إعاقة التحريات⁽¹⁾.

و رغم ما يتسم به هذا التدبير القسري من فعالية، إلا أن إتفاقية بودابست ضيقّت من نطاق تطبيقه إلى أبعد الحدود، فالمادة 32 منها لا تسمح بإمكانية الدخول بغرض التفتيش و الضبط في أجهزة حاسب أو شبكات تابعة لدولة أخرى بدون إذنها إلا في حالتين، الحالة الأولى إذا تعلق التفتيش بمعلومات أو بيانات متاحة للعامة، و الحالة الثانية إذا رضي المالك أو حائز هذه البيانات بهذا التفتيش، و هو موقف الإتفاقية العربية لمكافحة جرائم تقنية المعلومات⁽²⁾، و فيما عدا ذلك يخضع التفتيش وجوبا للمساعدة القضائية المعتادة⁽³⁾.

(1) Marie-Cristine Piatti , Les libertés individuelles à l'épreuve des nouvelles technologies de l'information, Presses universitaires de Lyon, 2001, p 167.

(2) تنص المادة 40 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات: "الوصول إلى معلومات تقنية المعلومات عبر الحدود : يجوز لأي دولة طرف، و بدون الحصول على تفويض من دولة طرف أخرى :

1. أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات.

2. أن تصل أو تستقبل - من خلال تقنية المعلومات في إقليمها - معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى و ذلك إذا كانت حاصلة على الموافقة الطوعية و القانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة.

(3) تنص المادة 39 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات: التعاون و المساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة :

و يعتبر التشريع السوري التشريع العربي الوحيد الذي أجاز التفتيش العابر للحدود، و إن لم ينص على جوازه صراحة ضمن المرسوم التشريعي السوري رقم 17 لسنة 2012 المتعلق بتطبيق أحكام قانون التّواصل على الشّبكة و مكافحة الجريمة المعلوماتية، إلا أنّ المادة 26 فقرة ج من القرار رقم 290 المتضمّن التعليمات التّوضيحية و التّنفيذية لقانون تنظيم التّواصل على الشّبكة و مكافحة الجريمة المعلوماتية قد حسمت ذلك بقولها "يجوز تفتيش الأجهزة و البرمجيات الحاسوبية المتصلة بأجهزة المشتبه به أيا كان مكان وجودها ضمن حدود الواقعة المسندة إلى المشتبه به"⁽¹⁾.

و من النّماذج القانونية المقارنة المؤيدة لهذا التّوجه، التشريع الهولندي الذي يأتي في طليعة التشريعات المقارنة التي أبحاث التفتيش على أراضي دولة أجنبية، حيث أجازت المادة 125 من قانون مكافحة جرائم الحاسب الآلي للسلطة المختصة بالتحقيق بأن تجري التفتيش داخل الأماكن الموجودة بها البيانات المطلوب التفتيش عنها أينما كانت سواء داخل الإقليم أو خارجه شريطة أن يكون هذا التّدخل مؤقتاً و مفيداً في إظهار الحقيقة⁽²⁾.

بيد أنّ التشريع الفرنسي يسترعي الإهتمام أكثر لتطابقه مع التشريع الجزائري حرفياً بخصوص هذه النّقطة، حيث نصّت المادة 57 من قانون الإجراءات الفرنسية لضباط الضبط القضائي أو لمن يعملون تحت مسؤوليتهم من مأموري الضبط القضائي، القيام أثناء تفتيش إجرونه وفقاً لأحكام هذا القانون بالدخول من خلال نظام حاسوبي موجود في الأماكن التي يجري فيها التفتيش، إلى معطيات تهّم التحقيق مخزّنة في هذا النظام أو في نظام حاسوبي آخر، ما دام أنّ هذه المعطيات متاح الدخول إليها من النظام الرئيسي أو من نظام مرتبط

1. يجوز لأيّ دولة طرف أن تطلب من دولة أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف لمعلومات المخزّنة و الواقعة ضمن أراضي الدولة الطرف المطلوب منها بما في ذلك المعلومات التي تم حفظها بحسب المادة السابعة و الثلاثين.

2. تلتزم الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرف الطالبة وفقاً للأحكام الواردة في هذه الاتفاقية.

3. تتم الإجابة على الطلب على أساس عاجل المعلومات ذات العلاقة عرضة للفقْدان أو التّعديل.

(1) قرار وزارة الاتصال السورية رقم 2012/290 المتضمّن التعليمات التّوضيحية و التّنفيذية لقانون تنظيم التّواصل على الشّبكة و مكافحة الجريمة المعلوماتية الصادر بالجريدة الرسمية بتاريخ 07 ماي 2012.

(2) أسامة بن غانم العبيدي، المرجع السابق، ص 94.

بالنظام الرئيسي، و إذا ثبت مسبقاً أنّ هذه البيانات يمكن الوصول إليها من النظام الأولي أو متاحة للنظام الأولي مخزنة في نظام حاسوبي آخر يقع خارج الأراضي الوطنية، يتم جمعها من قبل ضابط الشرطة القضائية وفقاً للشروط المنصوص عليها في الإلتزامات الدولية السارية⁽¹⁾.

و قد أثار تطبيق هذا النص إشكاليات هامة، أهمّها إشكالية إثبات العلم المسبق للسلطة القائمة بالتفتيش بأنّ النظام المعلوماتي المتصل بالنظام الأولي يقع خارج الإقليم الوطني، و الجزاء الإجرائي المترتب حال إتخاذ إجراء التفتيش المعلوماتي عبر الحدود رغم تحقّق العلم بتجاوز نطاق الإقليم، لأنّه من الناحية العملية سيكون كافياً لأيّ متهم يتمّ تفتيشه أن يتمسك أمام سلطة التفتيش عند الشروع في تنفيذ الإجراء أنّ تخزين بياناته يتمّ عبر خادم موجود خارج الإقليم الوطني، بحيث يجب على السلطة الإجرائية في هذه الحالة الخضوع للضوابط المنصوص عليها في الإتفاقيات الدولية لمواصلة عملية التفتيش⁽²⁾.

واقع الأمر أنّ الفقرة 3 من المادة 57 تحاول أن تتوافق مع قواعد القانون الدولي العام، من خلال إثبات "مبدأ عدم العلم بالتّخزين الرّقمي في الخارج" بشكل غير مباشر، و بالتّالي عندما يشرع ضابط الشرطة القضائية في التفتيش يكون البديل ممكناً بتجاهل تواجد النظام المعلوماتي خارج إقليم الدولة، و في هذه الحالة يكون التفتيش قانونياً، و الفرض الثاني تأكيد العلم المسبق بموقع النظام المعلوماتي و في هذه الحالة يجب أن تتمثل للإلتزامات فرنسا الدولية، و مع ذلك يمكن النفاذ إلى البيانات ضمن الخوادم الموجودة في الخارج، حتّى بدون

(1) تعتبر الفقرة 3 من المادة 5 من القانون 04/09 ترجمة حرفية للفقرة 3 من المادة 57 من قانون الإجراءات الجزائية الفرنسي و التي وردت بالصيغة التالية: " إذا تبين مسبقاً بأنّ المعطيات المبحوث عنها و التي يمكن الدخول إليها إنطلاقاً من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإنّ الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات الصلة وفقاً لمبدأ المعاملة بالممثل".

يقابلها النص الفرنسي:

L'art. 57-3 C. pr. pén. pénale « s'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur ».

(2) Alexandre Rousselet-Magri , op cit , p 663.

معرفة مسبقة بموقع الخوادم، في انتهاك لقواعد الإختصاص الإقليمي⁽¹⁾، لذا يجب التّحقق من مشروعية هذا الإجراء من خلال طلب للحصول على مساعدة قانونية متبادلة تتفّدها الدّولة التي يتواجد النّظام المعلوماتي على أراضيها فعليا⁽²⁾.

غير أنّ محكمة النّقض الفرنسية في قرارها الصّادر بتاريخ 6 نوفمبر 2013 و في تطبيقها لنص المادّة 57 فقرة 3 من قانون الإجراءات الجزائية، سلك مسلكا مخالفا لنية المشرّع، بحيث قرّرت مشروعية تفتيش معلوماتي أجري انطلاقا من نظام معلوماتي واقع بالنّطاق الجغرافي الفرنسي و امتدّ إلى نظام معلوماتي آخر مستضاف في الولايات المتحدة الأمريكية محمي بكلمة مرور سرية⁽³⁾.

و في تبريرها لموقفها ترى هذه المحكمة أنّ النّفاذ إلى نظام معلوماتي عن بعد لا يشكّل عملية تفتيش جديدة بل هو "بمثابة إجراء من إجراءات التّحقيق البسيطة التي تشكّل جزءا من التّفتيش الأولي على نحو لا يتطلّب إذنا قضائيا مستقلا من قبل قاضي الحرّيات و الحبس، و أن وجود الموقع الذي امتدّ إليه التّفتيش بالولايات المتحدة الأمريكية لا يبرّر لزوم طلب المساعدة القضائية الدّولية"⁽⁴⁾، و مع ذلك ما زال بعض الفقهاء يفسّرون هذا النّص خلاف تفسير محكمة النّقض، و يؤكدون على ضرورة طلب المساعدة الجنائية الدّولية من أجل السّماح بإجراء تفتيش على أراضي أجنبية⁽⁵⁾.

و هذا المسلك القضائي لقي تأييدا لدى بعض الفقه الفرنسي على أساس أنّ المبدأ الذي أرسته المحكمة يفضي إلى تفادي شلل عمليات التّفتيش المعلوماتي التي من الممكن أن تترتب على تقرير لزوم تجديد الأذن القضائية في كل عملية امتداد التّفتيش من قبل قاضي

(1) Alexandre Rousselet-Magri , Loc.Cit.

(2) D. Bénichoi, Cybercriminalité, jouer d'un nouvel espace sans frontière, AJ pénal 2005, p 225.

(3) cass. Crim, 6 nov. 2013, n° 12-87.13, Bulletin criminel 2013, n° 217.

(4) جاء في هذا القرار « : Cass. Crim. 6 nov. 2013, n° 12-87.13,

"les juges ajoutent qu'il s'agissait d'une simple investigation et non d'une perquisition distincte exigeant une nouvelle décision de ce magistrat [le juge des libertés et de la détention] et que la seule domiciliation du site en cause aux États-Unis ne justifiait pas la mise en oeuvre d'une procédure d'entraide pénale " .

(5) Sophie Sontag Koenig, Les perquisition 2.0 : quand l'informatique se saisit de l'immatériel, AJ pénal 2016, p 240.

الحرّيات و الحبس، قياسا على عمليات التفتيش التقليدي إذ لا يتطلّب كل فتح لخزانة معيّنة إذنا جديدا.

و من بين أهمّ الحجج التي يسوقها هذا الجانب من الفقه أنّه بالإمكان إجراء قياس بين موقع الخادم في المسكن و الوثيقة، فالمستند يستمد قيمته و الفائدة منه من المعلومات التي يتضمّنها، و بالتالي لا يمكن أن توفر الوثيقة الورقية سوى المعلومات في مكان وجودها، يمكن قراءتها فقط على دعامتها الماديّة، و هذا هو بالضبط ما يميّزها عن الملف الرقمي، إذ يمكن للمستند الممسوح ضوئيا -على الرّغم من أنّه موجود عن بُعد- أن يتيح هذه المعلومات نفسها، من مكان منفصل عن مكان دعامته الماديّة أي من المنزل الذي تمّ تفتيشه، و تأسيسا على ذلك فإنّ اشتراط إذن قضائي مسبق أو التسليم بعدم جواز الضبط بسبب عدم الإختصاص لن يضيف شيئا للحرّيات الفرديّة في وقت تضيع فيه فرصة إثبات الجريمة و حفظ الأمن⁽¹⁾.

بدون تردّد فإننا لا نؤيد هذا التّوجه إطلاقا، لأنّه يتجاهل الفارق الكبير بين التفتيش المادي و التفتيش المعلوماتي، و القول أنّ هذا الضّمان الإجرائي لا قيمة له في حماية الحرّيات الفرديّة قول خاطئ، لأنّ إجازة إمتداد التفتيش المعلوماتي العابر للحدود يتمّ بدون إشراف قضائي و بدون أيّ حدود واضحة من النّاحية الموضوعية إذ يجوز إمتداده إلى أكثر من نظام معلوماتي أيّا كان مكان تواجدها فيصبح عاما لا يتقيّد فقط بمعلومات المتّهم بل يشمل عددا لا يحصى من الأفراد، و ذلك كلّه مرهون بتقدير سلطة الضبط القضائي.

للأسف فقد تمسّكت محكمة النقض مرة أخرى بهذه السّابقة القضائية، في حكم صدر بتاريخ 26 فيفري 2013 إثر فصلها في مسألة مدى مشروعية امتداد التفتيش المعلوماتي عند تعدّد الأنظمة المعلوماتيّة و توزيعها عبر مناطق مختلفة، مؤكّدة أنّ النّفاذ إلى البيانات المحوسبة المخزّنة عن بُعد لا يستلزم تفتيشا جديدا. لذلك، لا يهم ما إذا كانت البيانات مخزّنة على نظام حاسوبي واحد أو تمّ تقسيمها على العديد من وسائط التخزين، لأنّ هذا النّفاذ يعتبر مجرد إمتداد للتفتيش الذي يتمّ في المباني "الطبيعية" للشخص الاعتباري⁽²⁾.

(1) Alexandre Rousselet-Magri, op cit, p 668.

(2) Com. 26 févr. 2013, n° 12-14.772, Bulletin 2013, IV, n° 32.

يبدو في اعتقادنا أنّ متطلبات الفعالية حذت بمحكمة النقض الفرنسية إلى تفسير نص المادة 57 من قانون الإجراءات الجزائية تفسيراً يخالف مقتضيات إتفاقية بودابست، فامتداد التفتيش يشكّل عملية تفتيش جديدة لأنها تنصّب على محل جديد يجاوز المحل المحدد في الإذن القضائي بدليل و أنّ العديد من التشريعات تشترط إذنا قضائياً مستقلاً لتقرير مشروعيته كما سبق و أنّ أكدته المحكمة الدستورية البلجيكية.

و من جهة أخرى فإنّ تكييف الإجراء بأنّه إجراء تحقيق بسيط أو جزء من إجراء آخر، لا يغيّر من القول بكون هذا العمل يعدّ إجراء من إجراءات التحقيق القسرية التي وجب خضوعها للإتفاقيات الدولية فهو يشكّل إنتهاكا صارخا لسيادة الدّول، فاتباع هذا النهج من قبل بعض الدّول يمكن أن يجعل الأمر يصل إلى مراحل القصوى إذا ما أعتد من بقية الدّول عملاً بمبدأ المعاملة بالمثل، و عاقبة ذلك هو الفوضى و استباحة الخصوصية بشكل غير معقول.

ب) - الاتجاه المناهض للتفتيش المعلوماتي العابر للحدود

لا ريب أنّه طبقاً لمبدأ الإقليمية لا يمكن لأيّ دولة أن تمدّد إختصاصها خارج حدود إقليم دولة أخرى ذات سيادة⁽¹⁾، إذ لا يسمح لدولة بأن تمارس وسائل قسرية على إقليم دولة أجنبية⁽²⁾، فالإجراءات القسرية - و من بينها التفتيش - التي تقع على إقليم دولة أخرى تعتبر غير مشروعة، إلاّ إذا كان القانون الدولي يجيزها⁽³⁾، و هذا المبدأ العتيد تتمسك به كافة الدّول، بحيث نستشعر ذلك من خلال حرص كافة الإتفاقيات الدولية على صونه، و قد أكّدت عليه الإتفاقية العربية لمكافحة جرائم تقنية المعلومات بموجب نصوص واضحة الدلالة.

(1) «Lotus» (France –Turquie), Arrêt du 7 septembre 1927, C.P.J.I., Série A, n° 10.

(2) شيماء عبد الغني محمد عطالله ، المرجع السابق ، ص 297.

(3) Conseil de l'Europe, la criminalité informatique ,(Recommandation no R (89) 9 sur la criminalité en relation avec l'ordinateur et rapport final du comité européen pour les problèmes criminels , Editions du Conseil de l'Europe, Strasbourg, 1990.p 98.

و إلى هذا الاتجاه يرجع موقف أغلب التشريعات العربية و المقارنة⁽¹⁾، كما حرصت المحكمة العليا الفيدرالية الأمريكية على احترام هذه القاعدة في قرار حديث صادر عنها في قضية **"United States v. Microsoft Corporation"** ⁽²⁾.

قصارى القول أنه مع التسليم جدلاً بكون فعالية هذا الإجراء مرهونة بسرعة إمتداده إلى أنظمة معلوماتية يعتقد إحتواؤها على عناصر الإثبات، إلا أنه لا يمكن مكافحة أفعال غير مشروعة بموجب إجراء غير شرعي⁽³⁾، لذ تبدو الدّول غير مستعدة في وقتنا الزّاهن لقبول طلبات إجراء التّفّتش المعلوماتي العابر للحدود التي تعتبرها بمثابة مساس بسيادتها⁽⁴⁾.

⁽¹⁾ تنص المادة 124 القانون اللبناني رقم 81 لسنة 2018 و المتعلّق بالمعاملات الإلكترونيّة و البيانات ذات الطّابع الشّخصي "...يمكن ضبط أية بيانات أو دليل رقمي مخزّن في نظام معلوماتي موجود على الأراضي اللبنانيّة إذا كان ممكناً الوصول إليها من النظام المعلوماتي المقرّر تفتيشه، يمكن الوصول إلى أية بيانات مخزّنة في نظام معلوماتي، وضبطها، أيّا كان مكان وجودها داخل أو خارج لبنان، إذا كانت موضوعة تحت تصرف الجمهور أو في حال موافقة الشّخص المخوّل قانوناً بإفشاء هذه البيانات من خلال نظام معلوماتي موجود على الأراضي اللبنانيّة... " و هو نفس الحكم الذي تمنه نص المادة 4 القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات و المادة 30 من القانون القطري رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونيّة.

⁽²⁾ في تفاصيل هذه القضية أنّه خلال سنة 2013، حصلت الضّبطية القضائية على أمر قضائي إستناداً إلى قانون خصوصية الاتصالات الإلكترونيّة لسنة 1986 (ECPA) موجّه لمقدم الخدمات Microsoft لمساعدة السّلطات في إجراء تفتيش معلوماتي خارج الحدود للكشف عن كل رسائل البريد الإلكتروني وغيرها من المعلومات المرتبطة بحساب العميل يعتقد أنّه متورط في الإتجار غير المشروع بالمخدرات. و قد قرّرت Microsoft أنّ محتويات البريد الإلكتروني الخاصة بالحساب تمّ تخزينها جميعاً في مركز بيانات Microsoft في دبلن (إيرلندا)، و قد طالب مقدّم الخدمات بإلغاء هذا الأمر دون جدوى و على إثر استئناف الحكم الابتدائي، تصدّت الدائرة الاستئنافية لهذا الإجراء بتقرير عدم مشروعيته مؤكّدة بالكشف عن الاتصالات الإلكترونيّة المعنية سيكون تطبيقاً غير مصرّح به خارج الحدود الإقليمية مؤكّدة أنّ القانون يجيز "الوصول" (عن بعد) إلى خادم تحت الولاية القضائية الإقليمية للقاضي الفيدرالي للولايات المتحدة، أما التّفّتش الذي يجري خارج الحدود الإقليمية الأمريكية و يجب خضوعه لإجراءات المساعدة القانونية المتبادلة الدوليّة.

United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018).

⁽³⁾ Marie-Cristine Piatti, op cit, p 168.

⁽⁴⁾ في دراسة أجرتها لجنة اتفاقية الجرائم الإلكترونيّة بمجلس أوروبا توصّلت من خلالها إلى أنّ طلبات المساعدة القضائية المتبادلة (غير فعّالة بشكل عام، لاسيما فيما يتعلّق بالحصول على أدلّة إلكترونية. بحيث تتراوح مدة الاستجابة للطلّبات بين ستة أشهر و 24 شهراً لذا عادة ما يتمّ التّخلي عن العديد من الطّلبات (التّحقيقات) و هذا ما يؤثّر على إنتزام الدّول بحماية المجتمع و الأفراد من جرائم الأنترنت و الجرائم الأخرى التي تتطوي على أدلّة إلكترونية

أمّا التشريع البلجيكي فنجدّه ينص صراحة بشكل قاطع على جواز امتداد الضبط المعلوماتي العابر للحدود عن طريق النسخ مع ضرورة إتخاذ إجراءات المساعدة القضائية المتبادلة لمواصلة عملية التفتيش⁽¹⁾، على أنّ الأمر لا يقف عند هذا الحد في إطار التشريع الجزائري إذ أنّ صياغة الفقرة 3 من المادة 5 من القانون 04/09 تفرز العديد من الإشكاليات:

أولاً، تطرق المشرع إلى حظر إمتداد نطاق التفتيش المعلوماتي بما يتجاوز الحدود الإقليمية إذا ما تبين مسبقاً بأنّ المعطيات المبحوث عنها و التي يمكن الدخول إليها إنطلاقاً من المنظومة الأولى تقع في دولة أخرى إلاّ عن طريق المساعدة القضائية الدولية، لكنه لم يتطرق إلى حظر التفتيش المعلوماتي الذي ينصبّ مباشرة على نظام معلوماتي يتواجد فعلياً على إقليم دولة أجنبية دون لزوم الوصول إليه بالمرور عبر النظام المعلوماتي المقرر تفتيشه⁽²⁾، و الموجود على الأراضي الجزائرية، لذا يتعيّن على المشرع سد هذا القصور لأنّ التفتيش العابر للحدود في كلتا الصورتين يشكّل إنتهاكاً لسيادة الدولة الأجنبية.

فسعي الدّول إلى إجازة التفتيش العابر للحدود إنّما بهدف التهرب من القيود التي تفرضها التشريعات الداخلية حال إتخاذ هذا الإجراء الخطير و هنا ينبغي أن نشير بأنّه لا يمكن لدولة أن تتصلّ من إلتزاماتها، باتخاذها إجراءً خارج إقليمها يُحظر عليها إتخاذه في إقليمها فقانون حقوق الإنسان يُطبّق عندما تمارس الدولة السّلطة خارج إقليمها، بحيث لا يمكنها أن تتصل من إلتزاماتها الدولية بحقوق الإنسان و أن تتجاهل قوانينها الوطنية الدّاتية

Conseil de l'Europe Rapport final du Groupe de travail du T-CY sur les preuves dans le clou, TCY(2016)5F Accès de la justice pénale aux preuves électroniques dans le cloud : Recommandations pour examen par le T-CY , Direction générale des droits de l'homme et de l'Etat de droit Conseil de l'Europe, Strasbourg, France, 2016,p 12.

(¹) l'article 39bis du Code d'instruction criminelle, inséré par la loi du 28 novembre 2000 et modifié par la loi du 6 juin 2010, "Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le procureur du Roi communique sans délai cette information au Service public fédéral Justice, qui en informe les autorités compétentes de l'état concerné, si celui-ci peut raisonnablement être déterminé.

(²) D. Bénichoi, op cit, p 225.

باتخاذ إجراءات خارج إقليمها يُحظر عليها اتخاذها في إقليمها، و من جهة أخرى فإنّ مسؤولية الدولة عن حماية الحق في الخصوصية لا تنتهي عند حدودها الجغرافية (1).

ثانياً، جاء حظر التفتيش المعلوماتي العابر للحدود بنص عام، إذا لم يتم الحصول على إذن من الدولة التي يوجد النظام المعلوماتي المستهدف بالتفتيش على أراضيها، على الرغم من أنّ اتفاقية بودابست و الإتفاقية العربية لمكافحة جرائم تقنية المعلومات نصتا على استثنائين، بحيث يمكن الوصول إلى أية بيانات مخزّنة و ضبطها، أيّا كان مكان وجودها داخل أو خارج الدولة، إذا كانت موضوعة تحت تصرف الجمهور أو في حال موافقة الشخص المخوّل قانوناً بإفشاء هذه البيانات (2) و كان على المشرّع تقييد النصّ بهذه الاستثناءات لأنّها تشكّل مظهر من مظاهر تحقيق التوازن بين متطلبات الفعالية و الشرعية.

ثالثاً: أغفل المشرّع الجزائري تحديد طبيعة الجزاء الإجرائي الذي يلحق التفتيش المعلوماتي و الدليل المستمد منه حال تنفيذ إجراء تفتيش على أراضي دولة أجنبية دون الحصول على المساعدة القضائية أو إذن هذه الدولة و هناك ثلاثة فرضيات يمكن تصورها في هذا الصدد، الحالة التي تتجاهل فيها السلّطة الإجرائية مبدأ الإقليمية و تباشر إجراءات توسيع التفتيش المعلوماتي خارج الحدود مع علمها مسبقاً بذلك، و الفرض الثاني يتعلّق بالحالة التي يتمّ فيها مباشرة التفتيش خارج إقليم الدولة بحسن نية أي دون تحقّق العلم المسبق بكون التفتيش يجري على أراضي دولة أجنبية (3)، و الحالة الأخيرة هي تلك التي يعذر فيها معرفة مكان إمتداد التفتيش حتّى بعد نهاية عملية التفتيش و هو وضع غالب الحدوث (4).

(1) موجز حلقة نقاش مجلس حقوق الإنسان المتعلقة بالحق في الخصوصية في العصر الرقمي، تقرير مفوضية الأمم المتحدة لحقوق الإنسان، وثيقة رقم A/HRC/28/39 بتاريخ 19 ديسمبر 2014، ص 22.

(2) المادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

(3) تطرقت لجنة اتفاقية بودابست إلى تعريف "حسن النية"، حيث لاحظت أنّ هذا الشرط يتمّ إستفاؤه في الحالة التي تكون فيها سلطة إنفاذ القانون أثناء التّحقيق، على يقين أو غير مدركة أنّ نظام الحاسوب المطلوب تفتيشه يقع على إقليم دولة أخرى، أو قد لا تعلم أيّ إقليم يقع فيه، أو أن تكون قد حصلت على أدلة واقعة ضمن إقليم بلد آخر عن طريق الخطأ .

Conseil de l'Europe Rapport final du Groupe de travail du T-CY sur les preuves dans le clou, op cit, p 54.

(4) في حالة تعذر معرفة المكان « disparition (de la connaissance) du lieu » أي عندما تكون البيانات "في مكان ما في السحابة"، فإنّها تنتقل من خادم إلى آخر و من مكان إلى آخر، بحيث يتم توزيعها في أماكن متعدّدة أو

أجاب المرشد الأمريكي لتفتيش و ضبط الحواسيب على هذا التساؤل، أنه عندما لا تعلم الضبطية القضائية أو حتى لا تستطيع معرفة أن البيانات المراد تفتيشها في منطقة واحدة موجودة فعلا خارج المنطقة، فإنّ الدليل الذي يتمّ ضبطه بعيدا عن منطقة أخرى من الطبيعي أن لا يؤدي إلى بطلان الدليل، حيث توصلت المحاكم إلى أن التفتيش الذي ينتهك المادة 41 من قانون الإجراءات الجنائية الفيدرالي لا يؤدي إلى بطلان الدليل المستمد منه إلا إذا تجاهل الضابط القضائي عمدا مقتضيات هذه المادة، فالمحاكم ترفض طلبات بطلان الدليل عندما يتعذر على أعضاء الضبطية القضائية الذين ينفذون عملية التفتيش معرفة ما إذا كانوا ينتهكون المادة 41 من قانون الإجراءات الجنائية الفيدرالي قانونا أو فعليا⁽¹⁾.

و مع ذلك فإنّه من الصّعب التّسليم بصحة هذا القضاء، ليس لكونه مخالف لقواعد الإختصاص و التي تعتبر من النّظام العام، أو لوجود انتهاك للسيادة الدّولية إذا ما تذرعت سلطات كل دولة بالجهل بالاختصاص، بل بأثر هذا المسلك على الحرّيات الفرديّة لأن مسألة الاختصاص في كثير من الأحوال مرتبط بمسألة الإمتداد، فالإختصاص مرتبط بالمحل الذي يجري تفتيشه و الذي يجب أن يكون محدّدا في الإذن القضائي كشرط مباشرة لتنفيذ التفتيش و جواز امتداد التفتيش دون تحديد عدد حالات الامتداد يشكل تجاهلا واضحا لنطاق لإذن القضائي، و عندئذ يصبح الحديث عن الضّمان القضائي مجرد فلسفة ليس إلا، كما انه من السير التمسك بعدم تحقق العلم المسبق بموقع التفتيش، لذا وجب البحث عن معيار آخر للاختصاص يراعي كل هذه المتطلّبات المتناقضة مع تكثيف التّعاول الدّولي في إطار

تتألف من عدة مجموعات فرعية من البيانات ضمن أماكن مختلفة، أو أنّ لها نسخ متطابقة، و بالتالي فهي متوفرة في أماكن متعدّدة في نفس الوقت، فإنّ التمسك بمبدأ الإقليمية لتحديد الإختصاص بإجراء التفتيش المعلوماتي أو ضبط الأدلة يثير صعوبات، و لهذا السّبب نؤيد توجه بعض الفقه الذي اقترح ضرورة إتباع نهج يتجاوز مبدأ الإقليمية، قد يمثّل هذا المعيار "سلطة الاستخدام" أو "المسؤول عن المعالجة" كأساس لشرعية التفتيش المعلوماتي و في حالة تعذر تحديد موقع البيانات على وجه اليقين، قد يتم ربط البيانات بشخص لديه القدرة على "التغيير أو المسح أو الحذف أو جعله غير قابل للاستخدام، و القدرة على منع الآخرين من الوصول إلى البيانات أو على استخدامها بأي شكل من الأشكال". حول معايير الإختصاص بالتفتيش المعلوماتي راجع:

Spoenle, Jan: cloud computing and cybercrime investigations: territoriality vs the power of disposal, Conseil de l'Europe, Strasbourg. Economic Crime Division Directorate General of Human Rights and Legal Affairs Council of Europe Strasbourg, 2010, pp 1-12 .

(¹) H. Marshall Jarrett, et al, op cit, p 85.

إتفاقيات دولية أو ثنائية تسمح بتقديم الطلب مباشرة إلى الأجهزة القضائية دون الإعتماد على الإجراءات التقليدية التي جرى عليها العمل في إطار المساعدات الدولية.

الفرع الثالث: الميقات الزماني لتنفيذ إذن التفتيش المعلوماتي

تعدّ قاعدة تحديد الميقات الزماني لإجراء التفتيش من أهم القواعد التي يحرص من خلالها المشرّع على تضيق نطاق التعدي على الحريات الفردية، باعتبارها مظهرا من مظاهر تحقيق الموازنة بين حق الهيئة الإجتماعية و حق الفرد كعضو من أعضائها، سواء من حيث ميعاد تنفيذ التفتيش (أولا)، أو المدة التي ينبغي تفتيش الإذن خلالها (ثانيا).

أولا: ميعاد تنفيذ إذن التفتيش المعلوماتي

إن تحوّل عملية التفتيش من خطوة واحدة إلى خطوتين يثير إشكالية هامة تتعلق بميعاد إجراء التفتيش في مرحلة التفتيش المادي (أ)، و إن كانت ذات الضمانات الزمنية تخضع لها مرحلة التفتيش المعلوماتي (ب).

أ- ميعاد تنفيذ مرحلة التفتيش المادي

تحرص التشريعات الإجرائية على حظر القيام بتفتيش المساكن و ما في حكمها في وقت معين، إمعانا في الحرص على تضيق نطاق الإعتداء على الحرية الفردية و حرمة المساكن⁽¹⁾، و لأنّ المسكن يعتبر حرما آمنا بنص دستوري، فإنّ المشرّع الجزائري نص على ضرورة أن يتمّ تفتيش المنازل في ميقات قانوني يحفظ له سكينته و حرمة شاغليه، فتنصّ المادة 47 فقرة أولى من قانون الإجراءات الجزائية "لا يجوز البدء في تفتيش المساكن أو

(1) قاعدة حظر إجراء التفتيش في وقت معين تندرج ضمن الشروط الشكلية للتفتيش و مع ذلك يذهب البعض إلى أنّها قاعدة موضوعية و يتناول بحثها عند الكلام في حصانة محل التفتيش و هذا الرأي لا يتفق مع المقصود من التفرقة بين الشروط الموضوعية للعمل الإجرائي و الشروط الشكلية له، فالشروط الموضوعية هي التي يلزم توفّرها لنشوء حق معين لشخص معين، و متى نشأ الحق فقد إستنفذت الشروط الموضوعية غرضها، و بقي أن تحدّد الشروط الشكلية الإطار الذي يتحرّك داخله الحق، أو بعبارة أخرى كيف ينبغي لهذا الحق أن يعمل فالشروط الشكلية إذن تنظّم كيفية ممارسة الحق بعد نشأته فعلا و ليس من شيء في أنّ حظر تفتيش مكان معين في وقت معين لا يتعلّق بثبوت الحق في اتخاذ الإجراء و إنّما يتصل بتنفيذ الإجراء بعد أن نشأ الحق في ممارسته بتوفّر شروط وجوده فهو ظرف شكلي للمعل مما يتصل بزمان اتخاذه.

حول هذا الموضوع: سامي حسن الحسيني، المرجع السابق، ص 294.

معابنتها قبل الساعة الخامسة (5) صباحا و لا بعد الساعة الثامنة (8) مساء إلا اذا طلب صاحب المنزل ذلك أو وجّهت نداءات من الدّاخل أو في الأحوال الاستثنائية المقرّرة قانوناً.

غير أنّه لا مجال للتمسك بهذا الضّابط الإجرائي عندما يتعلّق الأمر بجرائم المخدرات أو الجريمة المنظّمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبييض الأموال و الإرهاب و كذا الجرائم المتعلّقة بالتشريع الخاص بالصّرف⁽¹⁾.

و على ذلك فإنّ القاعدة العامة تقضي أن يتمتع مسكن الفرد أثناء اللّيل بحصانة تامة، و مع ذلك تباينت التّشريعات المقارنة في تنظيمها لهذا القيد، فمنها من حدّدت الميقات الرّماني بتفصيل دقيق، و تلك قاعدة إعتقها المشرّع الفرنسي بموجب المادّة 59 من قانون الإجراءات الجزائية محدّدا ميقات تفتيش المنزل من الساعة السادسة صباحا إلى غاية الساعة التاسعة ليلا⁽²⁾، و تباها المشرّع الأمريكي بموجب نص المادّة 41 من قانون الإجراءات

(¹) تنص الفقرة الثانية و الثالثة من المادة 47 من قانون الإجراءات الجزائية :

"غير أنّه يجوز إجراء التّفتيش و المعاينة و الحجز في كل ساعة من ساعات النّهار أو اللّيل قصد التّحقيق في جميع الجرائم المعاقب عليها في المواد 342 إلى 348 من قانون العقوبات و ذلك في داخل كل فندق أو منزل مفروش أو فندق عائلي أو محل لبيع المشروبات أو ناد أو منتدى أو مرقص أو أماكن المشاهدة العامة وملحقاتها، و في أي مكان مفتوح للعموم أو يرتاده الجمهور، إذا تحقّق أنّ أشخاصاً يستقبلون فيه عادة لممارسة الدّعارة.

و عندما يتعلّق الأمر بجرائم المخدرات أو الجريمة المنظّمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبييض الأموال و الإرهاب و كذا الجرائم المتعلّقة بالتشريع الخاص بالصّرف فإنّه يجوز إجراء التّفتيش و المعاينة و الحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النّهار أو اللّيل و ذلك بناء على إذن مسبق من وكيل الجمهورية المختص عندما يتعلّق الأمر بالجرائم المذكورة في الفقرة الثالثة أعلاه، يمكن لقاضي التّحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا و في أي مكان على امتداد التّراب الوطني أو يأمر ضباط الشّرطة القضائية المختصين للقيام بذلك.."

(²) Article 59 du cpc Modifié par Ordonnance 60-1245 1960-11-25 art. 12 JORF 27 novembre 1960

Sauf réclamations faites de l'intérieur de la maison ou exceptions prévues par la loi, les perquisitions et les visites domiciliaires ne peuvent être commencées avant 6 heures et après 21 heures.

Toutefois des visites, perquisitions et saisies pourront être opérées à toute heure du jour et de la nuit en vue d'y constater toutes infractions aux articles 334, 334-1, 335 du code pénal à l'intérieur de tout hôtel, maison meublée, pension, débit de boissons, club, cercle, dancing, lieu de spectacle et leurs annexes et en tout autre lieu ouvert au public ou utilisé par le public, lorsqu'il sera constaté que des personnes se livrant à la prostitution y sont reçues habituellement.

Les formalités mentionnées aux articles 56, 57 et au présent article sont prescrites à peine de nullité. »

الجنائية الفيدرالي يحظر تفتيش المساكن خارج النطاق الزماني المحدد من الساعة السادسة صباحاً إلى غاية الساعة العاشرة ليلاً بالتوقيت المحلي⁽¹⁾، و هناك من التشريعات من عالجتها بشكل عام بحظر التفتيش ليلاً كالتشريع القطري.

و رغم القيمة التي يمكن أن تضيفها هذه الضمانة الإجرائية على الحريات الفردية، إلا أننا نجد بعض التشريعات لم تحدّد وقتاً معيّناً لإجراء التفتيش، كالتفتيش المصري الذي ترك للقائم بالتفتيش تحديد الوقت المناسب للقيام به دون النظر إلى أي اعتبار آخر يتعلّق بالمحل المراد تفتيشه، و من ثمّ فهو جائز في كل أوقات الليل و النهار، و قد تواترت أحكام محكمة النقض المصرية على هذا المعنى⁽²⁾، و نفس التوجه نجده لدى المشرّع العراقي و الأردني، و انطلاقاً من قاعدة حظر تفتيش المساكن ليلاً، فإنّ مرحلة التفتيش المادي كخطوة أولى من خطوات تنفيذ التفتيش المعلوماتي تخضع لهذه القاعدة و إستثناءاتها المنصوص عليها قانوناً.

(¹) See Fed. R. Crim. P. 41 (effective December 1, 2009) ;

"..(B) "Daytime" means the hours between 6:00 a.m. and 10:00 p.m. according to local time....."

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(ii) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and ... "

(²) حيث قرّرت محكمة النقض المصرية "من المقرر قانوناً أن لمأموري الضبط القضائي إذا ما صدر إليهم إذن من النيابة بإجراء تفتيش أن يتخذوا ما يرونه كفيلاً بتحقيق الغرض منه دون أن يلتزموا في ذلك طريقة بعينها ما داموا لا يخرجون في إجراءاتهم على القانون، و يكون لهم تخير الطرف المناسب لإجرائه بطريقة مثمرة و في الوقت الذي يرونه ملائماً ما دام أنّ ذلك يتمّ في خلال الفترة المحددة بالإذن، لما كان ذلك، و كان التفتيش الذي قام به الضابط في هذه الدعوى مأذوناً به قانوناً فإنّ له أن يجريه بالطريقة التي يراها محققة للهدف منه بما في ذلك مفاجأة المطعم ضده في أي مكان و زمان ما دام أنّه قد التزم الحدود التي تضمّنّها إذن النيابة، و من ثمّ فلا تثريب عليه إن هو اقتحم على المطعم ضده غرفة نومه ليلاً و يكون ما انتهى إليه الحكم المطعم فيه من بطلان إجراءات القبض و التفتيش لا يقوم على سند من القانون مما يعيبه و يستوجب نقضه و الإحالة الطعن رقم 17 لسنة 49 جلسة 29/04/1979 س 30 مذكور لدى هلاي عبد الله أحمد، تفتيش نظام الحاسب الآلي، مرجع سابق، ص 175.

و في مقام الموازنة بين التشريعات المقارنة نرجّح موقف المشرّع الجزائري لأنّه يعكس بوضوح تمسّكه بالشّريعة الإجرائية و الحفاظ على سكينه الأفراد ليلا، فالمسكن يبقى دائما من أهم مجالات الحياة الخاصة فهو موضع هدوء الفرد و طمأنينته بعيدا عن فضول الغير، و مستقر أسراره، ففي غير حالات الضّرورة المبرّرة بمكافحة الجرائم الخطيرة يبقى المسكن متمتعا بحصانة تامة و مطلقة.

بيد أنّ هناك من الفقه من يرى أنّ هذه الضّمانة الإجرائية بدأت تتضاءل أهميتها بظهور إجراء التفتيش عن بعد *La perquisition à distance*⁽¹⁾، و هو قول غير صحيح على الإطلاق في اعتقادنا لكون التفتيش عن بعد وفقا لهذا المفهوم هو التفتيش السري الذي ينطلق من الأنظمة المعلوماتية المتواجدة بمقرات السّلطات المنتدبة لإجراء التّحقيق و هو في انتهاكه لحق السّرية أو الحرّية الفرديّة يتجاوز بكثير انتهاك حرمة المسكن ليلا، و تلك نتيجة طبيعية لظهور عصر المعلوماتية بحيث باتت وقائع حياة الفرد حتّى الحميمة منها تدور في الفضاء الإلكتروني الذي يخزّن عالما غير محدود من خصوصيات الفرد طيلة مراحل زمينة من حياته.

و من ثم فمن غير المجدي الإبقاء على أشكال التّمييز بين حرمة المسكن و حرمة البيانات، بحيث تتسع الفجوة بينهما رغم وحدة السرّ، لذا نرى عدم التّوسع في اللّجوء إلى التفتيش السري عن بعد بذريعة حماية حرمة المسكن، بل ينبغي الإبقاء عليه في حدود الضّرورة مع التّمسك بالقاعدة العامة بشأن الميقات الزّمني لإجراء التفتيش.

ب) - ميعاد تنفيذ مرحلة التفتيش المعلوماتي

تحدّد القواعد القانونية التي تنظم عملية التفتيش وجوب تنفيذ عملية التفتيش في غضون مدة زمنية محدّدة تسري من تاريخ صدور الإذن بالتفتيش، كما أنّه لا يجوز تفتيش المساكن قبل السّاعة الخامسة (5) صباحا و لا بعد السّاعة الثّامنة (8) مساء، و هذه المقتضيات معقولة إلى حد كبير في إقامة التّوازن بين الفعّالية و الشّريعة في البحث عن الأدلّة الماديّة، و هي الضّمانات التي تحكم الخطوة الأولى من مرحلة التفتيش المعلوماتي و لكن السّؤال يبقى مطروحا بالنّسبة للتفتيش المعلوماتي؟ هل تخضع هذه المرحلة لنفس الميقات الزّمني لإجرائها؟

(1) رشيدة بوكري، المرجع السّابق، ص 295.

معظم التشريعات بما فيها التشريع الجزائري، أغفلت معالجة هذه الإشكالية و أبقى التساؤل مطروحا، عموما هناك فرضيتين في هذا المقام:

الفرضية الأولى:

تطبيق المواعيد الإجرائية التقليدية على مرحلة التفتيش المعلوماتي، و مقتضى هذا المسلك أنه لا يمكن تنفيذ عملية التفتيش المعلوماتي قبل الساعة الخامسة صباحا و لا بعد الساعة الثامنة مساء، و هو معيار يستحيل اعتماده، لأنه لا يوجد أي سبب مقنع وفق فلسفة الشرعية الإجرائية يبرر منع الخبراء (من الضبطية القضائية) الذين يزاولون عملهم في مختبرات التحليل الحاسوبي الشرعي من مباشرة مهامهم ليلا ضمن الحدود الزمنية⁽¹⁾، التي يحظر فيها تفتيش المساكن، خاصة في أحوال الإستعجال أو القضايا ذات الخطورة الكبيرة على الأمن كالجرائم الإرهابية و التّجسس و غيرها.

الفرضية الثانية:

و مفاد هذا الإحتمال هو إسقاط متطلبات الميقات الزمنية على مرحلة التفتيش المعلوماتي، و هذا الفرض في الحقيقة ينطوي على قدر من التّجاوب مع الواقع العملي، و يظهر ذلك بشكل جلي في حالات امتداد التفتيش المعلوماتي أو حالة التفتيش العابر للحدود الذي لا يقتضي الحصول على الإذن المسبق للدولة التي يجري التفتيش على أراضيها (حالة المصدر المفتوح للجمهور ، أو الحصول على الموافقة الطوعية و القانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات)، فقد يقع تعارض بين التوقيت المحلي و توقيت الدولة الأجنبية و في ذلك ما يعرض التفتيش لعدم المشروعية مما يجعل هذه العقبة حائلا تمنع الوصول إلى الدليل قبل طمسه.

و بطبيعة الحال فإن الفرضية الثانية - و التي تعتبر عملية إلى حد كبير جدا- تترجع معها بعض الضمانات التقليدية و في مقدمتها حضور المتهم لعملية التفتيش، غير أنه لا وجود لأي بديل آخر فسواء تم التفتيش المعلوماتي (الخطوة الثانية) ليلا أو نهارا فإن ذلك لا يغير من الواقع شيئا لأنّ بعض حالات التفتيش المعقّدة إن لم نقل معظمها قد تستغرق عدة أسابيع أو أشهر و من غير المعقول و على فرض إتاحة الفرصة للمتهم لحضور عملية التفتيش أن يبقى بمقر المخبر يتربص الشروع في العملية طيلة هذه المدة الزمنية.

(1) Orin S. Kerr, Search Warrants in an Era of Digital Evidence, op cit, p 105.

ثانياً: مدة سريان الإذن في مرحلة التفتيش المعلوماتي

يشتمل الإذن عادة على تحديد مدة معينة ينبغي تنفيذ التفتيش خلالها و عندئذ يجب على الضبطية القضائية المنتدبة لاتخاذ هذا الإجراء مراعاة تنفيذه أثناء سريان المدة المحددة، و الذي ينبغي عند تحديد مدة سريان الإذن ألا تطول هذه المدة إلى الحد الذي يجعل المتهم مهدداً بالتفتيش لفترة طويلة، غير أن إنقضاء الأجل المحدد لإجراء التفتيش في الأمر الصادر به لا يترتب عليه بطلانه و إنما يصح تنفيذه بمقتضاه بعد ذلك إلى أن يجدد مفعوله لمدة أخرى كتابة، و يجوز لسلطة التحقيق أن تصدر أكثر من إذن لتفتيش المتهم و لكن تداخل مواعيد سريان أوامر التفتيش لا يعني أنها أوامر مفتوحة غير محددة المدة⁽¹⁾، و هو ما استقر عليه القضاء في ظل القصور التشريعي لأغلب الدول حيال هذه المسألة⁽²⁾.

و إن كان التشريع الجزائري و الفرنسي بقيا في غيبة من التعرض إلى تحديد النطاق الزمني لتنفيذ إذن التفتيش المعلوماتي في المرحلة المادية، فإن التشريع المصري استدرك هذا القصور بأن حدد مدة معينة يلتزم بها القائم بالتفتيش في تنفيذ الإذن، حيث نصت المادة 6 من القانون رقم 185 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات على أنه "لجهة التحقيق المختصة بحسب الأحوال، أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين لمدة لا تزيد عن ثلاثين يوماً قابلة للتجديد مرة واحدة.. البحث والتفتيش والدخول والنفاد إلى برامج الحاسب وقواعد البيانات و غيرها".

(1) سامي حسن الحسيني، المرجع السابق، ص 134.

(2) و من بين ما قرره محاكم النقض المصرية أنه "لما كان الشارع لم يشترط لصحة الإذن بالتفتيش الذي تصدره النيابة العامة أن يكون تنفيذه خلال مدة محددة فإذا ما رأيت النيابة تحديد المدة التي يجب إجراء التفتيش خلالها فإن ذلك منها يكون إعمالاً لحقها في مراعاة مصلحة المتهم و عدم تركه مهدداً بالتفتيش إلى وقت قد يتجاوز الوقت المحدد و إذا لم تحدد النيابة أجلاً لتنفيذ الإذن الذي أصدرته فإن هذا الإذن يعتبر قائماً و يكون التفتيش الذي حصل بمقتضاه صحيحاً قانوناً طالما أن الظروف التي إقتضته لم تتغير و إن تنفيذه تم في مدة تعتبر معاصرة لوقت صدور الإذن، لما كان ذلك و كان من المقرر أن الإذن الذي تصدره النيابة العامة لأحد مأموري الضبطية القضائية بتفتيش منزل مفعوله بتنفيذ مقتضاه فتمى أجرى الأمور المنتدب التفتيش فليس له أن يعيده مرة ثانية اعتماداً على الإذن المذكور - و لما كان المطعون ضده لم ينازع في أن تنفيذ الإذن كان المرة الأولى و في تاريخ معاصر لصدوره- اليوم التالي - فإن الحكم المطعون فيه إذ قضى ببراءة المطعون ضده على أساس أن إذن التفتيش صدر باطلاً لعدم تحديد مرات إستعماله يكون قد جانب صحيح القانون بما يعيبه و يوجب نقضه و الإحالة) الطعن رقم 1325 لسنة 49 جلسة 03/01/1980 س 31 ع 1 ص 32 ق 5.

كما حافظ التشريع الفيدرالي الأمريكي على هذا الضابط الإجرائي بحيث توجب المادة 41 من قانون الإجراءات الجزائية الفيدرالي أن يتضمن الإذن القضائي مدة محدّدة لتنفيذه و تلك المدة هي عشرة أيام و بعد خضوع هذا النص إلى التعديل سنة 2009 مددّ المشرع هذا النطاق الزمني إلى 14 يوما تسري من تاريخ صدور الإذن القضائي، غير أن ما يختص به التشريع الأمريكي أن هذه المدة هي المدة المحدّدة لتنفيذ مرحلة التفتيش المادي، و قد جاء ذلك واضحا في عبارة "يجوز وفقا للمادة 41 الإذن بضبط وسائط التخزين الإلكترونية أو ضبط أو نسخ المعلومات المخزّنة إلكترونيا ما لم ينص على خلاف ذلك، يأذن الأمر بالمراجعة اللاحقة للوسائط أو المعلومات بما يتوافق مع الإذن القضائي، ويشير وقت تنفيذ الإذن في القاعدة إلى ضبط أو نسخ محتويات وسائط تقنية المعلومات في الموقع، و ليس إلى أي وقت لاحق خارج الموقع..."⁽¹⁾، و في المقابل لا توجد قاعدة قانونية تنظم النطاق الزمني لمرحلة التفتيش المعلوماتي.

و قد تعمّد المشرع الأمريكي عدم النص على النطاق الزمني لتنفيذ التفتيش في مرحلته الثانية، موضحا الأسباب المبررة لهذا النهج الذي سلكه، و قد جاء في الأعمال التحضيرية لهذا التعديل أن الحقائق العملية للتفتيش المعلوماتي تحول دون التوصل إلى تحديد "مدة زمنية" تناسب جميع حالات التفتيش، لأنّ بعض العمليات تستنفذ وقتا طويلا بسبب تباين سعة التخزين الرقمي للوسائط التكنولوجية، فضلا عن الصعوبات الناشئة عن البيانات المشفرة أو المفحّخة، و كذا عبء العمل الجاري بمخابر التحليل الحاسوبي الشرعي، في مقابل ذلك لا تمنع هذه القاعدة القضاء من فرض مهلة زمنية لاستكمال عمليات التحليل و التفتيش، غير أنّ التحديد القانوني المسبق للفترة الزمنية يمكن أن ينجر عنه تزايد في طلبات منح مهل إضافية لاستكمال عمليات التفتيش⁽²⁾.

(1) See Fed. R. Crim. P. 41(e)(2)(B) (effective December 1, 2009) (B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review."

(2) Bartholomew, Paige "Seize First, Search Later: The Hunt for Digital Evidence," Touro Law Review: Vol. 30: No. 4, (2014), p 1037.

و كما سبق و أن أشرنا إليه سابقا، فإنّ مناط مشروعية الضبط أو التفتيش المعلوماتي لا يقتصر فقط على قصر النطاق الموضوعي للتفتيش المعلوماتي بل يعدّ معيار الوقت المناسب لتنفيذ الإجراء أساسا للحكم بمشروعيته بغية عدم ترك المتهم مهدداً بالتفتيش إلى وقت قد يتجاوز الوقت المعقول، لذا نجد أنّ القضاء الأمريكي و إزاء هذا القصور التشريعي قد اعتمد معيار "المعقولة" لتحديد ما إذا كان التأخير بين الضبط الأولي و التفتيش اللاحق دسوريا أم لا⁽¹⁾.

و حسنا فعل المشرع الأمريكي بعدم فرض نطاق زمني معين لتنفيذ مرحلة التفتيش المعلوماتي، لأنّ الحالات الواقعية تكشف أنّ معيارا زمنيا موحدًا لا يمكن أن يناسب جميع عمليات التفتيش، بسبب الاختلاف الواضح بينها بخصوص عدد أجهزة التخزين المضبوطة و سعة تخزين كل منها و تشفيرها من عدمه، في الوقت ذاته فإنّ هذا النطاق الزمني و على فرض تضيقه يفتح باب التعسف في بعض العمليات البسيطة التي لا تتطلب وقتا كبيرا، و

(¹) خلال سنة 2010 تم اتهام Metter و ستة متهمين آخرين بالمشاركة في جريمة الإحتيال و تنفيذًا للإذن القضائي تمكّنت الحكومة من ضبط مجموعة من الحواسيب من مكتب الشركة و منزل المتهم و شمل ذلك، من بين أمور أخرى، واحد و ستون محرك أقراص صلبة للكمبيوتر، و خادم البريد الإلكتروني للشركة، و محتويات الأقراص الصلبة الشخصية الأربعة للمتهم و قد تمّ نسخ البيانات مع رد البيانات الأصلية لمالكها، لكن الحكومة لم تجر تحليلا لمحركات الأقراص الصلبة إلا بعد مرور خمسة عشر شهرا على تنفيذ أمر الضبط، قدم المتهم طلبا ببطلان الأدلة، بحجة أنّ "التأخير الكبير للحكومة في إجراء عمليات تفتيش خارج الموقع يستوجب البطلان شامل لجميع الأدلة المضبوطة" لأنّ التأخير لمدة خمسة عشر شهرا كان غير معقول و ينتهك التعديل الدستوري الرابع، و قد ردت الحكومة على هذا الدّفع بكون الضبط الإجمالي لمحركات الأقراص الصلبة و الاستعراض اللاحق لهذه البيانات كان ضروريا نظرا لطبيعة الأدلة الرّقمية و فيما يتعلّق بالتأخير بين الضبط و التحليل الجنائي، قالت الحكومة "إنّ قيامها الفوري برد البيانات الأصلية لمالكها ينفي وقوع أيّ ضرر قد ينجم عن التأخر في التفتيش المعلوماتي للبيانات التي تمّ نسخها. و قد بدأت المحاكم تحليلها لهذا الطّلب من خلال طرح تساؤل مؤداه ما إذا كان احتفاظ الحكومة بالبيانات المضبوطة مدة 15 شهرا قبل الشروع في تفتيشها ينطوي على انتهاك للحق في الخصوصية أين قرّرت المحكمة أنّ الإجابة على هذا السّؤال يتطلب تحليلا واقعيًا دقيقًا لكل حالة على حدى "لأنّ ما قد يكون مناسبًا في إطار مجموعة واحدة من الوقائع و الطّروف قد أن لا يكون ذلك في إطار آخر". و مع ذلك، خلصت المحكمة إلى أنّ تأخر الحكومة أكثر من خمسة عشر شهرا" في مراجعة النسخة المصوّرة من الأدلة الإلكترونيّة المضبوطة، في ظل وقائع و ظروف هذه القضية بالذات، يشكّل "تجاهلا صارخ من الحكومة لمسؤوليتها" للشروع في تفتيش تحليل شرعي عاجل للأدلة المصوّرة، في ظل هذه الطّروف، كان غير معقول .

أنظر الحكم Metter, 860 F. Supp. 2d at 212، مذكور و معلق عليه لدى:

Bartholomew, Paige, op cit, p 1040 .

في هذه الأحوال يتيح الضبط المعلوماتي المتواصل للسلطة التحقيق إمكانية توسيع التفتيش دون حدود واضحة على نحو يجعل التأخير في تنفيذ التفتيش غير شرعي.

لذلك نحن نعارض توجه المشرع المصري الذي لم يفرق بين مرحلتى التفتيش (المادي و المعلوماتي) في تحديد النطاق الزمني لسريان الإذن القضائي، لأنه من غير المعقول أن يسمح المشرع بإطالة مدة سريان إذن تفتيش المساكن بحثا عن الدّعات المادية لمدة شهر كامل، لانعدام ما يسوّغ هذه المدة لأنّ التفتيش المادي لا يتجاوز دقائق و على الأكثر عدة ساعات، و من جهة أخرى فإنّ هذه المدة لا تتناسب مع طبيعة التفتيش و الهدف منه، لأنّ الجاني يحرص على إتلاف الأدلة المعلوماتية فور تمام مشروعه الإجرامي، فالفعالية تستوجب سرعة التنفيذ في هذه المرحلة، في مقابل ذلك، فإنّ تعقيد التفتيش المعلوماتي قد يتطلب أضعاف المدة التي قررها المشرع، لذا نرى أنّ المشرع المصري لم يتبصر عواقب تحديد الإطار الزمني للتفتيش، و الوضع على ما هو عليه في اختلال كبير بين طرفي المعادلة، فالمدة المحددة تهدر الفعالية و الشرعية بذات الوقت و في كلتا المرحلتين⁽¹⁾.

أما بالنسبة إلى التشريع الجزائري فهو لا يحدّد مدة معينة لتنفيذ الإذن بالتفتيش في كلتا المرحلتين خاصة بالنسبة لمرحلة التفتيش المادي، فمن غير المعقول إطلاقها من غير قيدها بنطاق زمني محدد و ترك المتهم مهذّا بالتفتيش إلى أجل غير مسمى، تاركا مصير حرّيته وفقا لتقدير الضبطية القضائية، لذا ينبغي الحد منه لاسيما و أنّه يتعلّق بحريات الأفراد و حرمة منازلهم و أسرهم و عوراتهم فمن الواجب صونها بكل السبل.

لقد آن للمشرع الجزائري أن يتدخّل و يعالج هذه المسألة بنص صريح يحدّد فيه مدة فاعلية الإذن بالتفتيش في مرحلة التفتيش المادي (مرحلة التفتيش عن الأجهزة المادية و ضبطها) فيضع حدا أقصى لا يتجاوز 14 يوم، على أن ينص أيضا على لزوم أن يتضمّن الإذن مدة محدّدة لتنفيذ مرحلة التفتيش المعلوماتي ضمن الإذن القضائي، سواء كان الضبط الأولي نتاج تفتيش مادي أو بواسطة الأمر بالتسليم الموجه إلى مزوّد الخدمات، مع ترك

(1) من الأمثلة البسيطة التي تثبت عدم صحة المطالبة بتحديد نطاق زمني على مرحلة التفتيش المعلوماتي، التعقيد التقني للتشفير الذي يعد عقبة كبيرة تحول دون إمكانية تنفيذ التفتيش خلال فترة زمنية محددة، ففي قضية R v ADJ 102 VSCA [2005] استغرقت السلطات الاجرائية في إنجلترا فترة تزيد عن اربعين اشهر لفك التشفير و الولوج الى النظام المعلوماتي لاسترداد الصور الإباحية للأطفال القصر. راجع:

Stephen Mason, Daniel Seng, op cit, p 263.

تقديرها لسلطة التحقيق حسب ظروف التحقيق، و جعلها قابلة للتجديد متى قامت المبررات الداعية إلى ذلك بموجب أمر كتابي من القاضي المختص، و في حالة عدم مباشرة التفتيش خلال النطاق الزمني الممنوح من قبل القاضي أو إنقضاء المدة دون تجديدها يقرّر حق المتّهم في المطالبة باسترجاع وسائط التخزين الرقمية في حالة ضبطها و المطالبة بحذف البيانات في حالة الضبط المعلوماتي.

تلك هي الأحكام العامة الواجب على المشرّع مراعاتها، في ظل هذا القصور التشريعي الذي نراه مخالفا للشريعة الدستورية لأنّه يتيح للسلطة الإجرائية القيام بالتفتيش متى شاءت و لا مرية أنّ إطالة أمد التفتيش هو اعتداء لا مبرر له على الحريّات الفرديّة لذا وجب وضع حدا لها.

المطلب الثاني: تحديد أسلوب تنفيذ التفتيش المعلوماتي

مهما بالغ المشرّع في تقييد التفتيش المعلوماتي بمختلف الضوابط السابق بيانها، فإنّ نجاحه في الحفاظ على الحق في الخصوصية يظل مرتعنا بمدى صون تلك الضوابط عند تنفيذ التفتيش، لأنّ غياب حدود مادية لمحل التفتيش يجعل التفتيش بدون حدود واضحة مما حذى بالقضاء الأمريكي إلى إرساء ضابط جديد من شأنه إعادة رسم الحدود المفقودة في هذه البيئة يطلق عليه استراتيجية التفتيش لذا سنتطرق إلى نشأة القاعدة (فرع أول) و المعالجة الفقهية القضائية لها في ضوء الجدل الخصب الدائر بشأن مدى دستوريته (فرع ثاني) ثم نستعرض الطرح الفقهي البديل لها (الفرع الثالث).

الفرع الأول: مدلول قاعدة لزوم تحديد أسلوب تنفيذ لتفتيش المعلوماتي

تقتضي الشريعة الإجرائية عند التنفيذ المعلوماتي الحد من حرّية المتّهم الشخصية بالقدر اللازم لتنفيذه دون تجاوز الغاية منه، غير أنّ غياب البعد المادي للدليل المعلوماتي، مع إنتشار عناصر الإثبات ضمن عالم من البيانات تختلط فيها البيانات المجرّمة مع البيانات البريئة و استحالة تحديد موقعها قبل تنفيذ التفتيش، مع لجوء المجرمين إلى جعل الملف البريء ستارا للملف المجرّم و دفنه ضمن المساحة الفارغة، ما جعل هذا الإجراء أكثر امتداد و توسّعاً للملفات التي يحتويها وسيط التخزين الرقمي، على نحو يتجاوز الغاية التي تبرّره، حيث تراجعت القاعدة لحساب الاستثناء.

و إزاء هذا الوضع لجأ الفقه و القضاء إلى المطالبة بإتباع "نهج خاص" **special approach** في تنفيذ إذن التفتيش المعلوماتي يحقق الدور الوقائي المتوخى من الضمانات الإجرائية التي تقيّد هذا الإجراء القسري بفرض شروط مسبقة يشرف عليها القاضي المختص للموافقة على إصدار إذن بالتفتيش المعلوماتي، إصطاح على تسميتها ببرتوكول التفتيش⁽¹⁾، و يقصد به إلزام الضبطية القضائية بأن تشرح لقاضي التحقيق خطة تنفيذ التفتيش مع مطالبتهم بتبريرها كشرط مسبق لإصدار إذن بذلك، و الغرض منها تقليل المخاطر المتزايدة على الحق في الخصوصية لأنها تجعل التفتيش أكثر تحديداً، و تلغي ضرورة الضبط الشامل و بذات الوقت تساعد القضاء على مراقبة عمل الضبطية القضائية التي يتعيّن عليها تكييف تفتيشها

(1) و تعزى فكرة وضع إستراتيجية تفتيش محدّدة توضّح الخطوات المسبقة التي يجب على المحلّل إتباعها للحد من نطاق امتداد التفتيش المعلوماتي إلى القرار الصادر سنة 1982 عن الدائرة التاسعة في قضية *United States v. Tamura* التي تصدى فيها القضاء الأمريكي إلى بيان موقفه بشأن الضبط الإجمالي العرضي و التفتيش الشامل للوثائق الورقية التي تتشابه فيها الوثائق الخارجة عن نطاق الإذن القضائي مع تلك التي تعدّ موضوعاً للدليل الجنائي، و في هذه القضية أجرى مكتب التحقيقات الإتحادي تحقيقاً بشأن جريمة رشوة بعد الحصول على إذن يسمح بضبط وثائق الشركة سعياً للوصول إلى دليل الجريمة، و لأنّ العاملون بالشركة رفضوا مساعدة الضبطية القضائية في تحديد الوثائق ذات الصلة بالجريمة، و بحكم المشقة و المدة التي تستنفذها عملية التفتيش، قامت هذه الأخيرة بضبط عدّة صناديق و عشرات الأدراج المليئة بوثائق ورقية مختلطة و من بينها تلك المستندات التي لا علاقة لها بالتحقيق الجاري، و تم نقلها خارج الموقع لتفتيشها لاحقاً، و على الرغم من أنّ هذه الجهة القضائية أشارت إلى أنّ الضبط الإجمالي للسجلات بما فيها الوثائق التي لا يشملها الإذن القضائي يعتبر مخالفاً للتعديل الدستوري الزابع، إلّا أنّها لم تقرّر بطلان الدليل الجنائي الذي تمّ ضبطه بشكل صحيح، غير أنّها قرّرت ضمانات إجرائية جديدة منعا من التوسع في التفتيش عبر الملفات البريئة، مؤداها أنّه في الحالات التي تكون فيها الوثائق متشابكة بحيث لا يمكن تصنيفها عملياً في الموقع، ينبغي على الضبطية القضائية تحريز المضبوطات و ختمها و الاحتفاظ بها ريثما يتمّ الحصول على إذن آخر يسمح بتوسيع نطاق التفتيش و بالتالي ينبغي لقاض محايد أن يرصد أية عملية ضبط إجمالي، ليس فقط حتى يكون هذا الأخير على علم بما أذن به، و لكن أيضاً حتى تترك الضبطية القضائية حدود التفتيش.

حول مدلول هذه القاعدة و نشأتها يراجع:

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

مع البيانات المطلوبة⁽¹⁾، و قد تمّ إرساؤه لأول مرة أمام الدائرة العاشرة في قضية **United States v. Campos**⁽²⁾.

بشكل عام قسّم الفقه القيود التي يمكن أن تحدّد عملية تنفيذ التفتيش المعلوماتي إلى أربعة شروط، القيود التي تحدّد من عملية الضبط في مرحلة التفتيش المادي، و الشروط التي تحدّد من النطاق الزمني للتفتيش المعلوماتي، الشروط المتعلقة بكيفية إجراء التفتيش المعلوماتي و الظروف التي ينبغي فيها رد المضبوطات⁽³⁾.

ففيما يتعلّق بشروط مرحلة التفتيش المادي، فإنّه يستحيل وقت الضبط الأولي تحديد البيانات المستهدفة بالتفتيش و فصلها عن غيرها من البيانات وسط هذا الكم الهائل من البيانات لأنّها عملية تستغرق وقتاً و البديل العملي الوحيد هو ضبط معظم أو حتّى جميع دعائم التخزين الرقمية و التفتيش عنها لاحقاً خارج الموقع و تعتبر الدائرة التاسعة الجهة القضائية الوحيدة التي استلزمت شرطاً إجرائياً إضافياً بحيث توجب على الضبطية القضائية ضرورة تقديم المبررات الكافية للضبط الشامل ضمن الإفادة الخطية (طلب الإذن) و ذلك في قضية **United States v. Hill**⁽⁴⁾.

أمّا النوع الثاني من القيود فيتعلّق بتحديد المهل الزمنية لاستكمال الخطوة الثانية من التفتيش و هي مرحلة التفتيش المعلوماتي لأنّ المادة 41 من قانون الإجراءات الجنائية الفيدرالي لا تحدّد سوى مدة إجراء الضبط الأولي و المقدرة بأجل أربعة عشرة يوماً، مما يترك

(1) H. Marshall Jarre, et al, op cit. p75.

(2) United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000).

(3) Kerr, Orin S, Ex Ante Regulation of Computer Search and Seizure, op cit , p 1251.

(4) جاء في قرار الدائرة التاسعة الصادر بتاريخ في 11 أوت 2006 في قضية **United States v. Hill** بعد الاعتراف بصعوبة عزل المواد الإباحية قبل الضبط الشامل ما يلي: " و مع ذلك، فإنّ هذا لا يعني أنّ الحكومة لديها سلطة إجراء تفتيش عشوائي عند إلتماس أو تنفيذ أذن التفتيش المعلوماتي، فعلى الرّغم من أنّ تكنولوجيا المعلومات قد تبرز من الناحية النظرية الضبط الشامل للأسباب المبينة أعلاه، فإنّه يقع على الحكومة أن تثبت للقاضي من الناحية الواقعية لماذا تكون هذه السلطة الواسعة للتفتيش و الضبط معقولة في الحالة قيد النّظر، فقد تكون هناك حالات لا يكون فيها للحكومة أساس للاعتقاد بأنّ التفتيش المعلوماتي ينطوي على نوع من التعقيدات التكنولوجية التي من شأنها أن تجعل التفتيش الفوري في الموقع و استرداد الأدلة المطلوبة أمر غير عملي...لذا يجب وضع حدود قبل أن تلجأ الحكومة "لضبط كومة قش للتفتيش عن الإبرة".

توقيت المراجعة اللاحقة لتقدير القائم بالتفتيش، و في مواجهة هذا الغموض، فرض بعض قضاة التحقيق متطلباتهم الخاصة بالإطار الزمني لعمليات التفتيش المعلوماتية⁽¹⁾.

و باقي أنواع القيود تحدّد كيفية تنفيذ مرحلة التفتيش المعلوماتية للحد من الوصول إلى بيانات تقع خارج نطاق الإذن القضائي، و تحول بذلك دون التوسع في التفتيش و بدورها تتوّع بحسب طبيعة الدليل المعلوماتية المستهدف⁽²⁾، و يضرب الفقه أمثلة عن بروتوكولات التفتيش

(¹) تعتبر قضية United States v. Brunette من بين أهمّ التطبيقات القضائية على هذا النوع من القيود الإجرائية، التي أصدر فيها قاضي التحقيق إدنا بنفتيش أجهزة الحاسوب مع تقييد النطاق الزمني للتفتيش المعلوماتية بمدة ثلاثين يوماً بعد التفتيش المادي. و قبل فترة وجيزة من انقضاء المدّة الزمنية، تقدّمت الضبطية القضائية بطلب منحها أجلاً إضافياً و تمّت الموافقة على الطلب بتجديد الميعاد الإجرائي بمدة ثلاثين يوماً، أين تمّت تفتيش أحد أجهزة الحاسوب خلال المدّة الإضافية، دون التمكن من تفتيش الجهاز الثاني خلال هذه الفترة الزمنية، وقد كشف كلا التفتيشين عن صور إباحية للقصر، قضت المحكمة بقبول الصور المكتشفة خلال الفترة الزمنية المضافة، لكن الصور المكتشفة على الحاسوب الثاني بعد انقضاء المدّة، تم اعتبارها دليلاً باطلاً بناءً على فشل الحكومة "في التقيّد بمتطلبات إذن التفتيش" و مع ذلك فإنّ هناك أحكام أخرى قرّرت مشروعية الدليل الجنائي و لو تجاوز التفتيش النطاق الزمني المفروض في الإذن القضائي.

يراجع بهذا الخصوص:

Orin S. Kerr, op cit, p 1252.

(²) في الحقيقة فإنّ هناك العديد من الجهات القضائية الابتدائية التي كانت سبّاقة إلى التمسك بمبدأ لزوم التقيّد بمنهجية التفتيش كشرط للموافقة على إذن التفتيش قبل صدور قرار الدائرة العاشرة، و من بين أهمّ الأحكام التي أشار إليها الفقه الأمريكي، الحكم الصادر عن المحكمة الابتدائية في مقاطعة Utah سنة 2001 لما قرّرت بطلان الأدلة المعلوماتية التي تمّ ضبطها من حاسوب المتهم، و خلصت إلى أنّه بمجرد علم الضبطية القضائية بوجود وثائق مختلطة على الحاسوب، كان ينبغي عليها تقديم منهجية تفتيش لجعل نطاقه أكثر تحديداً، و الحكم الصادر عن المحكمة الابتدائية لمنطقة إلينوي الشمالية، و ذلك في إطار التحقيق في جريمة غش ضريبي و بناء على طلب الحكومة أصدر هذا الأخير إدنا يجيز تفتيش منزل محاسب و ضبط أجهزة الحاسوب التي يتمّ العثور عليها بمقر إقامته، مع تقييد مرحلة التفتيش المعلوماتية بلزوم تقديم بروتوكول تفتيش مسبق يتضمّن وصف المعلومات التي تسعى الحكومة للحصول عليها و الأساليب التي تخطّط لاستخدامها بغية تحديد موقع هذه البيانات على نحو يحول دون استعراض باقي المعلومات التي لا علاقة لها بالجريمة موضوع التحقيق على اعتبار و أنّ الحاسوب منزلي يرجح أن يتضمّن بيانات خاصة جداً و بعد تنفيذ المرحلة الأولى، ناقش القاضي مع الحكومة الطّرق الممكنة لتضييق التفتيش المعلوماتية، بما في ذلك: "قصر التفتيش على فترات زمنية محدّدة"، أو "استخدام عمليات البحث عن الكلمات الرئيسية"، أو "قصر التفتيش على ملفات نصّية و استبعاد ملفات الصور"، و أمام الموقف السلبي للحكومة تم رفض الموافقة على إذن التفتيش المعلوماتية مع تحديد أجل واحد و عشرين يوماً لتقديم بروتوكول تفتيش أو رد جهاز الحاسوب إلى مالكه.

التي تحقّق هذه الغاية، و من بينها البحث التلقائي باستخدام الكلمات الرئيسية، أو البيانات الوصفية "Metadata"⁽¹⁾. و قد تأكّد هذا التّطبيق القضائي في قضية *United States v. Comprehensive Drug Testing* عندما واجهت الدائرة العاشرة نفس التّحدي مجدّداً، و هو اختلاط البيانات و تعدّد 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 الضّبط الموسّع هو جزء لا يتجزأ من عملية التفتيش المعلوماتي فإنّه لأجل تحقيق التوازن الصّحيح بين مصلحة الحكومة في التّطبيق الفعّال للقانون و حق الأفراد في التّحرر من عمليات التفتيش و الضّبط غير المعقولة عند فصل البيانات المعلوماتية الجائز ضبطها عن تلك التي ليس للحكومة سبب محتمل لها، و يجب إعتماد قاعدة *Tamura* بخصوص إشكالية الضّبط الموسّع (مرحلة التفتيش المادي).

أمّا بشأن مرحلة التفتيش المعلوماتي فإنّها قرّرت خمسة قيود جديدة تضيق بشكل كبير من نطاق امتداد التفتيش بحيث إشتراطت للموافقة على إذن التفتيش، أن تتنازل الحكومة عن الإعتماد على مبدأ الرؤية الكاملة (*the plain view doctrine*)، و أوجبت أن يتمّ فرز البيانات من قبل طرف مستقل فإن تمت هذه العملية من قبل متخصص حكومي و يجب عليه

حول مجمل هذا الموضوع راجع:

Christina M. Schuck, op cit, p 776.

(1) و هي طريقة مفيدة بشكل خاص عندما يركّز الإستعلام على مستندات محدّدة و تكون اللّغة المستخدمة متوقعة نسبياً، فعلى سبيل المثال تقوم عمليات البحث عن الكلمات الرئيسية بالعثور على المستندات التي تتضمّن فرداً معيناً أو تاريخاً محدّداً، و هناك برامج أخرى تسمح باستخدام عبارات أو مفاهيم معيّنة و من ثم تحدّد كل وثيقة تحتوي على معلومات ذات صلة بتلك البنود، بما يُمكن من قصر نطاق التفتيش على تلك المستندات التي تحتوي على بيانات مرتبطة بتلك العبارات أو المفاهيم بدلاً من فتح كافة الملفات و الإطلاع على محتوى كل وثيقة و تعدّد البيانات الوصفية أيضاً وسيلة قيمة للحد من نطاق التفتيش و تحول دون إقتال كاهل الدّولة، و هي معلومات يقوم الحاسوب بتخزينها تلقائياً حول كل مستند أو ملف موجود على محرك الأقراص الثابتة، تتضمّن بعض المعلومات التي تمّ إلقاطها بواسطة الحاسوب كتاريخ إنشاء مستند؛ حالة تعديل هذا المستند، و تاريخ إدخال التعديل عليه، المعلومات المحدّدة التي تمّ تعديلها؛ تاريخ طباعة المستند؛ و حتّى من قام بإنشاء تلك الوثيقة و من خلال إستغلال هذه المعلومات يمكن للضّبطية القضائية تحديد موقع العناصر ذات الصّلة بالتحقيقات دون إجراء تفتيش إستكشافي عام باستعراض كافة المستندات الموجودة على الحاسوب.

حول مجمل هذا الموضوع راجع:

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.

عدم الكشف سوى عن البيانات المستهدفة، و اشترطت أيضا أن تبين الإفادة الخطية لطلب الإذن عن المخاطر الفعلية التي قد تفضي إلى تدمير المعلومات، كما شددت على ضرورة وجود منهجية تفتيش مصممة خصيصا للكشف فقط عن المعلومات التي لها سبب محتمل، و أخيرا أكدت على ضرورة محو البيانات التي لا تستجيب للإذن القضائي دون استعراض محتواها⁽¹⁾.

إن هذا القرار يعتبر محاولة غير مسبوقة لوضع قواعد واضحة لحماية الحرية الفردية في مواجهة امتداد التفتيش المعلوماتي، إذ قيد مرحلة التفتيش المادي بوجود الكشف عن المخاطر الفعلية لتدمير البيانات في حالة معينة، بدلا من الاعتماد على المخاطر العامة لتبرير الضبط العرضي الشامل، لأن التفتيش المعلوماتي خارج الموقع قد لا يكون صحيحا دائما بسبب التطورات التكنولوجية التي أوجدت برامج متطورة تجعل التفتيش في الموقع ممكنا و ذلك ما قرره القضاء في قضية **United States v. Greathouse**⁽²⁾.

(1) United States. v. Comp. Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010).

و تتمثل و وقائع هذه القضية أنه في خلال سنة 2002، شرعت الحكومة في إجراء تحقيق حول توفير المنشطات غير الشرعية للاعبين البيسبول المحترفين في هذه الفترة، أبرمت رابطة لاعبي البيسبول بالدوريات الكبرى اتفاقاً جماعياً مع Major League Baseball ينص على اختبار المخدرات لجميع اللاعبين بدون استثناء أين قامت شركة خاصة تدعى Comprehensive Drug Testing بجمع العينات من اللاعبين؛ عقب ذلك تمت الاختبارات الفعلية بواسطة مخبر Quest Diagnostics، فاحتفظت الشركة بقائمة اللاعبين و نتائج الاختبار الخاصة بهم و قد وصل إلى علم السلطات أن هناك نتائج إيجابية تخص عشرة لاعبين على إثرها تحصلت الحكومة على إذن بالضبط، و عندما انتقلت الضبطية لتنفيذ هذا الإذن قام المختص بتحديد موقع مجلد رقمي يُعرف باسم "Tracey" و الذي يحتوي على السجلات. لم يحتوي دليل Tracey على نتائج اللاعبين العشرة المحددين في إذن الضبط فقط، ولكنه تضمن أيضاً نتائج الاختبارات لمئات من لاعبي البيسبول و غيرهم، خلص المتخصصون إلى أنهم يستطيعون نسخ الدليل دون ضرورة اللجوء إلى ضبط أجهزة التخزين الرقمية، و في وقت لاحق تم تفتيش هذا المجلد أين كان البحث أكثر امتدادا و توسعا عبر ملفات ليست لها علاقة بالموضوع، و عندها تقدمت الرابطة بطلب رد المضبوطات الخاصة بكل شخص لم يرد اسمه في الإذن القضائي وافقت المحكمة على ذلك بالأمر برد دليل Tracey باستثناء النتائج العشرة المذكورة في إذن الضبط، و أسست المحكمة قضاءها بناء على التّجاهل الواضح لحدود الإذن القضائي بتجاوز نطاق الإذن بشكل كبير و عند الاستئناف، تناولت الدائرة التاسعة قرار محكمة المقاطعة بشكل مفصل و اعتبرت أن الضباط تصرفوا بشكل معقول لم يكونوا مطالبين برد أي من المعلومات، و في الوصول إلى هذا الاستنتاج، اعتمدت المحكمة على ما تقرّر في قضية Tamura و التي مؤداها أن السبب المعقول لضبط ملفات ورقية معينة وردت في الإذن تسمح فنيا بضبط ملفات برئية أخرى مختلطة مع الملفات المشتبه بها.

(2) United States v. Greathouse, 297 F. Supp. 2d 1264, 1275 (D. Or. 2003).

و قيد مرحلة التفتيش المعلوماتي بحصر نطاق التفتيش عن طريق إستراتيجية تفتيش أو برنامج حاسوبي يستبعد البيانات الخارجة عن نطاق الإذن من التفتيش، كما قيد مرحلة ما بعد التفتيش بوجوب رد المضبوطات في حالة الضبط المادي أمّا في حالة الضبط المعلوماتي، فقد قرّر وجوب محو و حذف هذه البيانات كما حظر استخدام الأدلة الجنائية المكتشفة بشكل عرضي باستثناء الأدلة المستهدفة.

هكذا تمكن القضاء الأمريكي من استحداث مفاهيم إجرائية جديدة تتفاعل فيها الإجراءات الجنائية مع البيئة الرقمية، و لعلّ أهمّها هو البطلان كجزء إجرائي يلحق التفتيش و الدليل المستمد منه متى وقع بالمخالفة للشروط التي تقيد تنفيذ عملية التفتيش المعلوماتي بمعزل عن الضمانات الإجرائية الأخرى، و يطلق الفقه على هذا المفهوم الجديد للبطلان بالبطلان الاستباقي "preemptive suppression"⁽¹⁾.

و هذا المصطلح يعكس الهدف الذي تتوخاه القاعدة بغرض تتجنب انتهاك الحق في الخصوصية، عن طريق إخطار الحكومة مسبقا بلزوم التقيد بحدود الإذن و ما فرضه من شروط تحت طائلة بطلان الدليل الجنائي المستهدف بالتفتيش، لحملها على الإلتزام بالمشروعية التي باتت تستمد من الإذن ذاته، و إذا كان الوضع الطبيعي هو إنهاء الضبط برد المضبوطات إلى من له الحق في الملكية فإنّ الضبط المعلوماتي يستلزم محو البيانات التي هي في حوزة الحكومة إثر الضبط المعلوماتي و هو ما بات يعرف بالحق في الحذف (المحو و التدمير) "Right to Delete".

الفرع الثاني: المعالجة القضائية و الفقهية لقاعدة لزوم تحديد أسلوب تنفيذ لتفتيش المعلوماتي

لقيب قاعدة لزوم تحديد استراتيجية تنفيذ التفتيش المعلوماتي اهتماما متفاوتا إذ لا يجمع الفقه و القضاء على موقف واحد تجاه أهميته، بل و حتّى دستوريته على الرّغم من أنّ هذا الضابط الإجرائي المستحدث له أهمية بليغة في إعادة الإعتبار للحريات الفردية (أولا)، إلا أنّ هناك إتجاها فقهيًا يدعمه القضاء يعارض هذه القاعدة بناء على حجج لها وجاهتها (ثانيا).

(1) 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: (2012) Vol. 7: No. 4, p 22.

أولاً: الإتجاه المؤيد للقاعدة

ثمة اعتبارات عديدة يستند إليها مؤيدوا قاعدة وجوبية تحديد استراتيجية تنفيذ التفتيش المعلوماتي في الإذن للموافقة عليه و هي تركز عموماً على حماية الحريات الفردية، و ضمان الإشراف القضائي المباشر على عملية تنفيذ التفتيش، بالإضافة إلى اعتبارات عملية أخرى كما نوضحه بالتفصيل:

أ- حماية الحريات الفردية

مضمون هذه الحجة أنّ الضمانات الإجرائية التي تقررت لحماية الحريات الفردية في مواجهة التفتيش المعلوماتي سوف تفقد سبيلها للتطبيق بغير الإستعانة بهذه القاعدة، بحيث يصبح التفتيش عاماً دون حدود واضحة تضبط نطاقه، ففي سياق التفتيش الرقمي تتطافر الجهود بين القاضي و القائم بالتفتيش لأجل تحديد المكان الذي سيجري تفتيشه وفق متطلبات التعديل الدستوري الرابع، حيث يتكامل السؤال "المتعلق بكيفية التفتيش" مع مسألة "ما سيجري التفتيش عنه" لأنّ المفهوم المادي للحدود يصبح مجازياً في العالم الرقمي و من ثمّ فإنّ البروتوكولات المسبقة التي تحدّد كيفية القيام بالتفتيش هي الوسيلة الوحيدة لوصف موقع الأماكن و الملفات الرقمية التي سيتمّ تفتيشها على وجه التحديد⁽¹⁾.

فاستراتيجية تنفيذ التفتيش هي وسيلة لضمان شرط تحديد محل التفتيش، ففي سياق الإطار التقليدي يتمّ قصر التفتيش على جزء فقط مما هو مطلوب، كغرفة بدلاً من منزل بأكمله، أو صناديق تحتوي على علامات معينة بدلاً من مستودع، و كذلك تعتبر استراتيجية تنفيذ التفتيش مقبولة تماماً في العالم الرقمي، "إذ لا يتمّ الوصول إلى معلومات معينة من خلال الممرات و الأدراج، بل من خلال الأوامر والاستعلامات الموجهة لأجهزة الحاسوب. و بالمثل، عند محاولة وصف الأشياء التي يجب ضبطها، لن تكون هناك طريقة لتحديد أشياء محدّدة أو مساحات معينة عن طريق وصف الإحداثيات المادية الخاصة بها و لكن عن طريق وصف كيفية تحديد موقعها نتيجة لذلك، فإنّه في العديد من الحالات، تكون الطريقة الوحيدة الممكنة لتحديد منطقة معينة من الحاسوب هي تحديد كيفية التفتيش"⁽²⁾.

(1) Commonwealth v. Keown, 478 Mass. 232, 240-41 (2017).

(2) In re Search Warrant, 71 A.3d 1158, 1169 n.11 (Vt. 2012).

و من ناحية أخرى فإنّ الغرض من القاعدة ليس فرض قيود غير معقولة على عمليات التفتيش، بل ترمي إلى تحديد كيفية استبعاد المعلومات التي لا صلة لها بالجريمة من نطاق التفتيش، فعلى سبيل المثال، توجد برامج خاصة بحساب قيمة التجزئة للبرامج و الملفات المشتركة يُمكن استخدامها من فرز المعلومات المستهدفة عن ما يختلط بها من بيانات، كما أنّها تتيح للقائم بالتفتيش الذي لا يركّز على برامج معالجة النصوص استخدام قيمة التجزئة لهذا البرنامج لاستبعاده من المراجعة⁽¹⁾.

(ب) - الإشراف القضائي المباشر على التنفيذ

من بين الحجج التي يستند إليها الإتجاه المساند لهذه القاعدة، أنّ تقييد عملية تنفيذ التفتيش من شأنها الحيلولة دون حصول تجاوز من قبل الضبطية القضائية و إخضاع نشاطها لرقابة قضائية لصيقة، فهي لا تمنع التوسع غير المعقول للتفتيش و الضبط في البيئة المعلوماتية فحسب، بل إنّها تعيد أيضاً إحياء دور القاضي كحكم محايد مسؤول عن تحديد مدى دستورية سلوك الضبطية القضائية، ففي الوقت الحالي و بدون منهجية التفتيش، تتمتع الضبطية القضائية بسلطة تقديرية واسعة لتحديد معايير تفتيش حسب ما يترأ لها، مما يحدّ من سلطة القضاء في تقدير مدى معقولية عملية التفتيش المعلوماتي مسبقاً و قبل إجرائه⁽²⁾.

و الأهمّ من ذلك، إذا 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، فإنّ حماية الحرّيات الفردية بهذا الشكل تصبح خاضعة لتقدير الضبطية القضائية⁽³⁾، فمن خلال اشتراط منهجية التفتيش مع ضرورة الحصول مسبقاً على إذن قضائي بذلك، سيكون القضاء مجدداً في وضع يمكنه من تقدير عمليات التفتيش المعلوماتي غير المعقول⁽⁴⁾.

(¹) Christina M. Schuck, op cit, p 777.

(²) Derek Haynes, op cit , p 772.

(³) Christina M. Schuck, op cit, p 778.

(⁴) Derek Haynes, op cit , p 772.

(ج) - إعتبرات عملية

مفاد هذه الحجّة على أنّ استراتيجية تنفيذ التفتيش هي الطريقة التي من شأنها أن ترفع النّقل عن كاهل الحكومة فيما تتحمّله من نفقات و موارد بشرية لإجراء تفتيش معلوماتي لمستودعات غير محدودة من البيانات، فالنهج التقليدي للتفتيش و الضبط يسمح من الناحية النظرية بتطبيقه في البيئة الرقمية من خلال فحص كل ملف على حدى بحثاً عن الأدلة من غير داع لإتباع منهجية تفتيش محدّدة مسبقاً، لكن ذلك يجافي الواقع، فليس لدى الجهة القائمة بالتفتيش الوقت و الموارد اللازمة لفحص كل جزء من البيانات المخزّنة على أجهزة الحاسوب، الأمر الذي يدفع بالضبطية القضائية إلى استخدام أيّ طريقة ممكنة لتضييق مجموعة البيانات الفرعية التي يجب عليهم تفتيشها لاكتشاف الأدلة التي يشملها الإذن القضائي، و هذا التضييق في نطاق عملية التفتيش يحقّق مصلحة الأفراد و مصلحة الحكومة، ففي حالة وجود طرق تفتيش أقلّ مساساً بالحياة الخاصة و أكثر فعالية، سيكون من غير المعقول عدم مطالبة المحقّقين باستخدام تلك الأساليب⁽¹⁾.

ثانياً: الإتجاه المناهض للقاعدة

تتعالى منذ إرساء هذه القاعدة أصوات فقهية و قضائية منتقدة لهذه القاعدة و مطالبة باستبعادها و قد تعدّدت الحجج التي يتذرع بها الإتجاه المناهض لهذه القاعدة بعضها يقوم على الإعتبرات المتعلقة بالضمانات الدستورية و البعض الآخر على إعتبرات الفعالية، و انعدام الخبرة لدى القضاء في فرض مثل هذه الاستراتيجيات ذلك له على التّفصيل التّالي:

(أ) - الإعتبرات الدستورية

يرى المعارضون أنّه إستناداً إلى التّعديل الدستوري الرابع فإنّ فرض بروتوكولات التفتيش يعتبر تطبيق قضائي غير دستوري بحجة أنّ القضاة لا يتمتّعون بالسلطة القانونية التي تؤهلهم لفرضها، فدور قاضي التّحقيق عند إصدار أذن الضبط و التفتيش يقتصر فقط على تقدير مدى تحقّق شرطي السّبب المحتمل و عنصر التّحديد في الإفادة الخطية، دون أن يكون له الحق في رسم حدود كيفية تنفيذ هذه الأذن، لأنّ تقدير مدى معقوليتها يخضع

(¹) Lily R. Robinton, Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence, YALE J.L. & TECH V 12, (2010), p 343.

للمراجعة القضائية اللاحقة بأثر رجعي بدلا من المراجعة القضائية السابقة على التنفيذ، مستنديين في ذلك إلى مدلول النصوص القانونية في مختلف الولايات التي كانت صياغتها واضحة الدلالة في حرمان القضاة من سلطة رفض طلبات الحصول على إذن بالتفتيش بناء على كيفية تنفيذه، علاوة على ذلك فإن هذا التقييد ليس له أي أثر قانوني لأن تقدير مدى دستورية التفتيش تتوقف على ما إذا كان التفتيش معقولا إستنادا للحكم الصادر بعد التنفيذ، دون إعتبار لما إذا كانت الحكومة قد امتثلت فعلا للقيود المسبقة أم لا⁽¹⁾.

و هو ما قرّره الدائرة التاسعة في قضية **United States v. Schesso** فصلا في قضية إستغلال الأطفال في المواد الإباحية، رفضت طلب بطلان الأدلة المعلوماتية التي تم استردادها بموجب إذن قضائي واسع النطاق، بضبط و تفتيش حاسوب المتهم و جميع أجهزة التخزين الرقمية الخاصة به، على الرغم من طلب البطلان كان يستند عيب إجرائي شاب الإذن بالتفتيش بخلوه من برتوكول التفتيش يحظر امتداد نطاقه، و خلصت المحكمة إلى أن برتوكولات التفتيش لا يفرضها الدستور و لا يمكن معاتبة خبراء التحليل الحاسوبي أو الضبطية القضائية لاعتمادها لعدم إتباع بروتوكولات غير ملزمة لهم⁽²⁾، و بموجب هذا القرار تكون الدائرة التاسعة قد تراجعت عن الطابع الإلزامي لاجتهاداتها بأن جعلت تطبيق القاعدة يخضع للسلطة التقديرية للقضاة.

(1) Kerr, Orin S, Ex Ante Regulation of Computer Search and Seizure, op cit, p 1261.

(2) United States v. Schesso, 730 F.3d 1040 (9th Cir. 2013).

و تتعلّق وقائع القضية بصدور إذن بالتفتيش استهدف حاسوبا محمولا و محركين للأقراص الصلبة الخارجية بحثا عن صور للمتورطين في الجريمة و صورا للمواد المخدرة غير المشروعة، غير أن التفتيش اللاحق أفضى إلى الكشف عن صورة داعرة للقصر، و بناء على ذلك طالب المتهم ببطلان هذه الأدلة للتوسع في التفتيش خوفا عن نطاق الإذن القضائي نتيجة لعدم الإلتزام بقاعدة التّحديد المسبق لمنهجية التفتيش وقد تصدّت الدائرة العاشرة لطلبه بالرفض موضحة أن هذه المحكمة لم تطالب نهائيا لزوم أن تضمن أذون التفتيش استراتيجية تفتيش دقيقة قد يكون التفتيش المعلوماتي واسعا بقدر ما هو مطلوب بشكل معقول لتحديد العناصر الموضحة في إذن الضبط بناء على السبب المحتمل (الدلائل الكافية) و لم يقيد إذن التفتيش بناء على إسم امتداد الملف أو أسماء الملفات أو هيكلية الدليل، بدلا من ذلك تم تقييد نطاق التفتيش بشكل واضح من خلال قصر البحث عن الملفات الحاسوبية التي تشكل دليلا عن تعاطي المخدرات أو الإتجار بها و هذه الملفات يمكن أن تتخذ أشكالا عديدة. قد تكون عبارة عن ملفات نصية عامة، مستندات معالجة النصوص، برامج معالجة النصوص، ملفات برنامج البريد الإلكتروني، جداول بيانات أو ملفات قاعدة بيانات وغيرها.

إن أول من تصدى لهذا التقد هو القاضي **Sidney I. Schenkier** حيث يرى "أنّ الأساليب و المعايير التي بموجبها يتم إجراء التفتيش المعلوماتي ينبغي تقديمها إلى القاضي قبل إصدار إذن الضبط و إمّا أن تقدم لدعم إفادة خطية للحصول على إذن ثان أكثر تحديدا بمجرد اكتشاف وثائق مختلطة، و ليس صائبا أو مطلوب قانونا إتباع نهج يؤدي إلى نتائج أخرى.. لا نعتقد أنّ هذا النهج هو الذي إنصرفت إليه نية المحكمة العليا عندما أشارت بأنه يقع على المسؤولين عند إجراء عمليات التفتيش التقليل إلى أدنى حد ممكن من التداخلات غير المبررة على الخصوصية... فالغرض من مراجعة طلبات إصدار الأذن من قبل قضاة محايدين هو ضمان الوفاء بمتطلبات توافر الأسباب المحتملة و قيام شرط التّحديد في الإذن، و عندما تكون هناك مخاوف بشأن عنصر التّحديد في التفتيش... فمن المنطقي و المستوجب دستورياً معالجة تلك المخاوف في بداية العملية، و حسمها بطريقة تتجنّب فيما بعد بطلان الأدلة"⁽¹⁾.

و في هذا الصدد يرى الفقيه **Paul Ohm** أنّ القضاة ليس لهم فقط السّطة القانونية لفرض هذه القيود بل يقع واجب عليهم القيام بذلك، معتبرا إياه بمثابة ضمان إجرائي يحلّ محل السبب المحتمل و عنصر التّحديد المفقدين في أذن التفتيش المعلوماتي و ليس فقط لضمان التنفيذ المعقول و ذلك في كلّ حالة تفتيش معلوماتي تقريبا⁽²⁾.

فلا يوجد في التّعديل الدستوري الرابع ما يمنع قضاة التّحقيق من فرض شروط مسبقة تضع حدودا لنطاق الإذن القضائي طالما أنّ هذه القيود تسعى لتحقيق هدف دستوري (شرط التّحديد في الإذن القضائي) "فما ينبغي على القضاء التّأكد منه لا يتوقّف عند مجرد قيام سبب محتمل للإعتقاد بأنّ التفتيش قد يفضي إلى كشف الأدلة الجنائية، بل ينبغي التّأكد من قيام الأسباب المبررة لانتهاك حق الفرد في الخصوصية، فعلى الرّغم من أنّ القانون أجاز لأفراد حق في الطّعن في مشروعية التفتيش بعد تنفيذه فإنّ المراجعة اللاحقة لا تحقّق الغرض الذي لأجله تمّ تقنين حماية هذا الحق"⁽³⁾.

(¹) In re 3817 W. West End, First Floor Chicago, Illinois. 60621.2004 WL 138002272(ND III May 27,2004).

(²) Paul Ohm, Massive Hard Drives, General Warrants, and the Power of Magistrate Judges, Virginia Law Review, Vol 97, (2011), p 5.

(³)In re Search Warrant, 71 A.3d 1158, 1169 n.11 (Vt. 2012).

و ذات التبرير اعتمده المحكمة العليا في ماساتشوستس في قضية *Dalia v. United States* مؤكدة على دستورية هذه الضمانات الإجرائية و الحاجة إليها، نافية وجود أي تناقض بين هذا الضابط الإجرائي و سوابق المحكمة العليا، و استطردت قائلة بينما استقرت المحكمة العليا الفيدرالية على أنه "يترك عمومًا لتقدير الضباط المنفذين لتحديد تفاصيل أفضل السبل للمضي قدماً في إجراء تفتيش مرخص به بموجب إذن قضائي" (1)، فإن ذات المحكمة أيضا استقرت على أنه "يجب الحرص على التأكد من إجراء عمليات تفتيش بطريقة تقلل إلى أدنى حد ممكن من الانتهاكات غير المبررة على الحق في الخصوصية" (2).

و في هذه القضية و تحقيقا في جريمة سرقة الهوية Identity Theft صدر إذن بالتفتيش المعلوماتي يستهدف ضبط السجلات المرتبطة بالجريمة "أي شكل من الأشكال التي يعثر عليها" سواء في أجهزة الحاسوب أو وسائط إلكترونية، غير أن القاضي قيد نطاق التفتيش المعلوماتي ببرتوكول يتضمن عشرة شروط و هي 1) وجوب تخلي الشرطة على مبدأ الرؤية الكاملة في ضبط أي سجل رقمي غير مرخص به في الإذن و أي دليل معلوماتي لا يتعلّق بالجريمة (موضوع التحقيق، 2) تعيين طرف مستقل (فني متخصص) يتولى إجراء التفتيش و تزويد الشرطة ب الأدلة المعلوماتية المتعلقة فقط بهذه الجريمة، 3) إشتراط الفصل بين الأدلة المعلوماتية المتعلقة بالجريمة عن غيرها من البيانات المختلطة بها قبل تسليمها إلى المحقق "بغض النظر عن مدى تداخلها"، 4) منع أفراد الشرطة الذين يشاركون في التفتيش من الإداء بهذه المعلومات التي لا صلة لها بالتحقيق للنيابة العامة أو قضاة التحقيق، 5) قصر بروتوكول التفتيش على الأساليب المصممة للكشف فقط عن المعلومات التي يكون للحكومة سبب محتمل لها، 6) منع استخدام "تقنيات التجزئة" المتخصصة أو تقنيات تفتيش مماثلة دون الحصول على إذن محدد من المحكمة، 7) قصر النسخ فقط على الأدلة ذات الصلة بالنشاط الإجرامي المستهدف و تمكين الحكومة منها، 8) مطالبة الحكومة برد "البيانات الخارجة عن نطاق الإذن القضائي" و إبلاغ المحكمة بهذا الإجراء، 9) يتعين على الشرطة تدمير النسخ المتبقية من البيانات الإلكترونية في غياب إذن قضائي يقضي بغير ذلك، 10) مطالبة الحكومة بتقديم تقرير دقيق في غضون المهلة الزمنية المحددة بالإذن يتضمن الكشف عن البيانات التي تم الحصول عليها و التي تمت إعادتها و التي تم تدميرها و محوها. أين تقدمت الحكومة بطلب إلغاء القيود التي فرضت على تنفيذ التفتيش المعلوماتي و دعما لالتماسها إستندت هذه الأخيرة إلى الحجة التي تمسك بها الفقيه أرين كير و التي مفادها و أنّ القاضي ليس له سلطة فرض قيود مسبقة على التفتيش لكونها تحول دون فعالية التحقيق، فبدلا من التصريح بإجراء عملية تفتيش في مكان معين أو لأشياء معينة، كان القاضي يحاول إملاء الطريقة التي يجب أن تنفذ بها عملية التفتيش فالقيود المسبقة غير دستورية لأنها تحدّد مسبقاً معقولة التفتيش، الأمر الذي يتجاوز سلطة القاضي و قد رفض هذا الطلب و على مستوى المحكمة العليا تمت الموافقة على 03 قيود، القيد الثاني و الخامس و السابع.

(1) *Dalia v. United States*, 441 U.S. 238 (1979).

(2) *Andresen v. Maryland*, 427 U.S. 463 (1976).

أما بخصوص المرحلة الإجرائية التي يتدخل فيها القضاء للبت في مدى مشروعية التفتيش، فقد صرحت هذه المحكمة بأن القيود المسبقة لا تحل محل المراجعة القضائية اللاحقة لتحديد مدى دستورية التفتيش و أن لكليهما أهداف مختلفة، فبينما تعالج المراقبة القضائية اللاحقة الضرر الذي حاق بالفرد نتيجة التفتيش المخالف للدستور، تسعى البروتوكولات المسبقة إلى تفادي الضرر الذي تهدف سبل الإنصاف اللاحقة إلى التخفيف منه، و من ثم فإن قصر الإشراف القضائي على المراجعة اللاحقة لا يؤدي فقط إلى تمكن الحكومة من ضبط كميات هائلة من بيانات الأفراد فحسب بل يفضي إلى ترك الأفراد عرضة لعمليات تفتيش غير دستورية مما يجبرهم على الدفاع عن حقوقهم الدستورية بعد وقوع الضرر، فبروتوكولات التفتيش لها وظيفة وقائية منفصلة.

و من التطبيقات القضائية الدالة على وجوب التفاعل بين هاتين المقاربتين ما يكشف عنه آخر الإجتهد القضائي للمحكمة العليا في بنسلفانيا و ذلك في قضية **Commonwealth v. Johnson Lavelle** و في هذه السابقة القضائية أكدت المحكمة على ضرورة المحافظة على جميع الضمانات الإجرائية سواء المراجعة القضائية السابقة أو اللاحقة لتنفيذ الإذن، تأسيسا على أن التكنولوجيا الحديثة كما وقرت قدرة تخزين كبيرة لكميات هائلة من البيانات الشخصية مكنت أيضا من إيجاد برامج حاسوبية لإجراء عمليات تفتيش ضيقة و جاء التأكيد على لزوم مراعاة هذه الضمانة الإجرائية حتى في الحالة التي يتمكن فيها الإذن القضائي من تحديد الأشياء المراد ضبطها فإنه ينبغي أن تكون هناك قيود فعالة على عملية تنفيذ التفتيش منعا من امتداده و صيرورته عاما كما لفتت المحكمة الانتباه إلى ضمانات المراجعة القضائية اللاحقة تفاديا من جعلها مجرد مراجعة محدودة بل حرصت على أن تتاح فيها فرصة للأطراف للإدلاء بدفاعهم بخصوص نطاق التفتيش و الخطوات التي إتخذت لتضييق تفتيش البيانات الخارجة عن نطاق الإذن القضائي حتى يتم الوفاء بهذا القيد الدستوري⁽¹⁾.

(ب) - إعتبارات الفعالية

مؤدى هذه الحجة أن هذه القاعدة بمثابة قيد يحول دون فعالية التفتيش، لذا عارضت وزارة العدل الأمريكية بشدة اعتماد هذا القيد الإجرائي واصفة إياه بكونه "مرهق" و "غير مجدي" بل و "غير ضروري" و تقوم حجة هذه الأخيرة على إعتبارات فنية بذريعة أن فرض

(1) Commonwealth v. Johnson, L., Pet, 434 WAL 2018 (Pa. 2019).

قيود على كيفية تنفيذ التفتيش يؤدي إلى إعاقة سلطة الحكومة بشكل كبير جدا في اكتشاف الأدلة المعلوماتية، فإجراءات التحليل الحاسوبي الشرعي تتطلب من القائم بالتحليل الاعتماد على حدسه و اتخاذ الخطوات المناسبة بناء على الحقائق التي تواجهه وقت الفحص⁽¹⁾.

و من القيود المرهقة التي يمكن أن تفرض على المحقق أن يقتصر تفتيشه بالبحث على الملفات التي تحتوي على كلمات رئيسية معينة قد يتضمن تحليل الطب الشرعي عمليات بحث عن الكلمات المفتاحية، و لكن التحليل الشرعي الذي يتم تنفيذه بشكل صحيح نادرا ما ينتهي عند هذا الحد لأنّ عمليات البحث عن الكلمات المفتاحية سوف تفشل في العثور على أنواع عديدة من الملفات التي تقع ضمن نطاق إذن الضبط و بالإضافة إلى ذلك، يمكن أيضا إحباط عمليات البحث عن الكلمات المفتاحية باستخدام كلمات مشفرة⁽²⁾.

و لقد لقيت هذه الحجة تأييدا واسع النطاق من قبل القضاء، ففي قضية **United States v. Hill**، دفع المتهم ببطلان الدليل المعلوماتي على أساس أنّ الإذن القضائي لم يتضمن بروتوكول تفتيش يقيد تقدير الضبطية القضائية بخصوص ما يمكنهم فحصه عند التفتيش و أنّ الإفادة الخطية لم تبين سبب عدم وجود مثل هذا البروتوكول لأنّه كان يجب أن يقتصر التفتيش على بعض الملفات التي من المرجح أن ترتبط بحيازة الصور الداعرة للأطفال، مثل تلك التي تحتوي على امتدادات تشير عادة إلى احتواء الملفات على الصور أو تلك التي تحتوي على كلمة محددة مرتبطة بالجريمة، و في معرض تأسيسها لرفض الطلب أوضحت الدائرة الفيدرالية التاسعة أنّ منهجية التفتيش المقترحة من المتهم غير معقولة لأنّ سجلات الحاسوب تكون عرضة للتلاعب أو الإخفاء أو التدمير سواء كان ذلك بشكل متعمداً أو من دون قصد، فبالإمكان إخفاء الصور في جميع أنواع الملفات، و حتّى في مستندات معالجة النصوص و جداول البيانات. و أنّ المجرمون سيبدلون كل ما في وسعهم لإخفاء المواد المجرّمة، باستعمال أبسط الوسائل لتغيير أسماء الملفات و امتداداتها لإخفاء محتواها من المراقبة العادية، و من ثمّ فإنّ إجبار الضبطية القضائية على قصر عمليات التفتيش على الملفات التي وصفها المتهم بطريقة معينة سيكون أمراً شبيهاً بالقول أنّه ليس بإمكان هذه الأخيرة ضبط كيس بلاستيكي يحتوي على مادة بيضاء مسحوقة يشتهب بها إذا ما تمت تسميته

(1) H. Marshall Jarrett, et al, op , cit, p 79.

(2) H. Marshall Jarrett, et al, op , cit , Loc.Cit.

بالدقيق، إذ لا توجد طريقة لمعرفة ما هو موجود في ملف ما دون فحص محتوياته، تمامًا كما لا توجد طريقة مؤكدة لتحديد مادة الكوكايين إلا عن طريق خضوعها للتّحليل. و انتهت المحكمة بالقول "نحن ننظر بشكل إيجابي إلى إدراج بروتوكول التنقيش في الإذن القضائي؛ لكن غيابها لا يترتب عنه البطلان"⁽¹⁾.

و هو ما أكّده الدائرة العاشرة في قضية **BURGESS UNITED STATES v.** حين أبدت رفضا شديدا لهذا القيد و خلصت إلى القول أنّه "من غير العملي توقّع وجود إذن يقيد نطاق التنقيش المعلوماتي عن طريق إسم المجلد أو إسم الملف أو إسم الإمتداد أو محاولة هيكلة أساليب التنقيش بشكل مسبق، فهذه العملية يجب أن تظل ديناميكية... و من غير المعقول أن يحاول إذن التنقيش تقييد آليات التنقيش بفرض مثل هذه الحدود التي من شأنها أن تقيّد أهداف التنقيش المشروعة بدون مبرر، فلا يتوقع المرء أن يكون هناك إذن يضيق عملية البحث بالتنقيش عن الأدلة فقط ضمن 'خزانات ملفات في الطابق السفلي' أو 'ملف المجلدات المسماة العملاء'، لذلك لا يوجد سبب للحد من نطاق عمليات التنقيش المعلوماتي"⁽²⁾، و أصرت على موقفها هذا مجدداً في حكم حديث لها في قضية **United States v. Russian**⁽¹⁾.

(¹) United States v. Hill, 459 F.3d 966, 977 (9th Cir.2006).

تتلخص وقائع القضية في كون المتهّم وضع حاسوبه لإصلاحه لتكتشف الخبيرة أنّه يحتوى على صور داعرة للقصر على إثرها تمّ تبليغ الشرطة التي حصلت على إذن بتفتيش المحل و ضبط الحاسوب، و جميع وسائط التخزين الخاصة بالحاسوب، و جميع الصور الداعرة المخزنة. بحلول الوقت الذي وصل فيه الضابط إلى المحل لتنفيذ إذن الضبط، كان المتهّم قد استرجع حاسوبه، ليتمّ الحصول على إذن ثان استهدف منزل المتهّم، و إذن بمصادرة نفس الأشياء و أثناء تنفيذ عملية التنقيش لم يتم العثور على الحاسوب و بدلا من ذلك تمّ العثور بغرفة النوم على وسائط تخزين المتمثلة في عدد كبير من الأقراص المضغوطة و الأقراص المرنة، إثنان من الأقراص المضغوطة تمّ تحديدهما في النهاية لاحتوائهما صور فوتوغرافية إباحية للأطفال؛ أين طالب المتهّم ببطلان الأدلة لأنّ الإذن كان واسعاً بإجازة ضبط جميع وسائط تخزين الحاسوب المكتشفة بغض النظر عما إذا كانت تحتوي على صور إباحية للأطفال، و لعدم وضع قيود على عملية التنقيش المعلوماتي للمضبوطات أين رفضت محكمة المقاطعة هذا الطلب و تمّ تأييده من قبل جهة الاستئناف.

(²) United States v. Burgess, 576 F.3d 1078, 1093 (10th Cir. 2009).

تتعلق وقائع القضية بصور الإذن بالتنقيش المعلوماتي استهدف حاسوبا محمولا و محركين للأقراص الصلبة الخارجية بحثا عن صور للمتورطين في الجريمة و صوراً للمواد المخدرة غير المشروعة، غير أنّ التنقيش اللاحق أفضى إلى الكشف عن صورة داعرة للقصر، و بناء على ذلك طالب المتهّم ببطلان هذه الأدلة للتوسّع في التنقيش خروجاً عن

و نظراً للصعوبات العملية الملازمة لتطبيق منهجيات التفتيش الشامل، تجنبت الدائرة السادسة التمسك ببروتوكولات التفتيش و فضلت تقدير مدى مشروعية إمتداد التفتيش في كل حالة على حدى، إلا أنها إشتطت أن يكون الضباط واضحين بشأن ما يبحثون عنه على وسائل التخزين الرقمية و إجراء التفتيش بطريقة تتجنب البحث عن ملفات من نوعية غير محدّدة في الإذن، ففي نظرها فإنّ عملية التفتيش قد تكون واسعة النطاق بشكل معقول لتحديد العناصر الموضحة في الإذن، و أنّه إن كان الإلتزام بالشرعية الإجرائية يتطلّب عند تنفيذ التفتيش الإطلاع أولاً على الأماكن الأكثر وضوحاً ثمّ الإنتقال تدريجياً من الواضح إلى الغامض كلما دعت الضرورة إلى ذلك و تلك هي الغاية من فرض بروتوكول التفتيش الذي يبني عملية البحث عن طريق المطالبة بتحليل بنية الملف، ثمّ البحث عن مجلدات الملفات المشبوهة، ثمّ البحث عن الملفات و أنواع الملفات التي من المحتمل أن تحتوي على المواد المستهدفة عن طريق إجراء عمليات البحث عن الكلمات الرئيسية، و لكن في النهاية، قد لا يكون هناك بديل عملي للتفتيش الفعلي في العديد من المجلدات (و ربما جميعها) و في بعض الأحيان في المستندات الموجودة داخل هذه المجلدات⁽²⁾.

و من أهمّ الاعتراضات التي يسوّقها المناهضون لهذا القيد، أنّه لا يمكن تحديد محتويات أيّ مستند حاسوبي إلاّ من خلال فتحه و فحصه باستعراض ما تضمّنه، و قد تأكّد هذا التّطبيق في قضية **United States v. Gray**، أين رفضت المحكمة طلب بطلان التفتيش الذي كان أكثر امتداداً عبر ملفات لا صلة لها بالتحقيق رغم أنّ الفحص تمّ باستعمال برنامج حاسوبي يضمن قصر التفتيش على الملف المستهدف، و أشارت المحكمة إلى أنّه بالرغم من

نطاق الإذن القضائي نتيجة لعدم الإلتزام بقاعدة بروتوكول التفتيش و قد تصدّت الدائرة العاشرة لطلبه بالرّفص موضحة أنّ هذه المحكمة لم تطالب نهائياً لزوم أن تتضمّن أذون التفتيش استراتيجية تفتيش دقيقة قد يكون التفتيش المعلوماتي واسعاً بقدر ما هو مطلوب بشكل معقول لتحديد العناصر الموضحة في إذن الضبط بناء على السبب المحتمل و لم يقيد إذن التفتيش بناء على إسم إمتداد الملف أو أسماء الملفات أو هيكلّة الدليل، بدلاً من ذلك تم تقييد نطاق التفتيش بشكل واضح من خلال قصر البحث عن الملفات الحاسوبية التي تشكّل دليلاً عن تعاطي المخدرات أو الإتجار بها و هذه الملفات يمكن أن تتخذ أشكالاً عديدة. قد تكون عبارة عن ملفات نصية عامة، مستندات معالجة النصوص، برامج معالجة النصوص، ملفات برنامج البريد الإلكتروني، جداول بيانات أو قاعدة بيانات .

(1)United States v. Russian, No. 17-3157 (10th Cir. 2018).

(2)United States v. Richards, 659 F.3d 527 (6th Cir. 2011).

وجوب توخي الحذر لضمان عدم التوسّع الكبير في التفتيش المعلوماتي، فإنّ هذه العملية لا تقلّ دستورية عن عمليات التفتيش في السجلات الماديّة، حيث قد يتمّ فحص المستندات غير الضارة للتأكد من أهميتها، فعند البحث عن العناصر المدرجة في الإذن يجوز فحص جميع ملفات المتهم لتحديد ما إذا كانت تحتوي على عناصر تدخل في نطاق الإذن⁽¹⁾.

و استندت المحكمة إلى السابفة القضائية التي تقررت في قضية **United States v. Hunter**، و التي مقتضاها أنّ عمليات التفتيش في السجلات تتطلب البحث في كثير من المستندات، و عادة ما تكون جميعها في الموقع المستهدف، لأنّ "قلة من الأشخاص يحتفظون بمستندات معاملاتهم الإجرامية في مجلد يحمل عنوان "سجلات الجريمة".

و في تأييدها لهذا الوقف المتساهل عبّرت الدائرة العاشرة عن موقفها من عدم جدوى منهجية التفتيش صراحة في قضية **United States v. Burgess** قائلة: "بشكل عام قد لا يمنح بروتوكول التفتيش سوى وهما لحماية الحق في الخصوصية، خاصةً عندما يكون هدف التفتيش هو ملفات الصّور، ففي الحالة التي يكشف التفتيش المعلوماتي-الذي يستهدف أصلاً التتّيب عن أدلة متعلّقة بجريمة المخدرات- عن أسماء ملفات تشير إلى مواد إباحية للقصر، لا يُطلب من الضابطين سوى الحصول على إذن آخر لمتابعة التفتيش عنها، مما يؤدي إلى استعراض أغلب الملفات للتأكد من أنّها لا تحمل عنواناً مظلّلاً. و في النهاية سيتمّ الكشف

(¹) *United States v. Gray*, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999).

في هذه القضية صدر إذن بالتفتيش بحثاً عن أدلة بخصوص جرمي الدخول غير المصرّح به لنظام معلوماتي حكومي و جريمة التّسبب في إتلاف بيانات تابعة للمكتبة الوطنية للطّب، و تنفيذاً للإذن تمّ ضبط أربعة حواسيب خاصة بالمتهم و نسخ محتوياتها على أقراص مغناطيسية، باستخدام برنامج CompuPic يظهر صور مصغرة الحجم لجميع العناصر الموجودة في الملف أو الصّور أو المستندات النصّية على الشّاشة. مكّن هذا البرنامج عند فتح الملف تبين رؤية طبيعة المواد الموجودة داخله أي تمّ اكتشاف مجلد بعنوان bbs يحتوي على صور داعرة للبالغين و بداخله مجلد فرعي تبين أنّه يحتوي على صور فاحشة للقصر، تمّ التوقف فوراً عن التفتيش و استصدار إذن مستقل بشأنها على إثرها تمّت متابعة المتهم بهذه الجريمة الثالثة 'حيازة صورة داعرة للأطفال' و قد طالب المتهم ببطلان هذا الدليل المعلوماتي إستناداً إلى عدم مشروعية التّوسع في التفتيش الذي تجاوز نطاق الإذن القضائي، لعدم التّقيّد بالبرنامج الحاسوبي المستعمل في عملية النّسخ و التفتيش و بعدما استيقنت المحكمة فعلاً من صحة إدعاء المتهم بناء على تقرير الخبير بأنّه بالفعل كان بالمكان تعديل البرنامج أو تكميله بطريقة تجعل من الممكن تحديد ما إذا كان ملفاً معيّناً يتكون من صور أو نص دون عرض محتوياته رفضت المحكمة طلب بطلان الدليل للعلل المشار إليها في المتن.

عن المواد الإباحية، فالفرق الوحيد هو أنه سيتم اكتشافها لاحقاً، و ليس في وقت سابق... خاصة في حالة التفتيش عن ملفات الصور، و التي يمكن دفنها في أي مكان على وسيط التخزين⁽¹⁾.

و على هذا الاعتراض يردّ المؤيدون بأنّ هذا التوجه القضائي يعبر عن فهم خاطئ للغرض الذي لأجله تصمّم بروتوكولات التفتيش و ما تقضي إليه من فوائد، إذ أنّ منهجية التفتيش لا تحدّد المعلومات التي يحتويها المستند و ليس ذلك هو الهدف من فرضها، فهي ببساطة أساليب ترمي إلى إستبعاد المعلومات التي لا صلة لها بالتحقيق من نطاق التفتيش، فعلى سبيل المثال، إذا حدّدت الضبطية القضائية سبباً محتملاً للإعتقاد بأنّ حاسوب شخص معين يحتوي على صور سرقة حدثت بتاريخ ما، فقد تستخدم المحكمة البيانات الوصفية لوضع بروتوكول تفتيش يحدّ من نطاق التفتيش بقصره على المستندات التي تمّ إنشاؤها بعد تاريخ وقوع الجريمة، فلا يمتدّ التفتيش إلى غيرها من البيانات⁽²⁾.

فالغاية من هذا القيد هو منع إمتداد التفتيش إلى بيانات غير ذات صلة بمستهدف التفتيش عن طريق عزلها عما تختلط به من بيانات مجرّمة تشكّل موضوعاً للدليل الجنائي و هو ما يطلق عليه الفقه بإجراء تقليل البيانات "data reduction" و يتمّ ذلك عن طريق برامج التحليل الحاسوبي الشرعي التي أثبتت فاعليتها في هذا الصدد، فعلى سبيل المثال في قضية **United States v. Mann** صدر إذن بالتفتيش المعلوماتي لأجهزة التخزين الرقمية الخاصة بالمتهم المتابع بجرم إنتقاط صور لبعض الفتيات دون رضاهن و في أماكن تتميز بكثير من الخصوصية، أين قام خبير التحليل الحاسوبي الشرعي باستخدام برنامج يستهدف البحث و التنقيب عن الصور و مقاطع الفيديو فقط مع عزل باقي البيانات من الاستعراض و بالفعل تمّ التوصل إلى استرداد الدليل دون امتداد التفتيش إلى بيانات غير ذات صلة⁽³⁾، فطبيعة الجريمة و نوع الأدلة تحدّد كيفية تحليل البيانات على نحو يحول دون امتداد التفتيش و ذلك في كثير من الأحيان.

(¹) United States v. Burgess, 576 F.3d 1078 (10th Cir. 2009).

(²) Derek Haynes , op, cit, p 774.

(³) United States v. Mann, 592 F.3d 779 (7th Cir. 2010).

كما يرى القاضي **John M. Facciola** أنّ هذه القيود لا تشكل نهائياً إعاقة غير مبررة للكشف عن الجريمة أو الحد من قدرة الحكومة على إجراء تفتيش بشكل ديناميكي لسببين، أولاً، تستطيع الحكومة دائماً الرجوع إلى المحكمة لتقديم طلب آخر للحصول على إذن إضافي حسب ما تستدعيه الحاجة و ثانياً، لا يقتضي الطلب سوى توضيح أنّ بعض عمليات التفتيش تتطلب تقنيات إضافية، و أنّ ما هو مقترح هو مجرد ما تعتمزم الحكومة القيام به وقت تقديم هذا الطلب، إستناداً إلى المعرفة التي إكتسبتها أثناء تفتيش هذه الأجهزة، و في ضوء البيانات المحددة التي تسعى إلى ضبطها⁽¹⁾.

و ذات التبرير إعتدده زميله **David Waxse** مضيفاً أنّه سعياً لتحقيق توازن بين حق الفرد في الخصوصية و قدرة الحكومة على التحقيق في الجرائم بفعالية و كفاءة فإنّه بالإمكان دائماً الحصول على إذن إضافي بناء على عرض لاحق تتقدّم به هذه الأخيرة و تبين من خلاله ما يستدعي ذلك، أفضل من الموافقة على الطلب الأول الذي يمنح الحكومة سلطة غير دستورية واسعة النطاق في إجراء التفتيش.

(ج) - نقص خبرة القضاة في فرض إستراتيجية التفتيش

و لعلّ أهمّ اعتراض وجه لهذه القاعدة من قبل الفقه، هو نقص الخبرة الفنيّة لدى القضاة في فرض منهجية تفتيش معيّنة، إذ تعتمد القدرة على صياغة إستراتيجية تفتيش مفيدة و الموافقة عليها على الخبرة التقنيّة لقضاة التحقيق، غير أنّ هؤلاء غير مؤهلين بشكل كاف لتقييم ما إذا كان بروتوكول تفتيش معيّن هو أفضل الطّرق و أكثرها إستهدافاً لتحديد مكان الأدلة المخزّنة على أجهزة التخزين الرّقمية أم لا، فليس لهؤلاء سوى دراية محدودة و تغيب عنهم معرفة التفاصيل الدقيقة لعمل الحواسيب، كما تتوقف القدرة على وضع بروتوكول معيّن على العديد من العوامل التي يصعب تحديدها مسبقاً فحتّى خبراء التحليل الحاسوبي الشرعي الأكثر كفاءة و مهارة لا يمكنهم التنبؤ مسبقاً بالتقنيات المستوجبة للعثور على البيانات المحددة في الإذن القضائي⁽²⁾.

(1) United States v. Apple iPhone, IMEI 013888003738427, Criminal No. 2014-0278 (D.D.C. 2014).

(2) Orin S. Kerr, Searches and Seizures in a Digital World, op, cit, p 49.

و بناء عليه يستعصى عليهم أن يحدّدوا مسبقا ما سيواجهونه من تعقيدات تفرزها طبيعة البرمجيات الموجودة بجهاز التخزين الرقمي، أو الخطوات التي إتخذها المشتبه فيه لحماية أو إخفاء الملفات فهذه العملية هي فن أكثر من علم " as much an art as a science" و أمام هذا الوضع فقد يتمّ تمكين القضاة من بروتوكولات تفتيش محدّدة و هذه الأخيرة إمّا أن يكون قد عفا عليها الزمن أو أنّها تعرقل عمل الجهة القائمة بالتفتيش على التّكيف مع المتغيّرات⁽¹⁾.

و هذا التّقدّ الفقهي وجد صداه لدى القضاء الذي إعتمده كمبرر لرفض طلبات بطلان الدليل الجنائي الناتج عن التفتيش المعلوماتي الذي تمّ بدون فرض قيود مسبقة إمّا تأسيسا على إنعدام الخبرة لدى الضّبطية القضائية التي التمسّت الموافقة على إذن التفتيش المعلوماتي⁽²⁾ أو القاضي مصدر الإذن⁽³⁾.

يرى المؤيّدون، أنّ هذه الإنتقادات المعبرّ عنها منذ عقد مضى بدأت تتراجع أهمّيّتها مع مرور الوقت، ببروز قضاة قادرين على التّعامل مع بروتوكولات تفتيش الأكثر تعقيدا، و يضرب الفقه عديدا من الأمثلة عن المحاكم التي كشف عن دراية كافية بعلم الحاسوب تؤهلها للوقوف على التّقدير السليم لبروتوكولات التفتيش التي تعرض عليها و تعدّ المحكمة الإبتدائية لمنطقة كولومبيا القضائية برئاسة القاضي جون فاسيولا أبرز مثال على ذلك.

ففي قضية **United States v Milzman** طلب هذا الأخير من الحكومة وجوب تقديم بروتوكول لتفتيش عدة أجهزة إلكترونية و هاتف محمول غير أنّ الحكومة كانت متردّدة في الإستجابة لطلبه خشية عدم تمكنه من استيعاب المسائل التّقنية التي تتضمنها الإستراتيجية المقترحة، فكان ردها بشكل موجز بموجب إفادة خطية بسيطة تفيد بأنّ أحد خبراء الحاسوب هو من سيتولى نسخ البيانات و تحليلها، أين تصدّت المحكمة للطلب بالرّفض مرة أخرى موضّحة أنّه "يجب على الحكومة أن تبيّن للمحكمة ما تعترزم القيام به في كلّ تفتيش تجريه على الهاتف و لا ينبغي لها أن تخشى إستخدام مصطلحات مثل "قيم التّجزئة MD5"، و "البيانات الوصفية"، و "التسجيل"، و "حجب الكتابة"، كما لا ينبغي لها أن تمتنع عن تفسير

(1) Christina M. Schuck, op, cit, pp 775-776.

(2) Commonwealth v. McDermott, 448 Mass. 750, 776 (2007).

(3) United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999).

أنواع البرامج المستعملة و كيفية استخدامها للتفتيش عن أنواع معينة من البيانات و لا تشترط المحكمة استخدام مصطلحات أو أساليب بحث معينة و بدلا من ذلك، فإن المحكمة تريد موافقاتها بشرح و تفسير فني متطور للكيفية التي تعتمزم بها الحكومة إجراء التفتيش حتى تستيقن من كون الحكومة تبذل جهودا حقيقية للحد من نطاق عملية التفتيش المعلوماتي⁽¹⁾ و قد كشفت أحكام عديدة صادرة عن المحاكم الابتدائية مظاهر الدلالة على عدم صحة هذه الحجة التي يتمسك بها المناهضون لهذا القيد الإجرائي.

و خلافا لما يعتقد جانب من الفقه و القضاء، غالبًا ما يتمكن القضاة من إدراك منهجية التفتيش المعلوماتي، ففي معظم الحالات لا تكون التقنية المعتمدة معقدة بشكل خاص، و يمكن للخبراء تقديم التفسيرات الكافية للقضاة لفهمها⁽²⁾، و الجدير بالذكر أنه في بعض الحالات أبان القضاة براعة فائقة في هذا المجال، ففي إحدى القضايا تقدمت الحكومة بطلب الموافقة على إذن بالتفتيش المعلوماتي يستهدف أجهزة تخزين رقمية، رفض قاضي التحقيق الطلب لعدم تقديم بروتوكول يرسم نطاق التفتيش محددًا أجلًا لاستدراك ذلك و أثناء 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 أن هذا القيد لن يكون مفيدا لأن دليل الملفات لا يبين إلا تاريخ آخر مرة تمّ 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 تمّ فيه حفظ الوثيقة، بل تظهر أيضا كيف و متى تمّ إستلامها، أو إنشاؤها، أو الوصول إليها، أو تعديلها، و لم يقدم الخبير التقني الحكومي أي رد، تاركا للمحكمة إنطبعا راسخا بأنه لم يكن على دراية بمصطلح يتوقع أن يعرفه خبير في مجال الحاسوب⁽³⁾.

علاوة على ذلك، يمكن للقضاة الذين يفتقرون إلى المعرفة الضرورية المطالبة من الضبطية القضائية أو النيابة العامة تقديم بروتوكولات تفتيش مقترحة، كما يمكن لوزارة العدل

(¹) United States v. in the Matter of the Search Associated With Rwgann, Criminal No. 2014-0228 (D.D.C. 2014).

(²) Christina M. Schuck, op cit, p 777.

(³) In Re Search of 3817 W. West End, First Floor Chicago, Ill. 60621, 321 F. Supp. 2d 953 (N.D. Ill. 2004)

التّوصل إلى بعض البرتوكولات التّموجية لوجود موارد بشرية مؤهلة لذلك⁽¹⁾، و قد درج القضاة على اللّجوء إلى هذا الحل⁽²⁾.

و رغم مرور ما يقارب عشرة سنوات على صدور الإجتهاد القضائي لا يزال القضاء الأمريكي يبدي تردّدا ملحوظا حيال الإلتزام بهذه القاعدة و هو ما تكشف عنه أحدث الأحكام القضائية التي واصلت تخليها عن القاعدة و توسّعت في إضفاء المشروعية على امتداد التّفتيش المعلوماتي الذي لا يستند إلى بروتوكول مسبق مدفوعا باعتبارات عملية بحتة بحيث مالت كفة التّرجيح لاعتبارات الفعالية و قد تأثرت هذه الأحكام القضائية بالإنقادات الموجهة للقاعدة.

الفرع الثالث: بدائل قاعدة لزوم تحديد أسلوب تنفيذ التفتيش المعلوماتي

في ضوء النّقد الموجّه للقاعدة، خاصة النّقد المبني على مناقضتها لمتطلبات الفعالية و احتمال ضياع الأدلة المعلوماتية جراء شلل عملية التّفتيش بحكم القيود الضيقة التي تفرض عليها، نادى الكثير من الفقه بعدم التّوسّع في تطبيقها مع الإكتفاء بالمراجعة القضائية اللاحقة لكلّ قضية على حدى لتقدير مدى معقولية تنفيذ التّفتيش في نطاق الغاية منه، و أهمّ البدائل المقترحة لحد الآن من قبل الفقه هو النّهج القائم على وضع حد لامتداد التّفتيش المعلوماتي من خلال حظر استخدام أيّ دليل جنائي يكتشف خارج نطاق الإذن القضائي.

و في نظر هذا الجانب من الفقه فإنّ هذه المقاربة من شأنها استعادة الحدود المطلوبة على نطاق الضّبط بما يحافظ على فعالية عمليات التّفتيش من خلال تزويد الحكومة بالسلطة اللّازمة للتّفتيش عن الأدلة المحدّدة في الإذن القضائي و ضبطها و يؤدي بذات الوقت إلى تجنب صيرورة الإذن بالتّفتيش عاما، بتقييد سلطة الحكومة في إستغلال الأدلة المحدّدة في الإذن القضائي بشكل خاص⁽³⁾. و تقوم هذه المقاربة على ثلاثة أسئلة رئيسية: أولا، خلال مرحلة التّفتيش المادي، ما هي حدود سلطة الضّبطية القضائية في ضبط أجهزة التخزين الماديّة لتفتيشها لاحقا؟ ثانيا، أثناء مرحلة التّفتيش المعلوماتي، ما هي حدود سلطة الضّبطية

(1) Paul Ohm, op cit, p 12.

(2) Adam M. Gershowitz, op,cit , p 625.

(3) Kerr,Orin S ,Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data , op cit , p 4.

القضائية في تحليل البيانات المخزنة للوصول إلى الأدلة المطلوبة؟ ثالثاً، بعد مرحلة التفتيش المعلوماتي ما هي حدود سلطة الضبطية القضائية في استخدام المعلومات المكتشفة أثناء مرحلة التفتيش المعلوماتي؟⁽¹⁾.

بخصوص مرحلة التفتيش المادي يرى هذا الجانب من الفقه، أنّ كل من القانون و القضاء يسلّمان في الوقت الرّاهن بضرورة الضّبط العرضي الشّامل يليه إجراء التفتيش المعلوماتي لاحقاً لأنّ وسائط التّخزين الإلكترونيّة تحتوي على كمّيات كبيرة من المعلومات التي غالباً ما يكون من غير العملي مراجعتها في الموقع لذا ينبغي عدم فرض أيّ قيود على هذه المرحلة رغم الإقرار بتجاوز الضّبط لحدود الإذن نظراً لعدم وجود أيّ بديل آخر⁽²⁾، و الأمر كذلك بالنّسبة لمرحلة التفتيش المعلوماتي ينبغي تركها من غير قيد لعدم جدوى قاعدة لزوم تحديد محل التفتيش في تضيق نطاقه و لعدم دستورية قاعدة تحديد منهجية تنفيذه⁽³⁾.

أمّا المرحلة الأخيرة، و هي مرحلة استخدام الأدلة ، خلالها يتمّ فرض قيود تمنع استخدام أيّ دليل جنائي خارج نطاق الإذن القضائي لكون الضّبط الإجمالي في المرحلة الأولى هو ضبط معقول و مبرّر بضرورة تنفيذ الإذن القضائي، كما أنّ ضرورة التّحقيق تستوجب الإطلاع حتماً على الملفات البريئة في سياق التفتيش عن البيانات المستهدفة، بما يجعل الضّبط الأولي و الإطلاع اللاحق ضروري لتجنّب جعل الإذن مجرد حبر على ورق، بيد أنّ الضّبط المتواصل للبيانات التي لا تستجيب للإذن القضائي أو استخدامها لإثبات جرائم غير تلك التي إستهدفت بإذن التفتيش يجعل الإذن عاماً و يلغي تماماً دور قاعدة لزوم تحديد مستهدف التفتيش⁽⁴⁾.

و قد تمّ تبني هذه المقاربة الفقهية مؤخراً من قبل المحكمة العليا في أوريغون و ذلك في قضية **United States v. Mansor**، حيث أشارت المحكمة إلى أنّ هذا المذهب يشكّل قاعدة من قواعد قبول الأدلة المعلوماتية فبينما تسمح هذه القاعدة للحكومة بإجراء تفتيش معلوماتي واسع النطاق، فإنّها في نفس الوقت تحدّد من مقبولية الأدلة المتأّتية من هذا الإجراء بحيث

(1) Ibid , p 6.

(2) Ibid , p 11.

(3) Ibid , pp 13-14.

(4) Ibid , pp 25-27.

تستبعد الأدلة التي لا علاقة لها بالأسباب المحتملة التي من أجلها صدر إذن التفتيش⁽¹⁾، و التكريس القضائي لهذه القاعدة يرجع إلى سابقة الدائرة الفيدرالية الثانية في قضية **United States v. Ganius** و التي أقرت مظهرا جديدا من مظاهر تطبيق قاعدة استبعاد الأدلة المعلوماتية غير المشروعية⁽²⁾.

الواقع أنّ هذا البديل المقترح لا يتعلّق أصلا بالهدف الوقائي الذي تتوخاه القاعدتين محل البحث بل يرمي إلى التخفيف من الضرر اللاحق بالفرد جراء تفتيش معلوماتي يتجاوز الغاية منه باستبعاد أيّ دليل جنائي لا يستهدفه التفتيش، و من جهة أخرى فإنّ ترك مرحلتي التفتيش المادي و المعلوماتي من غير قيد و إتاحة سلطة واسعة للضبطية القضائية بهذا الشكل هو أمر غير معقول تماما بل يناقض مقتضيات التعديل الدستوري الرابع و يؤدي إلى إهدار كافة الضمانات التي تقوم عليها نظرية التفتيش.

و ما نخلص إليه في النهاية أنّه و إلى غاية الوقت الراهن لا يوجد أيّ اقتراح فقهي أو إجتهد قضائي نجح في إرساء قاعدة عامة -قابلة للتطبيق في كافة الظروف و الوقائع- 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 التفتيش المعلوماتي تحقّق الشرعية، و بذات الوقت تفضي إلى شلل عملية التفتيش لأنّه لا يمكن التنبؤ مسبقا بمكان تواجد الأدلة المعلوماتية قبل إجرائه بما يوجب الإطلاع على أسرار الأفراد قبل التوصل إلى الدليل المستهدف.

و من ناحية أخرى، فإنّ التطبيق الصّارم لقاعدة لزوم تحديد منهجية تنفيذ تفتيش هي الأخرى تفرض حدودا ضيقة على عملية تنفيذ التفتيش خاصة إذا اقتصرّت المنهجية على أسلوب واحد فقط، على نحو يناقض متطلبات الفعالية نتيجة لجوء المجرمين إلى إخفاء الملفات المجرّمة في أيّ مكان على وسيط التخزين الرقمي، مع جعل الملف الخارجة عن نطاق الإذن القضائي حجابا للملف المجرّم او السمتهدف بالتفتيش بإعطاء الملفات إسماء مضلّلا أو امتدادا خاطئا أو حمايتها بواسطة طرق التشفير، و هذا الذي دفع بالقضاء إلى التردّد في تطبيقها، فضلا على ذلك فإنّ المغالاة في الدفاع عن هذه القاعدة بتطبيقها الجامد،

(1) State v. Mansor, 421 P.3d 323 (Ore. 2018).

(2) United States v. Ganius, 755 F. 3d 125, 134 (2d Cir. 2014).

يجافي المنطق إذ كشفت الواقع العملي أنها جدّ مرهقة و تتطلّب وقتاً طويلاً نتيجة المطالبة بأدوات تفتيش جديدة في كل مرة تفشل فيها المنهجية المقترحة في إسترداد الدليل المستهدف.

في تقديرنا فإنّ القضاء الأمريكي قد خطى بمقتضى هذا الإجتهااد القضائي خطوات أخرى في اتجاه التّضييق من نطاق إمتداد التّفتيش المعلوماتي، و أهمّ ما يجعلنا نوّيد هذه القاعدة هو المفهوم الجديد الذي أصبغه القضاء على "مبدأ عدم تجاوز الغاية من التّفتيش".

فبعد أن كان هذا المبدأ من الضّمّانات الموضوعية للتّفتيش وفق منطق النظرية التقليدية للتّفتيش و من ثم يخضع للمراجعة القضائية اللاحقة بعد تنفيذ إذن التّفتيش، إنتفت القضاء الأمريكي إلى مسألة جوهرية تتعلّق أساساً بالتّداويات السّلبية التي يخلفها التّفتيش المخالف لهذا المبدأ على الهيئة الإجتماعية، و ليس فقط على المتهم و هي الضّرورة التي حذت به إلى إعتباره أيضاً من الضّمّانات الشّكلية التي تحقّق الدّور اللقائى الذي ينصرف إليه التّعديل الدّستوري الرّابع، من خلال فرض مجموعة من القيود ضمن إذن التّفتيش تضمّن تنفيذ الإذن في حدود الغاية منه، بحيث يترتب على مخالفتها البطلان.

و مثل هذه المتطلبات تجعل محضر التفتيش - الذي يضم بطبيعة الحال محضر الضبط الأولي - يأخذ حكم الخبرة التقنية، من حيث إحتوائه على كافة التفاصيل التقنية الدقيقة لعملية النسخ الرقمي و التحليل و المراجعة و الحفظ.

إذ يجب أن يتضمن محضر التفتيش بيانات شكلية يغلب عليها الطابع التقني بحيث يحدد وباستفاضة كافة الخطوات التي اتخذتها الجهة القضائية بتنفيذ التفتيش سواء الطبعية القضائية أو الخبير التقني المنتدب بداية من تاريخ تنفيذ الإذن في مرحلة التفتيش المادي مروراً بمرحلة الضبط الرقمي العرضي ثم مرحلة التفتيش المعلوماتي، و أيضاً عمليات الضبط النهائي للدليل إن وجد.

و تعتبر هذه الضمانة بمثابة خط دفاع لحماية حق الأفراد في الخصوصية لأنها تمكن الجهات القضائية من مراقبة مدى احترام القائم بالتنفيذ لتلك الاستراتيجيات او المنهجية المحددة في الإذن القضائي منعا من التفتيش الشامل او الموسع الذي لا تبرره تعقيدات فنية، لانه لا يمكن التعميم بأنه يستحيل اجراء تفتيش ضيق في بعض الأحوال و قد أشار إلى ذلك القضاء الأمريكي في عديد قراراته.

و اذا كان المشرع الجزائري لم يتعرض نهائيا لهذا الضباط طالما أنه لم يشترط الإذن القضائي في التفتيش المعلوماتي استنادا الى ما توصلنا اليه سابقا، فإنه أن الأوان لاستدراك هذا القصور التشريعي من خلال تبني ما تواتر عليه الإجتهد القضائي المقارن بهذا الخصوص.

خلاصة الباب الأول

لقد عالجتنا من خلال الباب الأول أهم الاشكاليات العملية التي تثيرها عملية التفتيش عن الادلة المعلوماتية فالرؤية الجديدة التي أخرجت الأدلة المعلوماتية المستمدة من التفتيش من النظرة الإستثنائية المتواضعة لتضعها في منطق الأصالة كأدلة كاملة في إطار مبدأ حرية الإثبات الجنائي، أفضت إلى طرح سؤال فرض نفسه على دراسات القانون الجنائي، يتناول موضوعه البحث في مدى إمكانية تجاوب الأحكام الإجرائية للتفتيش عن الأدلة المادية مع البيئة الرقمية دون تجاوز الضوابط التي يفرضها مبدأ الشرعية الإجرائية.

و التجاوب مع هذا التساؤل دفعنا إلى تأصيل فكرة التفتيش المعلوماتي من خلال الفصل الأول اين قمنا بتحديد مدلول التفتيش في البيئة الرقمية، و متى يقع بالضبط، ثم تطرقنا إلى تحديد معيار التمييز بينه و بين الضبط الرقمي، بحكم أنّ كليهما يقيد حق من الحقوق الشخصية ثم عالجتنا خصائص التفتيش المعلوماتي و ما يميزه عن التفتيش المادي كل ذلك من خلال المبحث الأول، و من خلال المبحث الثاني تناولنا مقدمات التفتيش عن الأدلة المعلوماتية اذ ينبغي التفتيش عن الأجهزة المادية قبل تفتيشها، و هو ما يسمى بالضبط العرضي سواء انصب الضبط على البيانات التي يحوزها المتهم أو تلك المتعلقة به و التي يحتفظ بها مزود الخدمات في اطار اداء الخدمة، و هو ما يعرف بالية الأمر بالحفظ و الأمر بالافصاح.

و اذ انتهينا من مقدمات التفتيش فقد كام لزاما علينا أن نحدد ضوابط هذا العمل الاجرائي الخطير من خلال الفصل الثاني، أين خصصنا المبحث الاول لدراسة الضوابط الموضوعية، و المتمثلة في سبب التفتيش المعلوماتي، و المحل الذي يجري تفتيشه في البيئة الرقمية و كيفية تحديده لانعدام الحدود و الحواجز المادية كل ذلك في ضوء السوابق القضائية للاجتهد المقارن. بينما خصصنا المبحث الثاني لمعالجة الضوابط الشكلية بالتطرق الى الاذن القضائي و اشكالية تحديد المستهدف بالتفتيش اثناء صياغة هذا الإذن، و ايضا اشكالية تحديد اسلوب تنفيذ التفتيش و تلك مسائل بالغة الاهمية باعتبارها ضمانات جوهرية و سياجا لحماية الحريات الفردية.

الباب الثاني
حجية الأدلة المعلوماتية
المستمدة من التفتيش

إذا كنا قد فرغنا من تحديد فكرة الشريعة الإجرائية للأدلة المعلوماتية في مرحلة التفتيش، فإن منطق الصراع بين التفتيش و مدى مشروعيته يظل قائما أمام محكمة الموضوع، فكيف يمكن لهذه الأخيرة أن تقدر مدى مراعاة قاعدة المشروعية باعتبار أن كافة ضمانات التفتيش ذات بعد تقني محض؟ فإن عجزت عن ذلك، فكيف لها أن تقدر القيمة الإقناعية للأدلة المعلوماتية المستمدة منه؟ أم أن الخبير في الحقيقة هو قاضي الدعوى؟ و أبعد من ذلك، أي قيمة تتمتع بها قاعدة الشريعة الإجرائية إذ لم يتقرر البطلان جزاء مخالفتها؟ أم يمكن فعلا للجزاء الفردية الموقعة على مرتكب التفتيش غير المشروع أن تحل محل قاعدة استبعاد الأدلة المعلوماتية المتسمة من تفتيش غير مشروع؟

إن هذه التساؤلات تحمل في طياتها مغزى مبناه أنه لا جدوى من الشريعة الإجرائية إذا لم تؤدي إلى الحقيقة الواقعية من خلال دليل يحقق اليقين القضائي، و لا قيمة لهذه الحقيقة على حساب الشريعة و لو تحقق اليقين بالإدانة، في ضوء هذه الفكرة يقع لزاما علينا أن نحدد القيمة الإقناعية للدليل المعلوماتي المستمد من تفتيش مشروع (فصل أول)، و بيان قيمته القانونية متى كان محصلة لتفتيش باطل (فصل ثاني).

الفصل الأول

القيمة الإثباتية للأدلة المعلوماتية المستمدة من تفتيش مشروع

المبدأ في الإثبات في المواد الجنائية هو حرية القاضي الجنائي في الإثبات و هذه الحرية لها وجهان وفق ما استقر عليه الفقه، أولهما أنّ للقاضي الجنائي سلطة قبول أيّ دليل يمكن أن يوفر له العقديّة و الإقتناع، ذلك أنّ جميع طرق الإثبات أمام القاضي الجنائي سواء، و ثانيهما أنّ القاضي ذاته هو الذي يقدّر بحسب اقتناعه الشخصي القيمة الدامغة أو القيمة الإقناعية لكلّ دليل، و مفاد ذلك أن الشقّ الأول من المبدأ العتيد يتعلّق بسلطة القاضي في قبول الدليل المعلوماتي المستمدّ من التفتيش (مبحث أول)، بينما يتعلّق الشقّ الثاني بسلطة القاضي في تقديره (مبحث ثاني).

المبحث الأول

حرية القاضي الجنائي في قبول الدليل المعلوماتي المستمد من التفتيش

إنطلاقاً من مبدأ حرية الإثبات الجنائي، فإنه يمكن القول أنّ جميع طرق الإثبات مقبولة أمام القاضي الجنائي، لكن هذه القاعدة ليست على إطلاقها فلها نطاق يحددها، كما أنها خاضعة لقيود هامّة هي مشروعية الأدلة، إذ يلزم لقبول الدليل أن يكون التفتيش عنه قد تمّ في ظلّ احترام هذا المبدأ، من هنا فإنّ مبدأ حرية الإثبات الجنائي في قبول هذا الدليل (مطلب أول)، محكوم إلى حد ما بمبدأ مشروعية هذا الدليل و نزاهته (مطلب ثاني).

المطلب الأول: ماهية حرية القاضي الجنائي في قبول الدليل المعلوماتي المستمد من التفتيش

جرت أقلام الفقه على استعمال عبارة "حرية الإثبات الجنائي"، غير أنّه ليس معقولاً أن يجري هذا القول على إطلاقه، إذ أنّ اعتبارات الشرعية قد تحدّد نطاق هذه الحرية في حالات معينة، لذا لا بد من التطرق لتحديد مفهوم هذا المبدأ الراسخ في النظام القانوني (فرع أول)، و بيان مبرراته (فرع ثاني)، و تحديد نطاقه (فرع ثالث).

الفرع الأول: مدلول حرية القاضي في قبول الدليل المعلوماتي المستمد من التفتيش

إنّ الإحاطة الشاملة بمفهوم مبدأ حرية الإثبات الجنائي في قبول الدليل العلمي بشكل عام و الدليل المعلوماتي على وجه التخصيص يوجب علينا تحديد مفهومه وفقاً لمنظور المشرّع (أولاً) و الفقه (ثانياً) و القضاء (ثالثاً).

أولاً: التحديد القانوني لمبدأ حرية القاضي في قبول الدليل المعلوماتي المستمد من التفتيش

إنّ مبدأ حرية القاضي الجنائي في قبول الأدلة مستقر في مختلف الشرائع الجنائية من أمد طويل، و مفاد هذا المبدأ أنّ الإثبات الجنائي لا يتقيّد بمصدر معين فهناك حرية كاملة في تكوين عقيدة القاضي من أيّ مصدر مشروع للإثبات يصلح لذلك⁽¹⁾، بمعنى أنّ القاضي يحكم في الدعوى المنظورة أمامه وفقاً لما تكوّنت لديه عقيدته و بحسب إقتناعه و أن يقدر

(1) أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، المرجع السابق، ص 445.

بكامل حرّيته قيمة الأدلة الخاصة بالدّعى تقديرا منطقيًا، و يذهب الفقه في هذا الإتجاه إلى تعريفه باتجاهين⁽¹⁾.

فأمّا الرّأي الأوّل فيرى أنصاره أنّ مبدأ الإقتناع القضائي يعني التّقدير الحرّ المسبّب لعناصر الإثبات في الدّعى أي أنّ القاضي يقدر بحرية قيمة الأدلة المقدّمة إليه. أمّا الرّأي الثّاني، يرى أنصاره أنّ مدلول المبدأ لا يقتصر على تقدير الأدلة المقدّمة في الدّعى بل يتّسع ليشمل حرّية القاضي الجنائي في الإستعانة بأيّ دليل يراه ضروريا لتكوين عقيدته و استبعاد أيّ دليل لا يطمئن إليه⁽²⁾.

و بدون الدّخول بين مقارنات بين الرّأيين، فإنّنا نرى وجهة الرّأي الثّاني ذلك أنّ مبدأ حرّية الإثبات الجنائي إنّما يستتبع الإقرار للقاضي بالحرّية في تكوين هذا الإقتناع من أيّ وسيلة قانونية يراها لازمة لذلك⁽³⁾، و كذلك فإنّ قصر مفهوم المبدأ على تقدير عناصر الإثبات يؤدي إلى الخلط بين مبدأ حرّية القاضي الجنائي في تكوين عقيدته و بين نظام الإثبات المختلط و الذي يعني تحديد عناصر الإثبات سلفا من قبل المشرّع و يترك للقاضي إختياره في التّقدير⁽⁴⁾.

(1) محمد سيد حسن محمد، ضوابط سلطة القاضي في تقدير الأدلة، دراسة مقارنة بالشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 2008، ص 39.

(2) لمزيد من التّفصيل حول إشكالية الحرّية و الحصرية لوسائل الإثبات راجع: أحمد ضياء الدين محمد خليل، المرجع السابق، ص 244 و ما بعدها.

(3) الواقع أنّ دراسة مختلف التّعريفات لمبدأ حرّية القاضي في الدليل الجنائي لا تزال تختلط بغيرها من التّعريفات التي ترد على مبدأ حرّية القاضي في الإقتناع و يرجع ذلك إلى أنّ الحدود الفاصلة بين حرّية القاضي الجنائي في "قبول الدليل" و حرّية القاضي الجنائي في "تقدير الدليل" لا تزال مختلطة في نظر الفقه لاسيما في فرنسا، حيث يجمع معظم الفقهاء هاتين الحرّيتين لتشكّل في النهاية أمرا واحدا و ليس هذا بصحيح، فالقاضي الجنائي ليس حرّا في تقدير الدليل كأننا ما كان و إنّما هو حر فقط في تقدير الدليل المقبول في الدّعى. و بالتالي فإنّ مسألة قبول الدليل ينبغي أن تحضي بتعريف و دراسة خاصة و سابقة بالحتم عن تعريف و دراسة حرّية القاضي في تقدير الدليل، لأنّ محل هذه الحرّية هو "الأدلة المقبولة". لمزيد من التّفصيل راجع: محمد زكي أبو عامر، الإثبات في المواد الجنائية، بدون رقم الطّبعة، الفنية للطباعة و النّشر، مصر، بدون سنة الطّبع، ص 104.

(4) محمد سيد حسن محمد، ضوابط سلطة القاضي في تقدير الأدلة، دراسة مقارنة بالشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 2008، ص 40.

ثانياً: التعريف الفقهي لمبدأ حرية القاضي في قبول الدلائل المعلوماتية المستمد من التفتيش

يطلق على هذا النظام بتعبير "نظام الأدلة الأدبية" و أحيانا "بالنظام الحر للأدلة" و قد يطلق عليه أحيانا بنظام "الإقتناع الذاتي للقاضي الجنائي"، و يقصد بكلّ هاته التعبيرات أنّ القاضي لا يتقيّد بأيّ قيد أو شرط يفرض عليه و إنّما هو مقيد بضميره الذاتي البعيد عن الأهواء و الأحاسيس الشخصية، حرّ في تقدير قيمة الأدلة المقدّمة له من قبل الخصوم، و لا دخل لإرادة المشرّع في فرض دليل أو تحديد قيمة دليل، المهم أن يصل إلى الحقيقة بأيّ وسيلة مشروعة يبيّنه هو لا يبيّن المشرّع⁽¹⁾.

عموما يرتكز هذا المبدأ على تتمتع كل من الإدعاء و المتهم و القاضي في العملية الإثباتية بالحرية الكاملة في اختيار وسائل الإثبات مهما كانت طبيعة الوقائع المراد إثباتها، و أيّا ما كانت تلك الوسيلة، و ذلك بشرط الإلتزام الكامل بضوابط المشروعية، و تعتبر حرية الإثبات في المسائل الجنائية من المبادئ المستقرّة في الإثبات الجنائي⁽²⁾، و العلة في ذلك ترجع إلى رغبة المشرّع في ترك الباب مفتوحاً أمام أيّ وسيلة إثبات جديدة يمكن أن تظهر مستقبلاً وفقاً للتقدم العلمي و تطور المعرفة الإنسانية⁽³⁾، و من ثم فمشروعية وجود الأدلة العلمية و المعلوماتية لا تثير أي إشكال استناداً لمبدأ حرية القاضي الجنائي في قبول الأدلة.

ثالثاً: التعريف القضائي لمبدأ حرية القاضي في قبول الدلائل المعلوماتية المستمد من التفتيش

على نقيض ما دأبت عليه المحكمة العليا الجزائرية في ترديدها لهذا المبدأ في معظم قراراتها من غير التطرق لمفهومه، لكونها- في اعتقودنا- لا ترى حاجة إلى ذلك⁽⁴⁾، فقد إستقر قضاء محكمة النقض المصرية على أنّ المقصود بحرية القاضي في تكوين عقيدته، أن يكون للقاضي الجنائي كامل الحرية في أن يستمد اقتناعه من أيّ دليل يطمئن إليه من الأدلة التي

(1) مفيدة سعد سويدان، المرجع السابق، ص 140.

(2) أحمد ضياء الدين محمد خليل، المرجع السابق، ص 241.

(3) FRIEDRICH, Cyrielle, Les nouvelles technologies dans la procédure pénale: aspects techniques et juridiques de ces moyens de preuve, Thèse de doctorat, Univ. Genève, 2013, p 71.

(4) القرار الصادر عن المحكمة العليا غرفة الجناح المخالفات بتاريخ 29 جانفي 1991 رقم 1991، المجلة القضائية للمحكمة العليا، قسم الوثائق و الدراسات القانونية و القضائية، العدد 4، 1992، ص 211.

تقدّم في الدّعى، دون أن يتقيّد في تكوين اقتناعه بدليل معيّن إلاّ إذا نصّ القانون على غير ذلك، فالقاعدة في الإثبات أنّه يجوز للقاضي إثبات الجرائم بكافة الطّرق⁽¹⁾.

أمّا منظور محكمة النقض الفرنسية لهذا المبدأ، فإنّه يبدو أكثر تشدّداً، بحيث تفرض على محاكم الموضوع تطبيق هذا المبدأ تطبيقاً صارماً، بدعوى أنّ هذا المبدأ يتيح الحرّية الكاملة في الإثبات، لذا فهي تشدّد في أحكامها على حرّية قضاة الموضوع في قبول أيّ دليل يمكن أن يحقّق إقناعهم الجازم بحقيقة الواقعة الجرمية المطروحة عليهم، بل ذهبت في بعض أحكامها إلى أبعد من ذلك، حيث ترى أنّه في الحالات التي لا يوجد فيها نص قانوني يستبعد صراحة دليلاً معيّنًا فلا يجوز للمحكمة عدم قبول أيّ دليل تقدّم به الأطراف حتّى و لو كان ذلك الدليل غير مشروع، بل حتّى و لو كانت عدم المشروعية ناتجة عن ارتكاب جريمة ما⁽²⁾، و إجمال ما تقدّم أنّ هذا المبدأ يعني ببساطة حرّية القاضي الجنائي في تكوين قناعته من أيّ دليل يقدر إليه، دون أن يكون المشرّع قد قيّده بدليل معيّن مسبقاً.

الفرع الثاني: مبررات مبدأ حرّية القاضي في قبول الدلائل المعلوماتية المستمد من التفتيش

إذا كان القانون الجنائي قد فتح الباب على مصراعيه أمام القاضي الجنائي و الأطراف للإستعانة بالدلائل المعلوماتية المستمد من التفتيش الجنائي بهدف الوصول إلى الحقيقة الفعلية، فإنّه يثور التساؤل حول مبررات تلك الحرّية لدى الفقه (أولاً)، و كذا المشرّع (ثانياً)، و القاضي (ثالثاً).

أولاً: السند المنطقي لسلطة القاضي في قبول الدلائل المعلوماتية المستمد من التفتيش

يذكر الفقه في هذا الصّدّد أسباباً عديدة لتبرير مبدأ حرّية الإثبات الجنائي و تبعاً لذلك سلطة القاضي الجنائي في قبول جميع أدلة الإثبات، بما فيها الأدلة العلمية على اختلاف مصادرها و تتبلور هذه الأسباب في نواح عدّة أهمّها:

أمّا من الناحية الأولى، فإنّ تحويل القاضي الجنائي سلطة قبول جميع أدلة الإثبات التي يرى لزومها لتكوين إقناعه يعدّ نتيجة منطقية لتبني المشرّع لنظام الإقناع القضائي الذي

(¹) الطعن رقم 2252 لسنة 12 جلسة 30/11/1942 س 6، مشار إليه لدى: محمد سيد حسن محمد، المرجع السابق، ص 38.

(²) Cass. Crim. 15 juin 1993, n° 92-82.509, Bull. crim, 1993 N° 210.

يستتبع في الوقت نفسه السّماح للقاضي بالإستعانة بجميع وسائل الإثبات، فسلطة القاضي في هذا الشأن تعدّ مظهراً من مظاهر الثقة التي منحها المشرّع للقاضي في أن يحكم في الدّعى حسب العقيدة التي تكوّنت لديه بكامل حرّيته، لتمكينه من أداء رسالته في إرساء العدالة⁽¹⁾.

أمّا من النّاحية الثّانية، فإنّ موضع الإثبات في هذه الأخيرة يتعلّق بوقائع مادية أو نفسية لها طابع إستثنائي و ليس تصرّفات قانونية، و من ثمّ يستحيل إعداد أدلّة إثباتها مسبقاً خلافاً لما يحدث في المواد المدنية⁽²⁾، و أنّ تقييد الإثبات في المواد الجنائية يحول دون مواجهة فعّالة للظاهرة الإجرامية حيث يعمد المجرمون إلى العمل في خفاء و يظللون السّلطات العامة و يحمون آثار جرائمهم كلّما إستطاعوا إلى ذلك سبيلاً، فتقييد أدلّة الإثبات مسبقاً لا يؤدي في نهاية المطاف سوى لخدمة مصلحة المجرم في الإفلات من المسؤولية الجزائية⁽³⁾، بل إنّ تقرير حرّية الإثبات يفيد المتهمّ نفسه عندما يسمح له بدحض أدلّة الإتهام و إثبات براءته بكافة الطّرق⁽⁴⁾.

أمّا من النّاحية الثّالثة، فإنّ مبدأ حرّية الإثبات و بالتّبعية حرّية القاضي في قبول جميع الأدلّة ليس حكراً على القاضي و ليس مقرّراً لمصلحة الإتهام فحسب أي لإثبات الإدانة وحدها، و إنّما هو مقرّر لمصلحة الدّفاع كذلك الذي يمكنه الإستعانة بجميع وسائل الإثبات اللّازمة لدعم طلباته أو أوجه دفاعه، و بعبارة أخرى فإنّ هذا المبدأ مقرّر لمصلحة الحقيقة و إقامة العدالة، فكما يهتمّ المجتمع عقاب كلّ جان فإنّه يعنيه أيضاً بالقدر ذاته - بل أكثر - براءة كلّ بريء⁽⁵⁾، أي أنّ هذا المبدأ ببساطة يهدف إلى التّوصل إلى الحقيقة التي تعدّ الهدف الرئيسي من جمع الأدلّة الجنائية⁽⁶⁾.

(1) السيد محمد حسن شريف، المرجع السابق، ص 230.

(2) محمد زكي أبو عامر، المرجع السابق، ص 104.

(3) Marie Marty, La légalité de la preuve dans l'espace pénal européen, thèse de doctorat, Université de Strasbourg, 2016, p 100.

(4) أحمد عوض بلال، قاعدة استبعاد الأدلّة المتحصّلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، الطّبعة الثّالثة، دار النّهضة العربية، 2014، ص 21.

(5) السيد محمد حسن شريف، المرجع السابق، ص 230.

(6) M. BENILLOUCHE, Les transformations de l'administration de la preuve pénale, Paris, Société de législation comparée, 2006, p. 20.

أمّا من النّاحية الرّابعة، فإنّ وجود قرينة البراءة و إنتاجها لأنّثارها في إلقاء عبء الإثبات كلية على عاتق النّيابة بكلّ ما في هذا العبء من صعوبة، قاد المشرّع الجنائي إلى إعتناق مبدأ حرّية القاضي الجنائي في قبول الدّليل حتّى يكون عوضاً أو مقابلاً لافتراض البراءة في المتهّم و تحميل النّيابة العامة عبء إثبات الدّعوى، فإذا كانت مصلحة الفرد و اعتبارات حماية الحرّية الشّخصية قد إستوجبت إفتراض براءته، فإنّ مصلحة المجتمع في مكافحة الجريمة و اكتشاف حقيقة الأمر في الدّعوى الجنائية إستوجب قانوناً قبول جميع طرق الإثبات حتّى يتحقّق التّوازن بين مصلحة المواطن و مصلحة المجتمع⁽¹⁾.

و في اعتقادنا فإنّ أهمّ مبررات هذه القاعدة تجد سندها في الغاية الأسمى للنّظام الإجرائي كلّ و هي كشف الحقيقة الواقعية، و لا سبيل إلى تحقيق هذا المسعى إلّا من خلال منح القاضي سلطة و حرّية في قبول أيّ وسيلة إثبات تطرح عليه فيأخذ ما يرتاح إليها و يطرح غيرها، في يحنّ فإنّ تقييد القاضي بدليل معيّن يتعارض مع هذا الهدف، فهذا المبدأ دائماً ما يتمّ الرّكون إليه لقبول أيّ دليل يستند إلى إكتشاف علمي أو تقني مستحدث⁽²⁾، و لا شك أنّه من بين فئة الأدلّة العلمية الحديثة، الأدلّة المعلوماتية المستمدة من التفتيش الجنائي.

ثانياً: السند التشريعي لسلطة القاضي الجنائي في قبول الدليل المعلوماتي المستمد من التفتيش.

أشرنا أنّه في نظام الإثبات المعنوي لا يرسم القانون طرقاً محدّدة للإثبات يتقيّد بها القاضي الجنائي بل يترك حرّية الإثبات لأطراف الخصومة في أن يقدّموا ما يرونه مناسباً لإقتناع القاضي، و هذا المبدأ يعتبر حجر الزّاوية في القوانين ذات الصّبغة اللاتينية، كالشّريع الفرنسي⁽³⁾، و الشّريع المصري⁽⁴⁾، و قد أقرّه المشرّع الجزائري بنص صريح في

(1) محمد زكي أبو عامر، المرجع السابق، ص 107.

(2) معتصم خميس مشعشع، إثبات الجريمة بالأدلة العلمية، مجلة الشريعة و القانون، جامعة الشارقة، الإمارات العربية المتحدة، السّنة الرّابعة و العشرون، العدد 56، 2013، ص 25.

(3) Article 427 du C.P.P.F dispose que « Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction. Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui ».

(4) تنصّ المادة 302 من قانون الإجراءات الجنائية المصري "يحكم القاضي في الدّعوى حسب العقيدة التي تكوّنت لديه بكامل حرّيته و مع ذلك لا يجوز له أن يبني حكمه على أيّ دليل لم يطرح أمامه في الجلسة. و كلّ قول يثبت

قانون الإجراءات الجزائية بموجب المادة 212 منه و التي تنصّ "يجوز إثبات الجرائم بكافة طرق الإثبات ما عدا الأحوال التي ينصّ فيها القانون على غير ذلك و للقاضي أن يصدر حكمه تبعا لاقتناعه الخاص...".

و يستخلص من هذا النصّ أنّ القاضي له حرية تامة في اختيار عناصر الإثبات، فهذا النصّ العام ينطبق أيضا على الدليل الجنائي المعلوماتي، و عمومية هذا المبدأ العام في نظرية الإثبات الجنائي جعلت المشرّع لا يفرد نصا خاصا بقبول الدليل الجنائي المعلوماتي، على الرّغم من تنظيمه لإجراءات جمعه و التّوصل إليه عن طريق إجراءات التفتيش و المراقبة الإلكترونية بموجب القانون 04/9 المتعلّق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال.

و يتضح أيضا موقف المشرّع الجزائري إقراره بالأدلة المعلوماتية بشكل صريح عند تدخله سنة 2004 و قيامه بتجريم بعض الأفعال الماسة بنظم المعالجة الآلية للمعطيات بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر سنة 2004⁽¹⁾، كون هذه الفئة من الجرائم يستحيل إثباتها بغير الدليل المعلوماتي، و هذا الموقف نلمسه أيضا لدى المشرّع المقارن كما هو الحال في التشريع الفرنسي⁽²⁾، و البلجيكي⁽³⁾ الذي أغفل إيراد نصوصا خاصة للاعتراف بمقبولية الأدلة المعلوماتية في الإثبات الجنائي.

أنّه صدر من أحد المتهمين أو الشهود تحت وطأة الإكراه أو التهديد به يهدر و لا يعول عليه" كما تنص المادة 291 من نفس القانون "للمحكمة أن تأمر، و لو من تلقاء نفسها أثناء نظر الدّعى، بتقديم أيّ دليل تراه لازماً"⁽¹⁾ القانون رقم 15/04 المؤرخ في 10 نوفمبر سنة 2004 المعدّل لقانون العقوبات الجزائري، الجريدة الرسمية المؤرخة في 10 نوفمبر 2004، عدد 71.

⁽²⁾ أنظر مثلا في التشريع الفرنسي زيادة على المواد 56 و ما بعدها من قانون الإجراءات الجزائية.

La Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, JORF n° 0263 du 14 novembre 2014.

la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale JORF n°0129 du 4 juin 2016.

⁽³⁾ أنظر كافة التعديلات المدخلة على قانون التحقيق الجنائي البلجيكي لاسيما التعديل الأخير:

Loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales JORF du 14 janvier 2017.

و بالنسبة إلى التشريعات العربية - التي تعتبر لاتينية النزعة- فإنّ اعتناقها بشكل صريح لمبدأ حرّية الإثبات و سلطة القاضي في قبول الدّليل الجنائي بشكل عام، لم يمنع المشرّع من إدراج نصوص خاصة تؤكّد الإقرار بمقبولية الأدّلة المعلوماتية المستمدة من التفتيش.

و يأتي التّشريع القطري في مقدمة التّشريعات العربية التي أقرّت بمقبولية هذا النوع من الأدّلة بنص صريح الدّلالة، حيث تنص المادة 15 القانون القطري رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية "لا يجوز إستبعاد أيّ دليل ناتج عن وسيلة من وسائل تقنية المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية بسبب طبيعة ذلك الدّليل"، و هو ما أكدته المادة 122 من القانون اللبناني رقم 81 لسنة 2018 حيث نصّ من خلالها المشرّع على أنّه "يعود للمحكمة تقدير الدّليل الرّقمي أو المعلوماتي و حجّيته في الإثبات، و يشترط أن لا يكون قد تعرّض لأيّ تغيير خلال عملية ضبطه أو حفظه أو تحليله".

أمّا بقية التّشريعات العربية فهي لم تورد نصوصاً صريحة للإقرار بمقبولية الأدّلة المعلوماتية و لكنها أقرّت بحرّية القاضي في تقدير حجّية الدّليل المعلوماتي المستمد من التفتيش، و الإقرار بسلطة القاضي في تقدير حجّية هذا النوع من الأدّلة العلمية هو إقرار ضمني بسلطته في قبولها، لأنّ المنطق يفرض أن تكون "مسألة قبول الدّليل" سابقة على "تقدير قيمته الإقناعية"، فتقدير القاضي لا يجري إلّا على دليل مقبول، و يتضح هذا النهج بشكل كبير جداً لدى التّشريع المصري⁽¹⁾، و السوري⁽²⁾.

الحقيقة أنّه حتّى بالنسبة للتّشريعات التي تتبنّى نظام الأدّلة القانونية كالنظام الإنجليزي و غيره فقد عكفت على إدخال بعض التّطبيقات على أنظمتها القانونية بحيث لم تعد تأخذ بنظرية الأدّلة القانونية على إطلاقها، بل بدأت تتقبّل حرّية تقدير الأدّلة و هذا بلا شك دعت إليه ضروريات الإثبات الجنائي بصورته المعقّدة و المتطوّرة باستمرار⁽³⁾.

(1) أنظر المادة 11 من القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.

(2) أنظر المادة 25 من المرسوم التشريعي السوري رقم 17 لسنة 2012 المتعلّق بتطبيق أحكام قانون التّواصل على الشّبكة و مكافحة الجريمة المعلوماتية.

(3) هلاي عبد الله أحمد، النّظرية العامة للإثبات الجنائي، المرجع السابق، ص 89 و ما بعدها.

ثالثاً: السند القضائي لسلطة القاضي الجنائي في قبول الدليل المعلوماتي المستمد من التفتيش

تطبيقاً لمبدأ حرية الإثبات الجنائي فقد إستقر القضاء المصري على أن " للقاضي الجنائي حرية الإستعانة بكافة وسائل الإثبات لتكوين إقتناعه حول حقيقة الوقائع المرفوعة عنها الدعوى، ففي سبيل ظهور الحقيقة لزم أن يكون للثبابة العامة و للقاضي الجنائي حق اللجوء إلى كافة طرق الإثبات، فالقانون حينما أمّد القاضي في المسائل الجنائية بسلطة واسعة و حرية كاملة في سبيل تقصي ثبوت الجرائم أو عدم ثبوتها و الوقوف على حقيقة علاقة المتهمين و مقدار اتصالهم بها، فتح باب الإثبات على مصراعيه يختار من كل طريقة ما يراه موصلاً إلى الكشف عن الحقيقة، و هذا هو الأصل الذي أقام عليه القانون الجنائي قواعد الإثبات لتكون ملائمة لما تستلزمه طبيعة الأفعال الجنائية و تقتضيه مصلحة الجماعة من وجوب معاقبة كل جان و تبرئة كل بريء" (1).

و قد أبانت محكمة النقض الفرنسية توسّعاً واضحاً في تطبيقها لهذا المبدأ في كثير من أحكامها و لو على حساب الشرعية الإجرائية، كل ذلك يرجع سنده إلى كشف الحقيقة و ترجيحاً لإعتبارات الفعالية، فطالما توافر الدليل الجازم على اقرار المتهم لما نسب إليه كان للقاضي حرية قبول أي دليل جنائي يقدم إليه، لأنّه من غير المتصور ترك الجاني حراً طليقاً إستناداً إلى مبادئ تخالف هذه الحقيقة التي تكوّنت لدى القاضي و تحقّق يقينه بها (2).

و نفس الأمر بالنسبة إلى القضاء الجزائري خاصة المحاكم الابتدائية التي عكفت على قبول الأدلة المعلوماتية المستمدة من التفتيش في بناء حكم الإدانة أو تقرير البراءة و إن لم تفصح صراحة عن مبررات إعتناقها لهذا المبدأ (3).

(1) ممدوح خليل البحر، نطاق حرية القاضي الجنائي في تكوين قناعته الوجدانية، مجلة الشريعة و القانون (جامعة الشارقة) الإمارات العربية المتحدة، عدد 21، 2004، ص 331.

(2) H. LECLERC, «Les limites de la liberté de la preuve; Aspects actuels en France», Rev. sc. crim.1992, p. 17: «pour la Cour de cassation, c'est essentiellement sa valeur probante, son rôle dans la manifestation de la vérité. Une preuve est une preuve et la Haute juridiction répugne à laisser impuni un coupable avéré et à sacrifier la vérité à des principes non écrits et dont la définition est l'objet de discussions».

(3) راجع العديد من التطبيقات القضائية في هذا الشأن و الصادرة عن مجلس قضاء الجزائر مذكورة لدى: مناصرة يوسف، المرجع السابق، ص 129 و ما بعدها.

الثابت من خلال كافة هذه الأحكام أنّ القضاء كان دوماً يؤسس إيمانه على مبدأ حرية الإثبات في قبول مختلف وسائل الإثبات إلى مبررات الفقه المساقاة آنفاً، مشيراً إلى الارتباط الوثيق بين "مبدأ الإقتناع القضائي" و "سلطة القاضي في قبول جميع الأدلة"، فطبيعة الأفعال الجرمية هي التي إقتضت إقرار حرية الإثبات لتكون موائمة لطبيعة هذه الأفعال سواء من حيث تنوعها أو من حيث طبيعة سلوك الجناة، فالمصلحة العليا للهيئة الإجتماعية تحتم الأخذ به توصلًا لكشف الحقيقة⁽¹⁾.

و إن وقع الإجماع بين الفقه و القضاء على ضرورة تنبي مبدأ حرية الإثبات الجنائي، سعياً لكشف الجريمة و إقامة الدليل على مرتكبها، و استناداً إلى كافة المسوغات المساقاة آنفاً كان على القانون و الفقه و القضاء حتماً مقضياً الإعتراف بمقبولية الأدلة المعلوماتية المستمدة من التفتيش إستناداً إلى مبررات هذا المبدأ، بيد أنّ سلطة القاضي الجنائي في أعمال تقديره حول مدى مقبولية هذه الطائفة المستحدثة من الأدلة الجنائية ليست مطلقة بل لها نطاق يحددها و هو ما نتطرق إليه بالبيان في الفرع الموالي.

الفرع الثاني: نطاق حرية القاضي الجنائي في قبول الدليل المعلوماتي المستمد من التفتيش

هناك قيود ترد على سلطة القاضي في قبول الدليل المعلوماتي المستمد من التفتيش و تنحصر في نوعين من القيود، يتمثل الأول في التقييد بأدلة معينة في إثبات جريمة الزنا (أولاً)، أمّا الثاني فيتعلق بطرق الإثبات الخاصة بالمواد غير الجنائية (ثانياً).

أولاً: قيد تحديد الأدلة في جريمة الزنا

برغم ما يتمتع به مبدأ حرية القاضي الجنائي في قبول الأدلة الجنائية من العمومية، إلاّ أنّه ليس مطلقاً، فليست كل طرق الإثبات مقبولة في كل حال، فهناك من جهة عدّة طرق لا يجوز للقاضي الجنائي قبولها أو تأسيس إقتناعه عليها برغم عدم وجود قاعدة قانونية تحظر قبول هذه الطرق في الإثبات الجنائي، فالقانون يتدخل أحياناً بالنص الصريح محدداً للقاضي الجنائي "طرقاً محدّدة" لا يجوز له أن يقبل غيرها في إثبات بعض الجرائم، و يجري القضاء مؤيداً برأي الفقه على أنّ القانون الذي يحدّد طرق الإثبات المقبولة في بعض المواد استثناء لا

(1) السيد محمد حسن شريف، المرجع السابق، ص 230.

يحول دون إمكانية قبول غيرها من الأدلة ما لم يكن قد صرّح في صلبه صراحة باستبعاد غيرها من طرق الإثبات⁽¹⁾.

ففي بعض الأحوال لا يتدخل المشرّع في اقتناع القاضي بقيام الجريمة من عدمه أو توفر الدليل أو إنتفائه و إنما يحدّد وسيلة إثبات الجريمة⁽²⁾، كما هو الحال بخصوص إثبات جريمة الزنا، حيث تنصّ المادة 341 من قانون العقوبات الجزائري على أنّ "الدليل الذي يقبل عن ارتكاب الجريمة المعاقب عليها بالمادة 339 يقوم إمّا على محضر قضائي يحزره أحد رجال الضبط القضائي عن حالة تلبس، و إمّا بإقرار وارد في رسائل أو مستندات صادرة من المتّهم و إمّا بإقرار قضائي"⁽³⁾.

و في هذا الصدد يلاحظ أنّ هناك تطوّر في الإجتهد القضائي الجزائري، حيث قرّرت المحكمة العليا في قرار حديث لها أنّ الدليل المعلوماتي المستمد من تسجيل صوتي يعتبر من بين أدلة إثبات الزنا في حالة ما إذا تضمّن التسجيل إقراراً من شريك الزوجة أو المتهمين على نفسه بارتكاب جريمة الزنا⁽⁴⁾.

إذ يعدّ التسجيل الصوتي في هذه الحالة بمثابة اعتراف لأنّه من المستقر عليه في الفقه أنّه لا يشترط أن يصدر الإقرار بالزنا من الشريك في مجلس القضاء أو أمام سلطة الإستدلال أو التّحقيق أو محضر رسمي بل يجوز إثباته بكافة الطّرق المشروعة و متى ثبت كان للمحكمة أن تأخذ به إذا اقتنعت بصحته⁽⁵⁾، في مقابل ذلك إستقرت هذه المحكمة على

(1) محمد زكي أبو عامر، المرجع السابق، ص 107.

(2) حسن صادق المرصفاوي، المرجع السابق، ص 654.

(3) تقابلها المادة 286 من قانون العقوبات المصري "إنّ الأدلة التي تقبل و تكون حجة على المتّهم هي القبض عليه حين تلبسه بالفعل أو إقراره أو وجود مكاتيب أو أوراق أخرى مكتوبة منه أو وجوده في منزل مسلم في المحل المخصّص للحريم".

(4) مما جاء في هذا القرار "حيث أنّه بالرّجوع إلى القرار المطعون فيه يتبيّن و أنّ قضاة الإستئناف أيّدوا حكم المحكمة و تبنا الأسباب التي جاءت فيه أين جاء في حكم المحكمة عند إثبات جريمة الزنا المتابع لأجلها الطاعنون على إقرار المتهمين الوارد في المكالمات الهاتفية المسجّلة من طرف الطّاعنة (ق.ح) على المستند الإلكتروني المتمثّل في بطاقة الذاكرة للهاتف النقال و بذلك فإنّ قضاة الاستئناف طبقوا صحيح المادة 341 من ق.ع...". القرار الصادر عن المحكمة العليا غرفة الجنح المخالفات بتاريخ 29 مارس 2016 رقم 1010894.

(5) ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دراسة مقارنة، الطبعة الأولى، دار المطبوعات الجامعية، مصر، 2009، 643.

أنّ الدليل المعلوماتي المتمثل في التصوير المرئي للواقعة الإجرامية (الزنا) لا يعدّ من أدلّة إثبات هذه الجريمة المحدّدة على سبيل الحصر في المادة 341 من قانون العقوبات⁽¹⁾.

و يتجه بعض من الفقه المصري إلى القول بانصراف حكم هذه المادة إلى "كلّ متّهم بالزنا" لأنّ القانون صريح في ذلك و لا اجتهاد مع صراحة النّص بينما يتجه الفقه و القضاء إلى إنصراف حكم المادة فقط إلى شريك الزّوجة الزّانية أمّا بالنسبة للزّوجة أو الزّوج أو شريكته فإنّ إثبات الزّنا على أيّ منهم يخضع لحكم القاعدة العامة في حرّية القاضي في الإثبات⁽²⁾، قصارى القول أنّه يجوز قبول الأدلّة المعلوماتية المستمدة من التفتيش الجنائي في إثبات جميع الجرائم بما فيها جريمة الزّنا متى إنطوى الدليل المعلوماتي على "إقرار" من أحد الزّوجين أو شريكه يمكن تحصيله من خلال المراسلات الإلكترونية بمختلف صورها.

ثانيا: قيد إثبات المسائل غير الجزائية

من المسلم به أنّ إثبات المسائل غير الجنائية التي تطرح على المحكمة الجزائية و يكون الفصل فيها مقدّمة ضرورية للفصل في الدّعى العمومية يخضع للقانون الخاص بتلك المسائل سواء كانت مدنية أو تجارية أو أحوال شخصية، و قد نصّت المادة 225 من قانون الإجراءات الجنائية المصري "تتبع المحاكم الجنائية في المسائل غير الجنائية التي تفصل فيها تبعاً للدّعى الجنائية طرق الإثبات المقرّرة في القانون الخاص بتلك المسائل، و يعدّ هذا النّص تطبيقاً لقاعدة أنّ "قواعد الإثبات إنّما ترتبط بالموضوع التي تردّ عليه لا بنوع المحكمة"⁽³⁾.

و من ثمّ إذا كانت الجريمة خيانة أمانة و صار نزاع بشأن العقد و كانت قيمته تزيد عن مائة الف دينار جزائري فلا يجوز إثبات هذا العقد بالدليل المعلوماتي إذ يلزم إثباته بالكتابة⁽⁴⁾ و ذلك ما لم يجرز للقانون إثباته بالبيّنة لتوافر مبدأ ثبوت بالكتابة أو لوجود مانع

(1) القرار الصادر عن المحكمة العليا غرفة الجناح المخالفات بتاريخ 24 جوان 2009 رقم 443709، المجلة القضائية للمحكمة العليا، قسم الوثائق و الدّراسات القانونية و القضائية، العدد 2، 2009.

(2) محمد زكي أبو عامر، المرجع السابق، ص 109.

(3) عائشة بن قارة مصطفى، المرجع السابق، ص 231.

(4) المادة 333 من من الأمر رقم 75-58، مؤرخ في 26 سبتمبر سنة 1975، يتضمن القانون المدني، الصادر بالجريدة الرسمية عدد 78 بتاريخ 30 سبتمبر 1975، المعدّل و المتمّم.

أدبي أو مادي يحول دون الحصول على الدليل الكتابي⁽¹⁾، لكن هذا القول لا يجري على إطلاقه ففي حالات كثير نجد الدليل المعلوماتي المستمد من التفتيش الجنائي قد يتمتع بقيمة إثبات التصرف القانوني، و يمكن أيضا أن يثبت الفعل الجرمي في الحالات التي لا يستوجب فيها القانون العقد الرسمي في إثبات المعاملة المدنية⁽²⁾.

من جهة أخرى لا يتقيد القاضي بقواعد الإثبات المقررة في القانون المدني إلا إذا كان قضاءه في الدعوى الجنائية يتوقف على وجوب الفصل في مسألة مدنية هي عنصر من عناصر الجريمة المطروحة للفصل فيه، أما إذا كانت المحكمة ليست في مقام إثبات إتفاق مدني، و إنما هي تواجه واقعة مادية بحتة فإنه يجوز إثباتها بكافة طرق الإثبات بما فيها الدليل المعلوماتي المستمد من التفتيش الجنائي.

و لقد ضيق القضاء من نطاق هذا القيد سالف الذكر فقصره على حالة الإثبات المؤدي للإدانة أما في حالة البراءة فقد أجاز الإثبات بكافة الطرق دون التقيد بقواعد الإثبات المدنية و قد علّلت محكمة النقض المصرية ذلك بقولها أنه "من المقرر أنّ المحكمة في جريمة خيانة الأمانة في حل من التقيد بقواعد الإثبات المدنية عند القضاء بالبراءة لأنّ القانون لا يقيد بها بتلك القواعد إلا عند الإدانة في خصوص إثبات عقد الأمانة إذا زاد موضوعه عن مائة جنيه احتياطياً لمصلحة المتهم حتى لا تتقرر مسؤوليته و عقابه إلا بناءً على الدليل المعتبر في القانون و لا كذلك البراءة لانقضاء موجب تلك الحيطة و إسلاسا لمقصود الشارع في ألا يعاقب بريء مهما توافرت في حقه من ظواهر الأدلة"⁽³⁾.

(1) تطبيقاً لذلك قضت محكمة النقض المصرية "بأنّ إثبات وجود عقد الأمانة في جريمة خيانة الأمانة يتعين الإلتزام فيه بقواعد الإثبات المذكورة في القانون المدني، أما واقعة الإختلاس أيّ التصرف الذي يؤتبه الجاني و يشهد على أنه حول حيازته من حيازة ناقصة إلى حيازة كاملة أو نفي هذا الإختلاس و يدخل فيه رد الشيء موضوع الأمانة فإنها واقعة مادية يجوز إتباعها بكافة طرق الإثبات بما فيها البيّنة رجوعاً إلى الأصل و هو مبدأ حزية إقتناع القاضي الجنائي". نقض جلسة 1968/12/9 س 19 ق 217 مشار إليه لدى عائشة بن قارة مصطفى، المرجع السابق، ص 232.

(2) حيث تنصّ المادة 323 مكرر من القانون المدني ينتج الإثبات بالكتابة من تسأل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها و كذا طرق إرسالها".

(3) الطعن رقم 14184 لسنة 67 جلسة 21/12/2003 س 54 ص 1256 ق 176، مشار إليه لدى: ياسر الأمير فاروق، المرجع السابق، ص 640.

المطلب الثاني: القيود الواردة على حرية القاضي في قبول الدليل المعلوماتي المستمد من التفتيش

إذا كان المبدأ العام في القانون الجنائي هو حرية القاضي في قبول أي دليل جنائي يستعين به في تكوين قناعته و استظهار الحقيقة، فإنه لا قيمة لهذه الحقيقة التي يتم التوصل عليها على مذابح الحرية و الأخلاق، لذا فإن مبدأ الحرية مقيد بوجود أن يكون التفتيش عن الدليل المعلوماتي قد تم في ظل إحترام القيود التي يفرضها القانون و الأخلاق فلا بد من مراعاة مبدأ المشروعية (فرع أول) و النزاهة في التفتيش عنه (فرع ثاني).

الفرع الأول: مبدأ مشروعية الدليل المعلوماتي المستمد من التفتيش

تمثل قاعدة مشروعية الدليل الجنائي المعلوماتي المستمد من التفتيش ضماناً أساسية لحماية المتهم من تعسف السلطة و شططها، و هذا ما يقتضي ضرورة الوقوف على حقيقة الماهية القانونية لهذه القاعدة بتحديد مدلولها (أولاً) و بيان نطاقها (ثانياً).

أولاً: مدلول قاعدة مشروعية الدليل المعلوماتي المستمد من التفتيش

الواقع من الأمر أن التشريعات لا تهتم بوضع تعريف لقاعدة مشروعية الدليل الجنائي و ليس من اليسر التوصل إليه، لأنه ليس مفهوم قانونياً بحت، فلا تتحدد الملامح العامة لهذا التعريف إلا بالتطرق إلى مفهوم هذه القاعدة بشكل عام (أ)، و تطبيقاتها على الدليل المعلوماتي المستمد من التفتيش في ضوء بعض الإجهادات القضائية المتناثرة (ب).

أ- المفهوم العام لقاعدة مشروعية الدليل الجنائي

من الأصول الدستورية الكبرى في نظام الدول الديمقراطية ما يعرف بمبدأ "المشروعية الجنائية" أو "إحترام القانون" أو "سيادة القانون"، أي إلزام الحاكم و المحكوم بالقواعد القانونية التي تصدرها السلطات المختصة، و هذا المبدأ هو ما يميز دولة القانون عن الدولة البوليسية أو الدكتاتورية و تعتبر الشرعية الجنائية صورة من صور هذا الأصل العام، و تعني لا جريمة و لا عقوبة إلا بنص، إذ لا يمكن توجيه الإتهام ضد شخص لارتكابه فعلاً معيناً ما لم يكن منصوصاً على تجريم هذا الفعل في القانون، كما لا يمكن تطبيق العقوبة ما لم تكن محددة مسبقاً، و لم يأخذ هذا المبدأ صورته العالمية إلا بمقتضى الإعلان العالمي لحقوق الإنسان⁽¹⁾.

(1) أحمد أبو القاسم، المرجع السابق، ص 307.

لكن الحماية التي يكفلها مبدأ "لا جريمة و لا عقوبة إلا بقانون" تبقى قاصرة طالما كان من الممكن المساس بحرية المتهم من غير طريق القانون، أو كان من الممكن إسناد الجرائم للناس و لو لم يثبت ارتكابهم لها عن طريق إفتراض إدانتهم، لذا كان لابد من تعضيد هذه القاعدة بقاعدة ثانية تحكم تنظيم الإجراءات التي تتخذ قبل المتهم على نحو يضمن احترام الحقوق و الحريات الفردية، و تسمى هذه القاعدة بالشرعية الإجرائية أو قاعدة مشروعية الدليل الجنائي⁽¹⁾.

غير أنه ليس من اليسير تحديد ماهية مشروعية الدليل الجنائي المعلوماتي في الإجراءات الجنائية لأن المفهوم ليس قانونيا بحتا، و لا يستقى من مصدر واحد، و لا تحرص التشريعات على النص عليه صراحة، و لا تتحدّد ملامحه العامة إلا في ضوء بعض التطبيقات التشريعية و جهود بعض الفقه و القضاء، و لا يجدي في تحديد تلك الماهية الإستعانة بمفاهيم قانونية أخرى أكثر تحديدا مثل البطلان، فذلك لا يرتبط دائما بماهية الفكرة و إنما بالجزءات الناجمة عن الإخلال بها، أي أنها تعد بحق معالجة لاحقة للفكرة a posteriori و ليست كما ينبغي أن تكون معالجة مسبقة a priori⁽²⁾.

لكن هذا الغموض لا ينفي محاولة إستعراض تلك الفكرة، إذ يقصد عموما بمشروعية الدليل الجنائي التوافق مع القواعد القانونية المستقرّة في المجتمع و المعترف بها من قبل أفرادها أيّا ما كان مصدرها، و هي بهذا المعنى تختلف عن الشرعية التي تعني على وجه الدقة مجرد التوافق مع أحكام القاعدة القانونية المكتوبة أو المنصوص عليها من قبل المشرّع، و على ذلك فالمشروعية في حقيقتها أوسع مضمونا من الشرعية التي تعتبر أحد عناصرها⁽³⁾.

(1) أحمد فتحي سرور، الشرعية الدستورية و حقوق الإنسان، المرجع السابق، ص 128.

(2) أحمد عوض بلال، قاعدة إستبعاد الأدلة المتحصّلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، الطبعة الثالثة، دار النهضة العربية، مصر، 2014، ص 21.

(3) يمكن القول بناء على هذا التّحديد لمفهوم المشروعية بأنّ لها مدلولين الأول معنى موسع و هو المفهوم الموضّح في المتن، و الثاني معنى ضيق و يقصد به ذلك المفهوم الذي غالبا ما يستعمله الفقه للدلالة على إتفاق العمل مع القاعدة القانونية بمعناها الضيق أي مع القاعدة التشريعية بالذات لتصبح المشروعية بهذا المعنى مرادفة تماما للشرعية و لذلك يتجه جانب من الفقه إلى تعريف اللامشروعية الجنائية بأنها تلك الحالة الناجمة عن المخالفة القاعدة القانونية التي حددها المشرّع و المناط بها حماية المصلحة القانونية إلا أنّ هذا الفقه قد أورد تعريفا آخر للمشروعية قد يبدو فيه العدول عن المفهوم الأول حيث يقرّر أنّ اللامشروعية الإجرائية أصبحت لا تعدو أن تكون مخالفة لمقتضى قاعدة قانونية تحمي ما تعارف عليه المجتمع من قواعد لأنّه شتان الفارق بين ما ينص عليه المشرّع من

و الشرعية الإجرائية إذن تقتضي أن يكون القانون وحده هو مصدر كل إجراء يتخذ حيال المتهم بغرض الوصول إلى الحقيقة، مع خضوع كل هذه الإجراءات لإشراف القضاء، و افتراض براءة المتهم، و إلا اعتبر الإجراء و ما بني باطلا "فلا جريمة و لا عقوبة و لا إجراء جنائيا إلا بنص"⁽¹⁾.

تفريعا على ذلك، يجب الإلتزام بهذه الشرعية روحا و مضمونا دون الإكتفاء باحترامها شكلا، فلا يجوز للقائمين على الإجراءات الجزائية مباشرة هذه الإجراءات بروح المساس بحقوق المتهم و حرّياته جريا وراء جميع الدليل المعلوماتي للإدانة، لأن المقصود هو كشف الحقيقة ناصعة بأعلى معانيها، فالعقل الذي يسعى إلى المعرفة ليس كافيا، بل لابد من أن يلازمه الضمير الإنساني الذي يستلهم الحق و يحمي الحرّية⁽²⁾.

و هكذا فإنّ مبدأ شرعية الإثبات لا يلقى ترجمته فقط عبر النصوص الجزائية، بل أيضا و خارج إطار هذه النصوص، ما يعكس الفكرة القائلة بأنه "لا يمكن إقامة البيئة بأيّ ثمن" ما يعني أنّ الغاية لا يمكن لها أن تبرّر الوسيلة⁽³⁾، و بناء على ذلك تضع محكمة النقض البلجيكية القاعدة في تحديد ماهية الدليل غير المشروع بقولها "يعدّ دليلا غير مشروع ليس فقط الدليل المستمد من فعل محذور قانونا بنص صريح بل يشتمل كلّ فعل يتعارض مع القواعد الجوهرية للإجراءات الجزائية أو المبادئ القانونية العامة"⁽⁴⁾.

من هذا المنطلق حرص المشرّع الجزائري على إيلاء هذه القاعدة مكانة هامة فجعلها في مقدّمة الإجراءات الجزائية بموجب المادة الأولى منه، و التي نصّت فقرتها الأولى على أنّه "يقوم هذا القانون على مبادئ الشرعية و المحاكمة العادلة و احترام كرامة و حقوق

قوانين و ما تعارف عليه المجتمع من قواعد. لمزيد من التفاصيل حول مفهوم الشرعية و المشروعية: أحمد ضياء الدين خليل، المرجع السابق، ص 584.

(1) أحمد أبو القاسم، المرجع السابق، ص 307.

(2) طارق إبراهيم الدسوقي، الأمن المعلوماتي النظام القانوني لحماية المعلوماتية، بدون رقم الطبعة، دار الجامعة الجديدة، 2015، ص 334.

(3) نبيل شديد الفاضل رعد، الدفوع الشكلية في قانون أصول المحاكمات الجزائية، الطبعة الأولى، المؤسسة الحديثة للكتاب، 2005، ص 846.

(4) Leroux Olivier, Poulet Yves, «En marge de l'affaire Gaia : de la recevabilité de la preuve pénale et du respect de la vie privée» Revue générale de droit civil belge (Mechelen), 2003, p 163.

الإنسان"، فهذا النص جعل لحرية القاضي في الإقتناع حدا لا يمكن تخطيه، و هو ضرورة إلتزام الأدلة بالمشروعية و لما كانت الخصومة الجنائية تتطلب ضمان حقوق المتهم و حرياته و ليس مجرد مباشرة إجراءات جمع الأدلة لإثبات حق الدولة في العقاب، فإنه يتعين على القاضي أن يتأكد أولا من مشروعية الدليل، و لا يحول دون ذلك أن يكون الدليل صارخا في مظهره واضحا في دلالاته على إدانة المتهم مادام مشبوها ملطخا بإهدار محارم القانون⁽¹⁾.

في بقية الدول ذات النزعة اللاتينية فإنه و إن كان الإثبات الجنائي حرا إلا أن حرية الإثبات لا تعني أنه يكفي البحث عن الدليل الجنائي بأية وسيلة كانت، ففي الواقع فإن احترام حقوق الدفاع و حماية الكرامة الإنسانية و نزاهة القضاء تستوجب أن يكون الحصول على الدليل الجنائي قد تم وفقا لطرق قانونية مشروعة⁽²⁾، و رغم ما تثيره هذه القاعدة في إطار التفتيش عن الدليل الجنائي المعلوماتي نتيجة التعارض الصارخ بين التفتيش و حرمة الحياة الخاصة، إلا أن كافة التشريعات لم تفرد لها مفهوما أو نطاقا تاركة مفهوما يلفه الغموض، أدى في غالب الأحيان إلى تراجع المفهوم الحقيقي للفكرة و الجنوح نحو تغليب مصلحة الهيئة الإجتماعية في مكافحة الإجرام.

ب)- تعريف المشروعية في مجال الأدلة المعلوماتية المستمدة من التفتيش

الواقع من الأمر أن التشريعات المقارنة لا تهتم -من حيث المبدأ- بوضع نظرية عامة لمشروعية الدليل الجنائي المعلوماتي المستمد من التفتيش الجنائي، كما أنها لا تحرص على أن تضع هذه الفكرة مسبقا ضمن المواد المخصصة للإثبات الجنائي، غاية ما في الأمر أن الباحث يستهدي بتطبيقات متناثرة على الفكرة بشأن فئة معينة من هذه الأدلة أو يستشرد بالقواعد العامة التي يضعها القانون أو إستقر عليها القضاء و الفقه لبيان مشروعيتها من عدمه⁽³⁾.

(1) أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، مرجع سابق، ص 468.

(2) هلاي عبد الله أحمد، بحث بعنوان حجية المخرجات الكمبيوترية في المواد الجنائية دراسة مقارنة، مقدّم إلى مؤتمر القانون و الكمبيوتر، المنعقد في الفترة بين 1 و 3 ماي 2000 جامعة الإمارات العربية المتحدة، كلية الشريعة و القانون، الطبعة الثالثة، 2004، ص 752.

(3) يلاحظ أن مفهوم قاعدة مشروعية الدليل الجنائي كانت دائما تستمد من ذلك الصراع بين مبدأ شرعية الإثبات و مبدأ حرية الإثبات و هو ما يثير دائما مشكلة متجددة مع بحث لا يتوقف عن وسائل مبتكرة لكشف الحقيقة تنطوي

عموما تخضع قواعد الإثبات الجنائي المعلوماتي لمبدأ الشريعة و مقتضاه أن الدليل الجنائي المستمد من التفتيش لا يكون مشروعا و من ثم لا يعد مقبولا في الإثبات إلا إذا جرت عليه التفتيش عنه و استرداده و إقامته أمام القضاء في إطار أحكام القانون و احترام قيم العدالة و أخلاقياتها التي يحرص على حمايتها، فإذا كان المشرع يلقي على كاهل المحقق مهمة كشف الحقيقة في شأن الجريمة و اللوج إلى الأنظمة المعلوماتية تفتيشا عن أدلتها، فإن عمله مشروط بأن يتم في رحاب الشريعة و ذلك باحترام حقوق الأفراد و حرّياتهم و عدم المساس بها إلا في الحدود التي يقرّها القانون، فإن تجاوز المحقق هذه الحدود و تمكّن من استرداد دليل المعلوماتي يثبت وقوع الجريمة و نسبتها إلى المتهم و يجب إطراح هذا الدليل و عدم قبوله في الإثبات⁽¹⁾.

و لقد وضعت الإتفاقيات الدولية⁽²⁾، و الدساتير الوطنية⁽³⁾، و القوانين الوطنية المختلفة⁽⁴⁾، نصوصا تتضمن ضوابط الشريعة الإجرائية الماسّة بالحرية الشخصية، و من ثم فإن مخالفة هذه النصوص في التفتيش عن الدليل المعلوماتي يصمّ هذا الدليل بعدم المشروعية، و من هنا فإنه لا يجوز للقاضي الجنائي أن يقبل في إثبات إدانة المتهم أدلة معلوماتية لم تتبع بشأنها الضوابط القانونية المقررة في قانون الإجراءات الجزائية للتفتيش أو

على خطر المساس بالحرّيات الفردية في الوقت التي تتظافر فيه الجهود لحماية هذه الأخيرة و إعلاء قيمتها لذا يجنح الفقه إلى تحديد حالات عدم مشروعية الدليل لبيان المفهوم المقابل و هو المشروعية.

لمزيد من التفصيل راجع: أحمد عوض بلال، المرجع السابق، ص 32 و ما بعدها، عادل عبد البديع آدم سحين، المرجع السابق، ص 117 و ما بعدها.

(¹) ياسر الأمير فاروق ، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دراسة مقارنة، الطبعة الأولى، دار المطبوعات الجامعية، مصر، 2009، ص 644.

(²) أنظر على سبيل المثال المادتين 5، 12 من الإعلان العالمي لحقوق الإنسان لسنة 1948، و المواد 2، 3، 4، 6، 7، 8، 13، من إتفاقية حماية حقوق الإنسان في نطاق مجلس أوروبا المعتمدة سنة 1950، و المادة 15 من إتفاقية مناهضة التعذيب و غيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة لسنة 184.

(³) راجع المواد 32، 40، 41، 46، 74، 56، 57، 58، 59، 60 من الدستور الجزائري لسنة 1996 المعدل سنة 2016، و المواد 7، 9، 10، 11، 17، 19، 20، 21، 23 من الدستور المصري لسنة 2014 و المعدل سنة 2019، و المادة 66 من الدستور الفرنسي لسنة 1958 المعدل سنة 2008.

(⁴) راجع المادة 1 من قانون الإجراءات الجزائية الجزائري و المادة 1 من قانون الإجراءات الجزائية الفرنسي.

غيرها من القواعد⁽¹⁾، كالدليل المعلوماتي المستمد من تفتيش لم تأذن به السلطة القضائية، أو نتاج تفتيش جرى تنفيذه بعد إنقضاء مدة سريان الإذن، أو تفتيش مخالف للغاية منه، أو لأسلوب تنفيذه.

ثانياً: نطاق قاعدة مشروعية الدليل المعلوماتي المستمد من التفتيش في حالة البراءة

في الفقه خلاف حول مدى إشتراط المشروعية بوجه عام في دليل البراءة، و يمكن رد هذا الخلاف إلى إتجاهات ثلاثة، الأول يتمسك باعتبار المشروعية شرطاً لازماً في كلّ دليل معلوماتي سواء دليل البراءة أو دليل الإدانة، و الإتجاه الثاني يقصر شرط المشروعية على دليل الإدانة وحده، أما الإتجاه الثالث فيرى بالترقية بين ما إذا كانت طريقة الحصول على الدليل المعلوماتي غير المشروع ترقى إلى مرتبة الجريمة من عدمه.

الإتجاه الأول: جواز إستناد الحكم بالبراءة على دليل معلوماتي غير مشروع

يذهب الرأى السائد في الفقه المصري إلى تأييد موقف محكمة النقض⁽²⁾، فيرى جانب من الفقه أنّ رجوع قاعدة عدم قبول الدليل المتحصّل عن إجراء غير مشروع إلى إحترام

(1) قرّرت محكمة النقض الفرنسية في قرارها الصادر بتاريخ 08 جويلية 2015 بعدم مشروعية إجراءات إسترداد الأدلة المعلوماتية المستمدة من إجراء "اعتراض المراسلات الإلكترونية"، في تفاصيل هذه القضية أنّ مصالح الجمارك تمكّنت من الحصول على معلومات كشفت عن جريمة تُصب و إحتيال من خلال استخدام البطاقات المصرفية المزوّرة باسم شخص تمّ إيداعه بالسجن، و بعد فتح تحقيق قضائي على مستوى محكمة مرسيليا تمّ ندب الضبطية القضائية لأجل القيام بإجراءات إعتراض المراسلات الإلكترونية المرسلة و المستلمة على العنوان المستخدم من قبل المتهم الموقوف مع الغير إنطلاقاً من مكان سجنه، و بناء على هذه الإنابة القضائية قام المحققون بضبط و استرداد مختلف الرسائل المخزّنة بعلبة البريد الإلكتروني بما فيها تلك الرسائل المخزّنة بتاريخ سابق عن صدور إذن الإعتراض، على إثرها تقدم المتهم بدفع مؤداه بطلان الأدلة المعلوماتية المستمدة من هذه الإجراءات تأسيساً على أنّ إعتراض المراسلات إنصبّ على مراسلات إلكترونية مخزّنة بتاريخ سابق عن صدور الإذن القضائي بالإعتراض، غير أنّ طلب قبول بالرفض من قبل قضاة الموضوع، أما محكمة النقض فقد تصدّت لهذه الإجراء المطعون فيه بالبطلان إستناداً لنصوص المواد 100 و ما بعدها من قانون الإجراءات الجزائية، تتأسس على أنّ البيانات المولّدة و المخزّنة قبل تاريخ صدور إذن إعتراض المراسلات الإلكترونية يتمّ إستردادها وفقاً لإجراءات التفتيش المعلوماتي، أمّا إجراء إعتراض المراسلات فيقتصر فقط على البيانات التي تتمّ في الوقت الحقيقي اعتباراً من تاريخ صدور الإذن القضائي و ليس قبله.

Cass crim8 juillet 2015, n° 14-88457, Bull. crim 2015, n° 176.

(2) تطبيقاً لذلك قضت محكمة النقض المصرية أنّه "و إن كان يشترط في دليل الإدانة أن يكون مشروعاً، إذ لا يجوز أن تبنى إدانة صحيحة على دليل باطل في القانون، إلّا أنّ المشروعية ليست بشرط واجب في دليل البراءة، ذلك بأنّه من المبادئ الأساسية في الإجراءات الجنائية أنّ كلّ متهم يتمنّع بقريئة البراءة إلى أن يحكم بإدانته بحكم

حقوق الدفاع يؤدي إلى نتيجة في غاية الأهمية أدركتها محكمة النقض المصرية، و هذه النتيجة هي إقتصار قيد المشروعية على دليل الإدانة لأنه هو وحده الذي يمس حق الدفاع، أما دليل البراءة فلا يخضع لهذا القيد⁽¹⁾، و يؤيد بعض الفقه هذا الرأي على أساس أن الأصل في الإنسان البراءة، و لا حاجة للمحكمة أن تثبت براءته و كل ما تحتاج إليه هو أن تشكك في إدانته، فضلا على ذلك فإن بطلان دليل الإدانة الذي تولد عن إجراء غير مشروع إنما شرع لضمان حرية المتهم ، فلا يجوز أن ينقلب هذا الضمان وبالا عليه⁽²⁾.

علاوة على ذلك، فإن المحكمة لا تحتاج في إثبات البراءة إلى اليقين، بل يكفي في ذلك مجرد الشك، و هو ما يمكن الوصول إليه من خلال أي دليل و لو كان غير مشروع، أضف إلى ذلك أن للمتهم الحرية الكاملة في اختيار وسائل دفاعه بقدر ما يسعفه مركزه في الدعوى و ما تحيط نفسه من عوامل الخوف و الحذر و غيرها من العوارض الطبيعية لضعف النفوس البشرية، و الإصرار على تطلب مشروعية دليل البراءة أسوة بدليل الإدانة يعرقل حق المتهم في الدفاع عن نفسه الذي يعلو على حق المجتمع في إستيفاء العقاب⁽³⁾.

في حين ذهب جانب من الفقه في تبرير موقفه إلى الإستدلال بنص قرآني، و يتجلى ذلك في قوله تعالى في الآية 138 من سورة النساء " لا يحب الله الجهر بالسوء من القول إلاّ

بات، و أنه إلى أن يصدر هذا الحكم له الحرية الكاملة في إختيار وسائل دفاعه بقدر ما يسعفه مركزه في الدعوى و ما تحيط نفسه من عوامل الخوف و الحرص و الحذر و غيرها من العوارض الطبيعية لضعف النفوس البشرية، و قد قام على هدى هذه المبادئ حق المتهم في الدفاع عن نفسه و أصبح حقاً مقدساً يعلو على حقوق الهيئة الإجتماعية التي لا يضيرها تبرئة مذنب بقدر ما يؤذيها و يؤذى العدالة معاً، إدانة بريء، هذا إلى ما هو مقرر من أن القانون - فيما عدا ما إستلزمه من وسائل خاصة للإثبات- فتح بابه أمام القضاء الجنائي على مصراعيه يختار من كل طرقه ما يراه موصلاً إلى الكشف عن الحقيقة و يزن قوة الإثبات المستمدة من كل عنصر، مع حرية مطلقة في تقدير ما يعرض عليه و وزن قوته التدلالية في كل حالة حسبما يستفاد من وقائع الدعوى و ظروفها، مما لا يقبل معه تقييد حرية المحكمة في دليل البراءة بإشترط مماثل لما هو مطلوب في دليل الإدانة...". الطعن رقم 6097 لسنة 53 جلسة 1984/02/15 مشار إليه لدى: ياسر الأمير فاروق، المرجع السابق، ص 654.

(1) محمد زكي أبو عامر، المرجع السابق، ص 117.

(2) هلاي عبد الله أحمد، النظرية العامة للإثبات الجنائي، دراسة مقارنة بين النظم الإجرائية اللاتينية و الإنجلوساكسونية و الشريعة الإسلامية، المرجع السابق، ص 502.

(3) محمد زكي أبو عامر، المرجع السابق، ص 117 و ما بعدها.

من ظلم و كان الله سميعا عليما"، و القياس على ذلك يجيز الإستناد في حكم البراءة على دليل غير مشروع، خاصة و أنّ المتّهم لا يكون له يد في عدم مشروعيته⁽¹⁾.

الإتجاه الثاني: عدم جواز إستناد الحكم بالبراءة على دليل معلوماتي غير مشروع

على عكس الإتجاه الأول، ينتقد قلة من الفقه مسلك محكمة النقض المصرية على أساس مخالفته لمبدأ مشرعية الدليل في المواد الجنائية و المدنية على حد سواء، و الذي يعدّ تطبيقا مباشرا للقواعد التي تقضي بأنه "إذا تقرّر بطلان أيّ إجراء فإنّه يتناول جميع الآثار التي تترتب عليه مباشرة دون تفرقة بين دليل الإدانة و دليل البراءة"⁽²⁾.

ثمّ إنّه ليس للقضاء أن يقرّر قاعدة أنّ "الغاية تبرّر الوسيلة" كمبدأ قانوني صحيح، و هو إذا أقرّها في خصوص جواز إثبات البراءة بكلّ السبل، فقد يقال فيما بعد أنّه حتّى التزوير و شهادة الزور و إرهاب الشهود حتّى يعدلوا عن أقوالهم تصبح كلّها أمور مشروعة لإثبات البراءة، هذا ما لا يمكن أن يقول به أحد، و لكن ينتهي إليه حتما منطق هذا القضاء الخاطيء، ثمّ من ناحية أخرى فإنّ الورقة الواحدة أو الدليل الواحد قد يفيد في الإثبات و في النفي في وقت واحد بحسب الجزء الذي يستند إليه صاحب المصلحة فيه أو بحسب الزاوية التي ينظر إليه منها في العمل إذا جاء هذا الدليل عن طريق غير مشروع و هل يمكن قبوله من زاوية و رفضه من زاوية أخرى في وقت واحد⁽³⁾.

ثمّ أنّه من المفروض أن تكون كلّ السبل القانونية المشروعة كفيّلة وحدها بإثبات براءة البريء في أيّ تشريع إجرائي قويم، و إلّا فإنّ البنیان الإجرائي كلّّه يكون مختلا متداعيا، إذا كان يسمح بإدانة البريء أو بالأدق إذا كان لا يسمح ببراءة البريء إلّا بإهدار مبدأ الشّرعية من أساسه، و من ثمّ فإنّه لا يصحّ أن يقال أنّ إثبات البراءة ينبغي أن ينفلت من قيد مشروعية الدليل الذي يعتبر شرط أساسي في أيّ تشريع لكلّ إقناع قانوني سليم⁽⁴⁾.

(1) محمد سيد حسن محمد، المرجع السابق، ص 148.

(2) هلاي عبد الله أحمد، المرجع السابق، ص 503.

(3) نفس المرجع السابق، ص 503-504.

(4) أحمد ضياء الدين خليل، المرجع السابق، ص 735 و ما بعدها.

الإتجاه الثالث: التفرقة بين ما إذا كان الدليل غير المشروع وليد جريمة أم مجرد مخالفة لقواعد الإجراءات

توسّط البعض بين الإتجاهين السابقين فأيد قضاء محكمة النقض و لكن في حدود معينة، و ذلك عن طريق التفرقة في شأن دليل البراءة بين ما إذا كانت وسيلة الحصول عليه تعدّ جريمة جنائية، أم أنّها مجرد مخالفة لقواعد الإجراءات، فإن كانت الأولى وجب إهدار الدليل و عدم الإعتداد به لأنّ القول بغير ذلك مفاده إستثناء بعض الجرائم من العقاب و الدّعوة إلى إرتكابها و هو ما لا يجوز و تأباه الشرائع القويمة. أمّا إن كان الحصول عليه تمّ بالمخالفة لقاعدة إجرائية فحسب، فهنا يصحّ الإستناد إلى الدليل في تبرئة المتّهم تحقيقاً للغاية من تقرير البطلان، و لأنّ الغرض أنّ البطلان الذي شاب وسيلة التّوصل إلى الدليل إنّما يرجع إلى فعل من قام بالإجراء الباطل و بالتّالي لا يصحّ أن يضار المتّهم بسبب لا دخل له فيه⁽¹⁾.

و بناء على ذلك يرى هذا الجانب من الفقه جواز إستناد المحكمة في تبرئة المتّهم إلى دليل جاء من أوراق ضبطت لدى المدافع عن المتّهم على خلاف القانون أو رسائل ضبطت لدى هيئة البريد بمعرفة النيابة العامة دون إذن من القاضي المختصّ، إلى غير ذلك من الأدلّة النّاجمة عن تفتيش باطل و لا يصحّ لها التّعويل على دليل توصل إليه المتّهم بطريق السرقة أو التّزوير و نحو ذلك من الجرائم⁽²⁾.

و في خضمّ كلّ هذا الإختلاف الفقهي نجد أنّ المشرّع الجزائري قد حسم الخلاف إثر التّعدّلات الأخيرة المدخلة على قانون الإجراءات الجزائية بموجب القانون رقم 17-07 مؤرخ 27 مارس سنة 2017، بحيث أنّ المادة الأولى منه نصّت على أنّه "يقوم هذا القانون على مبادئ الشّريعة و المحاكمة العادلة و احترام كرامة و حقوق الإنسان"، فعمومية النّص تفيد بضرورة إستتراط المشروعية في كلّ من دليل الإدانة أو البراءة على حد سواء و عدم قصرها على دليل دون آخر.

في مقام الموازنة بين هذه الإتجاهات و موقف المشرّع الجزائري، فإنّنا نرى الإتجاه الثالث هو الأولى بالتأييد لأنّنا لو تمسّكنا باستبعاد الدليل المعلوماتي الذي يثبت براءة المتّهم لعدم

(1) سامي حسني الحسيني، المرجع السابق، ص 471.

(2) نفس المرجع السابق، نفس الموضوع.

مشروعيته فإنّ ذلك سيقود إلى نتيجة خطيرة جدا و هي إدانة بريء رغم إقتناع القاضي ببرائته عند تمحيص هذا الدليل، إلا أنّ عدم المشروعية يحول دون ذلك و هو أمر غير مستساغ نهائيا عقلا و منطقا، لأنّ ذلك مناهض أصلا لقيم المجتمع و العدالة، و الضمير، خاصة في الأحوال التي تكون فيها عدم مشروعية دليل البراءة قد تسببت فيها السلطة الإجرائية، كما هو الحال في شأن الدليل المعلوماتي المستمد من تفتيش نظم معلومات تشملها السرية المهنية، أو أنّ التفتيش كان شاملا متجاوزا لغايته، فانهى إلى ضبط دليل براءة المتهم فمن غير المعقول إستبعاد الدليل المعلوماتي في هذه الأحوال على أساس بطلان التفتيش لأنّه "لا يضير العدالة إفلات مجرم من العقاب بقدر ما يضيرها الإفئات علي حرّيات الناس و القبض عليهم بدون وجه حق".

و بناء عليه فإننا نرى أنّ مبدأ مشروعية الدليل الجنائي المعلوماتي المستمد من التفتيش محكوم إلى حد ما بمبدأ حرية الإثبات الجنائي، بحيث يجب أن تطغى الحقيقة على أيّ حق آخر في نظرنا متى كان الأمر يتعلّق بدليل البراءة، على أن تكون عدم مشروعية الدليل راجعة إلى مجرّد مخالفة لقواعد الإجراءات تسببت فيها السلطة الإجرائية، أمّا إذا كان دليل البراءة نتاج جريمة اقترفها المتهم سعيا لإثبات براءته فإنّه يصبح دليل غير مقبول يقع لزاما استبعاده و القول بخلاف ذلك دعوة صريحة إلى الإجرام و الفوضى بذريعة أن نبيل الغاية يبرر الوسيلة.

الفرع الثاني: مبدأ نزاهة الدليل المعلوماتي المستمدة من التفتيش

لا يكفي لمشروعية الدليل المعلوماتي المستمد من التفتيش أن تراعى فيه الضوابط القانونية، فالإلى جانب هذه القواعد يوجد أيضا "مبدأ النزاهة" أو "مبدأ الأمانة" الذي يساهم أيضا في تحديد الإطار التي يجب أن تجري في حدوده عملية التفتيش عن الدليل المعلوماتي و استردادها، و هذا المبدأ الذي يستمدّ وجوده من الأخلاق و الآداب العامة، يثير تساؤلات عديدة في الواقع العملي، لأنّ المشرّع لم يفكّر في تنظيمه أو الإشارة إليه، لذا لا بد من التّطرق إلى مفهومه (أولا) و إلى استعراض محدّداته (ثانيا).

أولا: مفهوم مبدأ نزاهة الدليل المعلوماتي المستمد من التفتيش

إنّ حرية الإثبات الجنائي لا تعني أنّه يكفي البحث عن الدليل المعلوماتي و استرجاعه بأيّة وسيلة كانت، ففي الواقع فإنّ إحترام حقوق الدّفاع و حماية الكرامة الإنسانية و نزاهة القضاء تستوجب أن يكون الحصول على الدليل الجنائي قد تمّ وفقا لطرق قانونية مشروعة و

نزيهة أيضا⁽¹⁾، غير مخالفة لمبادئ الآداب و الأخلاق و هو ما يعبر عنه "بمبدأ النزاهة" أو "مبدأ الأمانة في الإثبات" **Le Rrincipe De Loyauté Des Preuves**.

عموما فإنّ مبدأ أمانة الإثبات الجنائي هذا المبدأ لم يرد عليه نص في القانون، فعلى سبيل المثال فإنّ قانون الإجراءات الجزائية الفرنسي رغم أنّه لا يتضمّن نصوصا تتعلّق بمبدأ النزاهة في البحث عن الحقيقة القضائية حتى بعد تعديلاته الأخيرة، إلا أنّ الفقه و القضاء كانا دائما بجانب هذا المبدأ في الوصول إلى الدليل الجنائي، لذا يشير الفقه الفرنسي إلى أنّ القضاء قد قبل إستخدام الوسائل العلمية الحديثة في البحث و التّقيب عن الجريمة تحت تحفظ أن يتمّ الحصول على الأدلة الجنائية و من بينها الأدلة المعلوماتية بطريقة شرعية و نزيهة⁽²⁾.

و رغم أنّ القضاء الفرنسي لا يتردّد في تطبيق هذا المبدأ في أحكامه كشرط لقبول الدليل الجنائي معتبرا إياه شرطا جوهريا من شروط المحاكمة العادلة، إلا أنّه لم يضع له تعريفا محدّدا⁽³⁾، و عادة ما تكفي محكمة النقض الفرنسية عند الحاجة لبيان مفهوم مبدأ نزاهة الأدلة الجنائية بالإشارة إلى "وقوع تدليس من شأنه أن يعيب البحث عن الحقيقة و إثباتها"⁽⁴⁾.

واقع الأمر أنّه يقصد بمبدأ "الأمانة في الإثبات" أو مبدأ "نزاهة الأدلة الجنائية"، تلك الطريقة أو ذلك المنهج الذي يجب أن يتبع في التفتيش عن الأدلة، و الذي يتفق أساسا مع احترام حقوق الفرد و كرامة العدالة و يقتضي ذلك المبدأ وفقا لهذا المعنى ضرورة إلتزام المحقق باحترام الأمانة في كلّ ما يمارسه من إجراءات⁽⁵⁾.

إن هذا المبدأ يحوي قدرا كبيرا من القيم غير المكتوبة التي تتبع أساسا من الضمير و من التأسّي باعتبارات العدالة، و يترتّب على مخالفتها أو الخروج عليها البطلان دون حاجة

(1) هلاي عبد الله أحمد، المرجع السابق، ص 752.

(2) المرجع نفسه، ص 753.

(3) Renucci, Jean-François. « Droits de l'homme », Revue de science criminelle et de droit pénal comparé, vol. 4, no. 4, 2014, p 843.

(4) معتصم خميس مشعشع، المرجع السابق، ص 61.

(5) Bouzat Pierre, La loyauté dans la recherche des preuves, in Problèmes contemporains de procédure pénale. Recueil d'études en hommage à Louis Huguency, Paris, Sirey, 1964, p. 172.

إلى نص مباشر يفرضه، و ذلك تأسيساً على ما تعنيه تلك المخالفة من إهدار لقاعدة جوهرية مقررة لمصلحة الدفاع، و يسيطر مبدأ الأمانة في البحث عن الأدلة على كافة الأنظمة القانونية بصفة عامة دون حاجة للنص عليه، و إن كان يتفاوت قدر الإحترام المقرر لمفهومه خاصة فيما يترتب على مخالفته من آثار حسب النظام القانوني و فلسفته من ترجيح أيّ من المصلحتين العامة أم الخاصة أثناء المراحل المختلفة للدعوى الجنائية، إلا أنّ هناك جانباً من التشريعات قد حرصت برغم ذلك على النص على ضرورة إحترام المبدأ و مراعاة مفهومه⁽¹⁾.

و مبدأ بطلان إجراءات التفتيش إذا سبقتها أو صاحبها أعمال مخالفة لمبادئ الآداب و الأخلاق يعتبر من أهمّ النظريات التي لجأ إليها القضاء في فرنسا لحماية الحريات الفردية من الإجراءات التعسفية أو الشائنة التي لا يوجد لها تنظيم قانوني أو التي لم يجرّمها القانون بنص صريح، حتى قيل أنّ هذه النظرية تعتبر أهمّ مميّزات العصر الحاضر، و أساس تلك النظرية أنّ المحقق يجب أن لا يكتفي بمراعاة القواعد التي نصّ عليها صراحة في القانون لتنظيم إجراءات التفتيش عن الأدلة، بل يجب عليه فوق ذلك مراعاة المبادئ العامة غير المكتوبة التي تميلها روح القانون و إن لم تشر إليها نصوصه، لأنّ هذه المبادئ العامة تعتبر جزءاً لا يتجزأ من نظامنا القانوني و القضائي⁽²⁾.

و إذا إنتقلنا من العموم إلى الخصوص لوجدنا أنّ مبدأ أمانة الإثبات يمثل قاعدة جوهرية هامة و يجب أن تسيطر على كافة إجراءات التفتيش عن الدليل المعلوماتي، فيعدّ من تطبيقات عدم الأمانة أيّ أسلوب أو وسيلة تتضمّن في جوهرها أيّ قدر من عدم المشروعية و التحريض و التّحايل للحصول على القرائن التي كشفت عن وقوع الجريمة، أو عن وجود الأشياء اللّازمة للتّحقيق و التتقيب في نظام معلوماتي أو منظومة تخزين معلوماتية ، فإنّ كلّ ما ينتج عن هذه الوسائل غير المشروعة يجب إستبعاده و لا يصحّ مبرراً للتفتيش⁽³⁾.

(1) أحمد ضياء الدين، الخديعة و أثرها على الدليل الجنائي، المجلة العربية للدراسات و التّدريب، المجلد 2، العدد

2، الرياض، أكتوبر 1985، ص 87.

(2) توفيق محمد الشاوي، المرجع السّابق، ص 214.

(3) المرجع نفسه، ص 212.

ثانيا: متطلبات نزاهة الأدلة المعلوماتية المستمدة من التفتيش

إنّ العلاقة الجدلية غير المستقرة بين مبدأ حرية الإثبات و مبدأ أمانة الإثبات، تفرض علينا تحديد بعض متطلبات النزاهة في التفتيش عن الدليل المعلوماتي، محاولة منا لرسم حدود لحرية القاضي الجنائي في قبول الدليل المعلوماتي إستنادا إلى الأخلاق و الآداب، و لعل أهمها حضر اللجوء إلى الحيلة و الخديعة و التحريض على الجريمة (أ)، و حضر تجاوز حد معين من الإكراه في تنفيذ التفتيش المعلوماتي (ب)، و حضر تفتيش النظام المعلوماتي للأنتى بغير الإستعانة أثنى (ج).

أ- حضر الخديعة و التحريض على الجريمة حال التفتيش عن الدليل المعلوماتي

يثور التساؤل في ضوء متطلبات نزاهة الدليل المعلوماتي المستمد من التفتيش عن معيار النزاهة الذي يحدّد مشروعية هذا الدليل من عدمه؟ أو بعبارة أخرى، ما هو المعيار الذي يجب الأخذ به في التمييز بين العمل الإجرائي الذي يهدف إلى كشف الجريمة بغية إقامة قرائن تبرّر التفتيش المعلوماتي و انتهاك حريات الأفراد و خصوصياتهم المعلوماتية و بين الأعمال التي تعتبر بحد ذاتها تحريضا على ارتكاب الجريمة؟

تعتبر الخديعة من أخطر الوسائل غير الأمانة التي قد يلجأ إليها الباحثون و المحققون للحصول بمقتضاها على أدلة إدانة المتهم، و يقصد بها تلك الأعمال الخارجية التي يقوم بها المحقق لتأييد ما يدعيه من أقوال كاذبة للإيهام بصحة الواقعة و ذلك لتظليل المتهم أو المحتال عليه بقصد التأثير عليه و الحصول منه على ما يؤيد إدانته أو يسهل من ثبوتها أو يساعد في تقديم أية عناصر إيجابية قد تسيء من مركزه⁽¹⁾.

الواقع من الأمر أن كلاً من المشرّع و القضاء في الجزائر لم يضعوا معيار ثابتا يهتدى به لتحديد مدى نزاهة الأدلة عند إستعمال الحيلة في التفتيش عن الدليل المعلوماتي، إلا أننا نجد أنّ محكمة النقض الفرنسية قد حاولت عبر العديد من قراراتها رصد مقياس يحدّد ضوابط النزاهة في التفتيش عن الأدلة الجنائية، يعبر عليه الفقه بمعيار "سببية الأعمال الإجرائية" *Causalité Des Actes De Procédure*.

و يقوم هذا المعيار على التفريق بين فعل التحريض على ارتكاب الجريمة « *provocations à l'infraction* » و فعل الإستدراج سعيا لجمع الأدلة الجنائية « *provocation* »

(1) أحمد ضياء الدين، المرجع السابق، ص79.

«a la preuve»، فبينما يناقض الفعل الأول مبدأ النزاهة في التفتيش عن الدليل المعلوماتي، يعدّ الثاني مقبولاً في الإثبات الجنائي⁽¹⁾.

حيث يتحدّد الفارق بين فعل التحريض لارتكاب الجريمة و الاستدراج لجمع الدليل الجنائي في ضوء الإجابة على سؤال مفاده هل "الأعمال التحريضية" أو "الحيل" التي سلكتها السلطة الإجرائية أسفرت عن ارتكاب الجريمة أم أنّها تهدف ببساطة إلى جمع الأدلة من جريمة ارتكبت بالفعل أو على وشك ارتكابها؟⁽²⁾، و قد كانت المحكمة الأوروبية أكثر دقة في رصد معيار التفريق بين العمليين و الذي يجري في ضوء التجاوب مع تساؤل مؤداه "هل كانت الجريمة لتحدث و تتحقّق لولا تدخل السلطة الإجرائية بمنقضى هذا الفعل أم لا"؟⁽³⁾.

وفقاً لهذا المعيار يلزم في الخديعة التي تعيب الدليل المعلوماتي المستمد من التفتيش و من ثمّ تبطله أن تُحدّث الوسيلة الخداعية قدرًا من التّظليل للمتهم أو الشّخص الموجهة إليه، و ذلك بإيهامه و تغليطه في أمر على غير حقيقته مما يجعله ينطلي عليه و يصدّقه، فتتأثر به إرادته و تستجيب لإرادة المظلل أو المخادع و تتصاع لغايتها و تسلّم لها بكل ما تريد، مع ضرورة صدور الدليل سواء بصورة مباشرة أو غير مباشرة كأثر لوقوع هذه الخديعة و ما أحدثته في نفس المتهم، بحيث لولاها لما كانت إستجابته لإرادة المدّلس و من ثمّ إلقاءه بما أدلى به من إقرار أو مساهمة بأيّ قدر للحصول منه على دليل مما يجدر بالتالي ضرورة إستبعاده لصدوره نتيجة لهذا الخداع⁽⁴⁾.

من بين التّطبيقات القضائية على اعتماد هذا المعيار في رصد مدى نزاهة الأدلة الجنائية المعلوماتية المستمدة من التسرب الإلكتروني، ما قضت به محكمة النقض الفرنسية حين قضت بأنّه "لا يشكّل تحريضاً على الجريمة من قبل موظّف عمومي أجنبي لارتكاب

(1) Renucci, Jean-François, op cit, p 843.

(2) Halard, Guillaume, Réflexions sur la provocation policière, Revue de science criminelle et de droit pénal comparer, vol. 1, no. 1, 2018, pp. 31-58.

(3) CEDH, arrêt RAMANAUSKAS c. LITUANIE, du 5 févr. 2008, n° 74420/01, §73 « la Cour estime que les agissements de AZ et VS ont eu pour effet de provoquer le requérant à commettre l'infraction pour laquelle il a été condamné et que rien n'indique que, sans leur intervention, celle-ci aurait été commise. Compte tenu de cette intervention et de son utilisation dans la procédure pénale litigieuse, le procès du requérant a perdu le caractère équitable requis par l'article 6 de la Convention. »

(4) أحمد ضياء الدين، المرجع السابق، ص 80.

جريمة، قيام شرطة نيويورك بتصميم موقع إلكتروني يتيح لمستخدمي الأنترنت تبادل ممارسات الإحتيال في البطاقات المصرفية، تأسيسا على أنّ هذا الموقع الإلكتروني كان يهدف إلى جمع أدلة على إرتكاب الجرائم و تحديد هوية الجناة، غير أنّ هذا الفعل لم يصل إلى درجة تحريض الأفراد على إرتكاب الجرائم⁽¹⁾.

في مقابل ذلك إعتبرت ذات المحكمة في قرار مغاير لها أنّ "الجوء ضابط الشرطة القضائية إلى الإتصال بشبكة الأنترنت و التّكر في شخصية طفل قاصر لم يبلغ 11 سنة من عمره يبحث عن علاقات جنسية يشكّل "تحريضا لارتكاب الجريمة بما يخالف مبدأ النزاهة في البحث عن الدليل المعلوماتي"⁽²⁾.

و هكذا تواترت أحكام القضاء الفرنسي على تحديد عدم نزاهة الدليل المتحصّل عليه نتيجة التّحريض الذي يشكّل إكراها أخلاقيا بقصد حماية "الشّخص الذي تصرف تحت تأثير قوّة أو قيد لم يكن بوسعه أن يقاوم أيّ منها"⁽³⁾، معتبرة إياه فعل يقوّض مبدأ نزاهة الأدلة بما يناقض الحق في محاكمة عادلة، فالتّحريض على إرتكاب جريمة من قبّل أو من خلال موظّف من موظفي السّلطة العامة، يجعل الأدلة التي يتمّ الحصول عليها تبعا لذلك غير مقبولة⁽⁴⁾، إلاّ أنّه في غالبية الحالات نجد أنّ القضاء الفرنسي يقرّر نزاهة الأدلة على أساس أنّ الأفعال الصّادرة عن الضّبطية القضائية و المطعون في نزاهتها و أمانتها "لم تقضي على إرادة المتّهم بأيّ شكل من الأشكال"⁽⁵⁾.

و هذا الموقف الغالب على قضاء محكمة النقض الفرنسية محل نظر في تقديرنا لأنّه لا يمكن إنكار حقيقة لا تقبل الجدل تتمثل في تأثير عمل الضّبطية القضائية على إرادة المتّهم حتى و إن لم تعدمها، فهذه الأعمال الإجرائية يمكنها على الأقلّ تيسير إرتكاب الجريمة و تسهيل تنفيذها، و أحيانا قد تهّيء الفرصة لتحقيقها، و هو ما يثير التّساؤل فيما إذا كانت هذه الأعمال ترمي إلى تجنّب وقوع الجرائم أو التّحريض على إرتكابها، ذلك الغموض الذي جعل

⁽¹⁾ Cass crim 30 avr 2014, n° 13-88.162, Bull. Crim, n° 119.

⁽²⁾ Cass crim. 11 mai 2006, n° 39-85.995, Bull. Crim, n° 132.

⁽³⁾ Halard, Guillaume, op cit , p 35.

⁽⁴⁾ Cass crim. 11 mai 2006, n° 05-84.837, Bull. crim. 2006, n° 132.

⁽⁵⁾ Cass crim. 22 juin 1994, n° 92-85.123, 92-85.124 et 92-85.637, Bull. crim. 1994, n° 247.

القضاء المقارن لا يستقر على رأي واحد بين من يفسر نزاهتها إستنادا إلى طبيعة الجريمة و صعوبة إثباتها خاصة تلك التي يسهل ارتكابها من خلال النظم المعلوماتية⁽¹⁾، و بين متمسك بشرط الأمانة كمبدأ عام في القانون حتى في مواجهة أخطر الجرائم.

الحقيقة أنّ هذا المعيار في التفرقة بين الدليل المتسم بالنزاهة و المفقّد لها معيار صعب للغاية من الناحية العملية على الأقل، و مرجع هذه الصعوبة يكمن في إرتباط العامل الإجرائي (الحيل و الخدع و التّحايل) الرّامي إلى الكشف عن الدليل المعلوماتي دوما بارتكاب جريمة جديدة نتيجة لهذا العمل، هذه الحقيقة الواقعية جعلت المشرّع البلجيكي يتصدى لهذه الأفعال بالحظر بموجب المادة 47 ter من قانون التّحقيقات الجنائية - على الأخص في باب التفتيش - التي تنصّ "في إطار تنفيذ طريقة تفتيش معيّنة، لا يمكن لضابط الشرطة تحريض المشتبه فيه على ارتكاب جرائم أخرى غير تلك التي يعترزم المتّهم ارتكابها"⁽²⁾، و هو ما انتهت

(¹) في إحدى القضايا التي فصل فيها القضاء الإنجليزي بنزاهة الدليل المعلوماتي المستمد من تفتيش مواقع التّواصل الإجتماعي رغم قيام الشرطة بفعل تحريضي تتلخص وقائعها في أنّ المتّهم أعلن عن رغبته بإقامة علاقات جنسية مع فتيات تتراوح أعمارهن بين ثمانية سنوات و ثلاثة عشر سنة مقابل المال و وضع التفاصيل الخاصة بالتّواصل معه في رسومات وجدت في عربة قطار، تظاهر أحد أفراد الشرطة بأنّه فتاة و قام بالتّواصل مع المتّهم عن طريق رسائل نصّية أرسلها عبر الهاتف الخليوي، أجرى المتّهم حوارا مع رجل الشرطة معاقب عليه قانونا، تمّ إلقاء القبض على المتّهم، و أسندت إليه عدّة تهم و هي محاولة إغواء فتاة قاصر على القيام بأفعال جنسية وفقا للمادة 8 من قانون الجرائم الجنسية لسنة 2003، و قد قضت محكمة الإستئناف بتأييد حكم محكمة الموضوع بعدم وقف الإجراءات و شدّدت على أنّ هذا النوع من الجرائم يرتكب باستخدام وسائل الإتصال الحديثة (الأنترنت) حيث يستطيع الشّخص إخفاء هويته حتى ذلك الوقت الذي تصيح فيه الضّحية في حضرة الجاني و يصبح في وضع يمكنه من ارتكاب جريمته بصورة سرّية، و من ثمّ فإن صعوبات الكشف عنها تعتبر ظروف مادية بحثة تلفت الإنتباه إلى الحاجة الملحة للشرطة للقيام بتحريات سرّية للكشف عن الأنشطة الإجرامية على أساس أنّ سلوك الشرطة في هذه الحالة مجرد إعطاء فرصة للمتّهم للشروع في ارتكاب جريمة ممثلة و الحصول على دليل ضروري للحكم بالإدانة.

أنظر الحكم: 008(QB 460 at 472); EWCA Crim 118 (2007) R V Jones، مشار إليه لدى: سامي حمدان الرّواشدة، المرجع السّابق، ص 38.

(²) Art. 47 ter du code d'instruction criminelle.

إليه محكمة النقض الفرنسية التي تقرّر حظر وسائل الخداع و التّحريض التي لا تستند إلى نشاط إجرامي سابق بغرض "الكشف عنه" أو "منع إستمراره"⁽¹⁾.

لذا نرى أنّه لا يكفي لنزاهة الدليل المعلوماتي المستمد من التفتيش مثلا وجود أسباب و قرائن تبرّره، بل يجب أن تكون هذه الأسباب و الوقائع مشروعة، فإذا وجدت لدى المحقّق قرائن جدية على أنّ نظاما معلوماتيا ما يحتوي أدلة معلوماتية يمكن التفتيش عنها و ضبطها لصالح التّحقيق جاز له أن يفتش هذا المحل، و يفتشه بناء على تلك القرائن بشرط أن تكون تلك القرائن قد وصلت إليه بطريق قانوني و مشروع⁽²⁾.

أمّا إستعمال الخديعة و الحيل و الغش للإيقاع بالمتّهم و تغليطه بما يعيب إرادته فإنّ ذلك ينافي مبدأ عدم جواز تجريم الذات، و قد إعتبرتها محكمة النقض الفرنسية قديما بأنّها

(¹) Cass crim., 9 août 2006, pourvoi n° 06-83.219, Bull. Crim. n°202 ; 4 juin 2008, n° 08-81.045, Bull. n°141 ; 8 juin 2005, n°05-82.012, Bull. n°173 ; 30 avril 2014, n°13-88.162, Bull. n°119 ; 25 octobre 2000, n°00-80.829, Bull. n° 317 ; 8 juin 2005, n°05-82.012, Bull. n°173.

(²) يرى جانب من الفقه أنّ الحيلة تتيح بلا شك للمحقق وسيلة هامة تساعده في إمكانية الكشف عن غموض الجريمة و التّعرف على الحقيقة فيها بينما إستبعادها أو الحرمان منها بصورة مطلقة يعني تجريده من وسيلة هامة من وسائله و من سلاح لا يمكن إنكار جدواه في الوصول إلى هدفه، و على ذلك فإنّ المعيار الذي نرى إمكانية الإستعانة به للتّمييز بين الدّهاء المقبول و الخداع المرفوض يعتمد أساسا على القول بأنّه لا يجوز للشرطة إستعمال طرق الدّهاء إلّا إذا كانت هناك ضرورة تدفع إليها و هذا يقدّر بخطورة الجريمة و طبيعتها و مدى المشغولية التي أحدثتها للرأي العام مع مراعاة شخصية المنحرف، و يقوم معيار التّمييز بين ما هو مسموح و ما هو محظور على ثلاثة عناصر:

- (1) أن تقتصر إجراءات الدّهاء المقبول على مرحلة جمع الإستدلالات من قبل مأموري الضّبط القضائي دون مرحلتي التّحقيق و المحاكمة و ذلك بقصد التّوصل إلى جمع الإستدلالات عن الجريمة.
- (2) أن تكون هناك ضرورة ملحة تحتم اللّجوء إلى وسيلة الدّهاء تلك على أن تستفاد تلك الضّرورة أساسا من أحد الأمرين الأوّل مما يكتنف إرتكاب الجريمة من غموض مما يجعل إمكانية التفتيش فيها للكشف عن مرتكبيها يتميّز ببعض الصّعوبات و الثّاني مدى جسامة الجريمة.
- (3) ألا يترتّب على استخدام وسيلة الدّهاء تفويت أو تقليل فرصة المتّهم في الدّفاع عن نفسه و ذلك يتأتّى حين تسفر تلك الوسيلة عن دليل الإدانة الوحيد في الواقعة محل البحث مما يجعل من المعقول ضرورة التّشكيك في صحة الدليل و لذلك فإنّه يلزم دائما لإمكان قبول ما تسفر عنه تلك الحيلة من نتائج أن يتوافق ذلك الدليل مع بقية أدلة الواقعة الأخرى و تتأيّد جميعها دون أيّ تعارض أو تناقض.

لمزيد من التّفصيل حول هذه النقطة راجع: أحمد ضياء الدين، المرجع السّابق، ص 86 و ما بعدها.

أفعال تحط من "كرامة القضاء" و معاونه، فشرف الوظيفة يوجب مراعاة هذا المبدأ في تحقيق غاياتها⁽¹⁾.

ب)- حضر إجبار المتهم على البوح بالأرقام السرية لإجراء التفتيش المعلوماتي

توصلنا عند الحديث عن خصائص التفتيش المعلوماتي أنه إجراء قسري يقتضي تنفيذه الحد من حرية المتهم الشخصية بالقدر اللازم لتنفيذه و ذلك بحسبان أن القهر لا غنى عنه لتنفيذ هذا الإجراء، لكن السؤال المطروح ما هي حدود أعمال العنف و الإكراه الجائزة للقائم بالتفتيش، و التي يفرض تجاوزها إلى مخالفة مبدأ النزاهة؟

إن القاعدة العامة التي إستقر عليها القضاء أن العنف و الإكراه الذي يجيزه تفتيش الشخص هو ما يلزم لوضع اليد على الشخص "إذا لم يذعن المتهم للتفتيش أو بدت منه مقاومة كان لمن يباشر إجراءات التحقيق أن يتخذ كل ما من شأنه أن يمكنه من القيام بمهمته و لو كان عن طريق الإكراه"، و هذا المبدأ الذي يسير عليه القضاء يعتبر تطبيق سليم لمقتضى القواعد التي تجيز التفتيش لأن جواز الإطلاع يجيز الأعمال التي يستلزمها تمكين المحقق من مباشرته⁽²⁾. إلا أن التفتيش عن الأدلة المعلوماتية يطرح إشكالية التفسير الذي يمنع السلطة القائمة بالتفتيش من الولوج إلى الأنظمة المعلوماتية و تنفيذ التفتيش، فهل يملك قاضي التحقيق أو من يندبه سلطة الجبر و الإكراه على الشخص الخاضع للتفتيش للبوخ بالأرقام السرية التي تحول دون الولوج إلى النظام المعلوماتي المستهدف؟

إذا سلمنا للمحقق بشيء من السلطة على الأعضاء المادية في جسم الإنسان، فيجب القول بأن هذه السلطة تقف عند هذا الحد، فمحل التفتيش هو جسم الإنسان المادي بحثا عن أجهزة التخزين الرقمية و لا يمكن أن يمتد إلى الجانب الروحي أو النفسي في شخصية المتهم، لإجباره على البوح بالأرقام السرية لنظامه المعلوماتي "محل التفتيش" لأن هذه المسألة مرتبطة بأهم حقوق المتهم و هو الحق في الصمت و عدم تجريم ذاته⁽³⁾.

(1) Rousselet Marcel, Les ruses et les artifices dans l'instruction criminelle, Revue de science criminelle et de droit pénal comparé, 1946, n° 1, p.-56. " employé un procédé s'écartant des règles de la loyauté que doit observer toute information judiciaire et constituant, par cela même, un acte contraire aux devoirs et à la dignité du Magistrat ."

(2) توفيق محمد الشاوي، المرجع السابق، ص 249.

(3) بحثت المؤتمرات الدولية موضوع حق المتهم في الصمت، فقررت اللجنة الدولية للمسائل الجنائية المنعقدة في برن سنة 1929 "أنه من المرغوب فيه أن تقرّر القوانين بوضوح مبدأ عدم إلزام الشخص باتهام نفسه و إذا رفض

لقد بات من المسلم به في معظم التشريعات الحديثة أنّ للمتهم أن يمتنع عن الإجابة عن الأسئلة الموجّهة إليه أو أن يدلي بأية معلومات قد تؤدي إلى إدانته، باعتباره حق وثيق الصلة بمبدأ أنّ الأصل في الإنسان البراءة الذي يعتبر أحد مقومات المحاكمة العادلة، إذ لأيّ شخص متهم بارتكاب جريمة جنائية الحق في التزام الصمت و عدم المساهمة في تجريم نفسه⁽¹⁾، و هما معيارين دوليين معترف بهما عموماً و يمثلان أساساً لمفهوم الإجراءات العادلة من خلال توفير الحماية للمتهم ضد تعرضه لإكراه غير لائق من السلطات، و هي حصانة تكفل تجنب إساءة تطبيق الأحكام العادلة، و يسري هذا الحق على جميع أنواع الجرائم الجنائية بغض النظر عن مدى خطورتها⁽²⁾، و في جميع مراحل الدعوى العمومية ابتداء من سماع الضبطية لتصريحات المتهم⁽³⁾.

و نظراً لأهميته فقد حرصت بعض الدول على إضفاء الطابع الدستوري على هذا الضمان الإجرائي، إذ ينص التعديل الخامس من الدستور الفيدرالي الأمريكي على أنه "لا

المتهم الإجابة فإنّ تصرفه يكون محل تقدير المحكمة بالإضافة إلى باقي الأدلة التي جمعت دون اعتبار الصمت كدليل على الإدانة"، و من ضمن توصيات المؤتمر الدولي السادس لقانون العقوبات المنعقد في روما سنة 1954 "لا يجبر المتهم على الإجابة و من باب أولى لا يكره عليها فهو حر في اختيار الطريق الذي يسلكه و يراه محققاً لمصلحته" و في المؤتمر الدولي الذي نظّمته اللجنة الدولية لرجال القانون في أثينا في يونيو سنة 1955 قرّرت لجنة القانون الجنائي أنّ المتهم يستطيع أن يرفض الإجابة أمام الشرطة و سلطة الإتهام و يطلب سماعه بواسطة القاضي و لا يجوز للمحكمة أن تجبره على الكلام" و في الحلقة الدراسية التي نظمتها الأمم المتحدة لدراسة حماية حقوق الإنسان أثناء الإجراءات الجزائية و التي انعقدت في فيينا سنة 1960 أجمع الأعضاء على أنّ للمتهم ان يرفض الإجابة و لا يؤثر هذا الرفض على قرار الإدانة و قد أوصت لجنة حقوق الإنسان بهيئة الأمم المتحدة سنة 1962 بأنّه "لا يجبر أحد على الشهادة ضد نفسه و يجب قبل سؤال أو استجواب كل شخص مقبوض عليه أو محبوس أن يحاط علماً بحقه في الصمت".

لمزيد من التفصيل حول هذه المسألة راجع: سامي صادق الملا، إعراف المتهم، الطبعة الثانية، دار النهضة العربية، مصر، 1975، ص 203 و ما بعدها.

(1) CEDH, Arrêt Funke c. La France du 25 février 1993, Série A, n° 256-A, § 44.

(2) CEDH, Arrêt Saunders c. Royaume-Uni, du 17 décembre 1996, n° 19187/91, §45.

(3) مما جاء في هذا القرار "على الرغم من عدم النص صراحة على حق المتهم في الصمت أثناء استجواب الشرطة له، و خلال المحاكمة في الاتفاقية الأوروبية لحقوق الإنسان و حرياته الأساسية لعام 1950 إلا أنّ هذا الحق يعتبر متضمناً في مبدأ عدم جواز الإكراه على الإعراف بالذنب".

CEDH, Arrêt John Murray c. Royaume-Uni, 8 février 1996, n° 18731/91, §45

يمكن إجبار أيّ شخص في الدّعى الجزائية على أن يشهد ضد نفسه"، في حين إكتفت بقية الدول في النّص عليه ضمن تشريعاتها الإجرائية.

ففي الجزائر مثلا على الرّغم من عدم وجود نص صريح يقرّر حق المتّهم في الصّمت، إلّا أنّ هذا الحق يستفاد ضمنا من نص المادة 114 فقرة 5 من قانون الإجراءات الجزائية التي ورد فيها "و يتعيّن أن يذكر بمحضر التّحقيق أنّ المتّهم قد نبّه إلى أنّه حرّ في عدم الإدلاء بأيّ تصريح"، و ذات الحكم نجده في المادة 116 من قانون الإجراءات الجزائية الفرنسي، و بالرغم من النص على هذا الضباط الاجرائي في القانون كحق من حقوق المتهم فان القضاء وسع من مفهومه بحيث يستلزم تحت طائلة البطلان أن يتم إعلام المتّهم و تبلغه بحقه في الصمت و عدم الإجابة على الأسئلة التي تطرح عليه قبل مباشرة التّحقيق معه، تأمينا لحقه في عدم تجريم الذات بشكل كلي⁽¹⁾.

و إذا إنتقلنا من العموم إلى الخصوص، من القواعد الإجرائية التّقليدية إلى القواعد الإجرائية الجنائية المعلوماتية لوجدنا أنّ مبدأ عدم إتهام الشّخص لذاته يضع حدودا قويّة في حفظ حق المتّهم في الصّمت و عدم جواز جبره على التّعاون الفعّال في التّحقيقات المتعلّقة بجريمته، ففي المجر فإنّ المتّهم لا يكون مكرها على إثبات براءته، و في مستهل إستجوابه يجب أن يكون متنبّها إلى أنّه غير مجبر على الإدلاء بأيّ بيان، و بمقدوره أن يرفض الإجابة على الأسئلة أثناء الإستجواب، و ذلك يعني بوضوح أنّ المشتبه فيه أو المتّهم لا يكون مجبرا على طبع سجلات الحاسب أو الإمداد بالأكواد أو كلمات السرّ⁽²⁾.

كما أنّ مشروع قانون الإجراءات الجنائية في بولندا يقرّر في المادة 63 على أنّ المشتبه فيه أو المتّهم لا يمكن إكراهه على تقديم مطبوعات الحاسب أو كشف الشّفرات السّرية، و تحرص الإجراءات الجنائية البولندية بشدّة على حق المتّهم في رفض أيّة إيضاحات، و هذا الرّفص لا يمكن أن يقابل بأيّ إجراء قسري و لا أن يتمّ تفسيره إضرارا بالمتّهم⁽³⁾.

(1) Cass. Crim, 14 mai 2019, n° 19-81.408, Bull. crim. 2019, n° 92.

(2) هلاي عبد الله أحمد، تفتيش نظم الحاسب الآلي و ضمانات المتّهم المعلوماتي، المرجع السّابق، ص 207.

(3) المرجع نفسه، ص 208.

و قد سبق للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات و أن أولى أهمية لهذا الحق فأوصى " بأنه لا يُجبر أحد على أن يساعد بأسلوب إيجابي مباشرة أو بطريقة غير مباشرة في اتهام نفسه جنائياً، المتهم له الحق في الصمت و صمته لا يستخدم ضده"⁽¹⁾.
الواقع أنّ دراسة مختلف الأحكام الصادرة عن المحكمة الأوروبية لحقوق الإنسان يلحظ عدم وجود معايير واضحة يتبين من خلالها نطاق هذا الحق إزاء سلطة الدولة في إلزام المتهم على البوح بالأرقام السرية لفك التشفير المحيط بملفاته الرقمية، و يعدّ الحكم الصادر عن هذه الجهة القضائية في قضية **Saunders v. the United Kingdom** أبرز مثال على ذلك، حيث أشارت المحكمة إلى أنّ استخدام الأدلة التي تمّ الحصول عليها بالإكراه ينطوي على انتهاك لأحكام الإتفاقية، و أنّ الحق في عدم تجريم النفس هو حق أساسي في إحترام إرادة المتهم في إلزام الصمت، غير أنّ نطاق الحق في الصمت لا يشمل استخدام المواد التي يمكن الحصول عليها من المتهم من خلال استخدام الصّلاحيات الإلزامية المخولة للسلطات الإجرائية، و التي لها وجود مستقلّ عن إرادة المشتبه فيه، مثلها مثل الوثائق التي تمّ الحصول عليها عملاً بأمر قضائي، أو عينات الدّم و عينات البول و عينات من الأنسجة الجسدية لغرض إختبار الحمض النووي ADN⁽²⁾.

و يبدو أنّ قرار المحكمة الأوروبية لحقوق الإنسان كان له تأثير بارز على القضاء الإنجليزي حيث قضت محكمة الإستئناف و ليز في قضية **R v S** أنّ طلب الحصول على معلومات فك التشفير مسألة مستقلة تنفصل عن إرادة المتهم، و من ثم فهي لا ترى عدم نزاهة الأدلة المعلوماتية متى أجبر المتهم على البوح بالأرقام السرية الخاصة بنظامه المعلوماتي⁽³⁾.

(1) XVe Congrès international de droit pénal (Rio de Janeiro, Brésil, du 4 au 10 septembre 1994), Revue Internationale de Droit Pénale, 1-2 ème trimestres Editions ERES, Paris 1995, p 32-33.

(2)CEDH, Arrêt SAUNDERS v. UNITED KINGDOM du 17 December 1996, Série A, n° 19187/91 § 69. " The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere, it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing."

(3)**R. v S** [2008] EWCA Crim 2177 (09 October 2008).citing Choo, Andrew, Compelling the Provision of Information: The Privilege Against Self-Incrimination as a Human Right ,Warwick School of Law Research Paper , University London, V10,2010, p 5.

و في هذه القضية طعن المتهّم بحكم الإدانة الصادر بحقه لمخالفته أحكام قانون تنظيم الصّلاحيات التّحقيقية لسنة 2000، و ذلك بامتناعه عن الكشف عن مفاتيح فك التّشفير الخاص بالملفات المخزّنة على حاسوبه الشّخصي على سند من القول أنّ طلب الكشف عن مفاتيح فك التّشفير يشكّل إنتهاكا لحق الإنسان في عدم تجريم نفسه و الحق في الصّمت.

و ردّت محكمة الإستئناف الإنجليزيّة الطّعن تأسيسا على أنّ مفاتيح فك التّشفير و التي تمكن من الولوج إلى المعطيات المحمية مثل المعلومات ذاتها تتفصل عن إرادة المتهّم و أضافت المحكمة " بذات الطريقة التي تشكل من خلالها عينة الدم أو عينة البول التي يتقدم بها سائق المركبة " حقيقة مستقلة عن السائق، و التي تفضي إلى الكشف على أنّ مستوى الكحول الذي تعاطاه هذا الأخير قد تجاوز الحد المسموح به أم لا، فإنّ أجهزة الحاسوب هي الأخرى سواء أكانت تحتوي على بيانات مُجرمة أم بريئة فإنّ معرفة الكلمات السّرية التي تسمح بالولوج إلى هذه الأنظمة المعلوماتية هي حقيقة مستقلة عن محتويات الأجهزة ذاتها... باختصار، على الرّغم من أنّ وسائل التّفاد إلى البيانات يشملها الحق في عدم تجريم الذات، فإنّ معرفة السلطات لمفاتيح فك التّشفير لا تتطوي على انتهاك لهذا الحق، إلّا إذا كانت هذه الكلمات السّرية بحد مواد مُجرمة، أمّا في الأحوال الأخرى التي تكون فيها الكلمات السّرية بريئة أو محايدة غير مرتبطة بالمواد المُجرّمة فإنّ معرفة وسائل الوصول إليها لا يشكل انتهاكا لهذا الحق " (1).

إلّا أنّنا نبدي قدرا من التحفظ حيال هذا الموقف القضائي، ففي اعتقادنا فإنّ هذا القضاء ليس صحيحا في جميع السّياقات، فممارسة أيّ إكراه على المتهّم لحمله على التّصريح بالأرقام السّرية للولوج إلى أنظمتها المعلوماتية أو تجريم فعل الصّمت في هذه الحالة يعتبر فعلا منافيا لحريّات الفرد و لحق المتهّم في عدم تجريم نفسه، أمّا إذا تمكّنت المحكمة من الوصول إلى البيانات السّرية (التّشفير) عن طريق أمر بالتسليم إلى مزوّد الخدمة فإنّ الوضع في هذه الحالة يختلف لانعدام عنصر الإكراه على إرادة المتهّم.

(¹) R. v S [2008] EWCA Crim 2177 (09 October 2008) " In much the same way that a blood or urine sample provided by a car driver is a fact independent of the driver, which may or may not reveal that his alcohol level exceeds the permitted maximum, whether the defendants' computers contain incriminating material or not, the keys to them are and remain an independent factIn short, although the defendants' knowledge of the means of access to the data may engage the privilege against self-incrimination, it would only do so if the data itself ... contains incriminating material. If that data was neutral or innocent, the knowledge of the means of access to it would similarly be either neutral or innocent ."

لذا نرى أنه لا يمكن أن تبرّر أهميّة المصلحة العامة التدابير التي تخلّ بجوهر حقوق الدفاع بما في ذلك عدم تجريم الذات، و لا يمكن الإعتماد على المصلحة العامة في تبرير إستخدام الإجابات التي تمّ الحصول عليها إجباريا في أيّ تحقيق غير قضائي لتجريم المتهمين⁽¹⁾، فللمتهم الحق في إلتزام الصّمت دون جواز تأويل هذا الصّمت ضده⁽²⁾، فإن كانت محاربة الجريمة و الكشف عن مرتكبيها سعي نبيل، إلّا أنّ تحقيق هذا المسعى عن طريق إجراءات مشبوهة و ملطّخة بإهدار الكرامة الإنسانية، في الحقيقة يعدّ سلوكا مشينا تأباه الشرائع القويمة.

و من هنا فإنّ نزاهة الدليل المعلوماتي تستلزم عدم قبول دليل يكون التفتيش عنه قد تمّ بطريقة منافية للأخلاق، فحرية القاضي في الإثبات الجنائي لا تعني أن يجري التفتيش عن الدليل بأيّ طريقة كانت، بل إنّ هذا التفتيش مقيد باحترام "حقوق الدفاع" من جهة، و "قيم العدالة" و "أخلاقياتها" من جهة أخرى، فالدليل المعلوماتي المتحصل عليه من إكراه هو دليل تمّ الحصول عليه على حساب "قيم العدالة" و "أخلاقياتها" و "مقتضيات الحفاظ على الكرامة البشرية" للمتهم و حقه في الدفاع، و هو بهذا الوصف إجراء مخالف لمبدأ الأمانة و غير مقبول في الإثبات الجنائي، و يعتبر من قبيل الإكراه التعذيب النفسي أو البدني و التهديد و الوعيد و وثوب الكلب البوليسي على المتهم مما يجعله يرتاع من هجوم الكلب عليه من الإصابات التي أحدثها بجسده، و يعتبر في حكم الإكراه الحصول على البيانات بعد إستجواب مرهق أو نتيجة إستجواب تمّ في ظروف شاقة أو مضنية⁽³⁾.

لذا نرى أنه لا يجوز ممارسة أيّ مظهر من مظاهر الإكراه على المتهم لأجل حمله على البوح بالأرقام السرية لأجل فك التشفير أو حمله على طباعة بعض البيانات الرقمية سواء الإكراه المادي كالتعذيب أو بعض الوسائل الحديثة التي تتعارض مع حصانة النفس و الضمير كالتتويم المغناطيسي و التحليل النفسي التخديري و غيرها، و إلّا إعتبر ذلك مساسا

(1) Conseil de l'Europe/Cour européenne des droits de l'homme, Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p37 , disponible sur www.echr.coe.int (consulté le 12/11/2019).

(2) la Directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, art. 7.5, J.O.U.E., L 65 du 11 mars 2016, p 8.

(3) جلول شيتور، ضمانات تقييد الحرية الفردية، أطروحة دكتوراه، كلية الحقوق، جامعة بسكرة، 2006، ص 153.

بمبدأ النزاهة، و هذا المسلك إنتقده بيكاريا على أساس أنه يؤدي إلى نتائج غريبة فمن غير المنطقي أن يكون المجرم في وضع أحسن حال من البريء لأنّ الثاني يعترف بالجريمة تحت وطأة التعذيب فتقرّر إدانته، أمّا الأول فإنّه يختار بين ألم التعذيب و ألم العقوبة التي يستحقها فيختار الألم الأول لأنّه أخف لديه من ألم العقاب فيصمّم على الإنكار و ينجو من العقوبة⁽¹⁾.

و هكذا فإنّه و بدل التفكير في الأساس الذي يبرّر الأخذ بهذه الإجراءات القسرية المناهضة لحقوق الأفراد و حياتهم، فإنّه يقع على الدولة العمل على تأهيل السلطات الإجرائية للتمكن من تجاوز العقوبات التقنيّة التي يفرضها المجرم بدل محاربة الجريمة بجريمة أخرى، و هذا يحملنا على دعوة المشرّع إلى إستحداث نص يقّر صراحة هذا الحق مؤداه "للمتهم الحق في الصمت، و لا يجوز إجباره على أن يساعد بأسلوب إيجابي مباشرة أو غير مباشرة في تجريم نفسه، و لا يمكن تفسير ممارسة هذا الحق بمثابة قرينة ضده، و كلّ دليل يتمّ تحصيله بالمخالفة لهذا الضمان الإجرائي يعتبر باطل و عديم الأثر".

(ج) - حضر تفتيش النظام المعلوماتي للأنثى بغير الإستعانة بأنثى

لما كانت الخصومة الجنائية تتطلّب ضمان حقوق المتهم و حرّياته و ليس مجرد مباشرة إجراءات جمع الأدلّة لإثبات حق الدولة في العقاب، فإنّه يتعيّن على القاضي أن يتأكد أولاً من نزاهة الدليل و لا يحول دون ذلك أن يكون الدليل صارخا في مظهره واضحا في دلالاته على إدانة المتهم ما دام مشبوها ملطخا بإهدار محارم القانون⁽²⁾، أو الأخلاق و الآداب العامة السائدة في المحيط الإجتماعي، لأنّه في كثير من الأحيان قد تتطابق عدم نزاهة الأدلّة مع عدم المشروعية الأخلاقية و أبرز مثال على ذلك تفتيش الأنثى بغير الإستعانة بأنثى.

إنّ هذا الحظر يجد له أساسا في الآداب العامة، و القيم الخلقية المستقرّة في ضمير الجماعة التي توجب صيانة عرض المرأة و كرامتها، و يتعلّق بتنفيذ التفتيش بالنسبة للأنثى، فرغم أنّ الدراسات أسهبت و استفاضت في التطرق إلي هذا الضابط الإجرائي الأخلاقي في معرض التفتيش التقليدي، إلاّ أنّه لا توجد أي دراسة - في حدود البحث الذي أجريناه -

(¹) حول الأدلّة الجنائية الناجمة عن الإكراه راجع: محمد زكي أبو عامر، المرجع السابق، ص 119، سامي صادق الملا، المرجع السابق، ص 104 و ما بعدها.

(²) أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، المرجع السابق، ص 468.

تتعرض إلى هذا الضابط الإجرائي في سياق التفتيش المعلوماتي، و ليس المقصود هنا وجوب التقييد بهذه القاعدة بمفهوم مادي في صورة أن يتم تنفيذ التفتيش عن وسائط التخزين الرقمية بمعرفة أنثى متى كان المتهم من جنس أنثى، منعا من تحسس جسمها، لأنّ الخطورة الأولى من التفتيش (مرحلة التفتيش المادي) بكافة الفروض التي يمكن تصورها تخضع للقواعد التقليدية، و إنّما المقصود وجوب تنفيذ التفتيش المعلوماتي للنظام الخاص بالأنثى عن طريق أنثى أي خضوع مرحلة التحليل الرقمي لهذا الضمان.

حيث أنّه لا خلاف بين الفقه و القضاء على أنّ كلّ تفتيش لشخص الأنثى دون ندب أنثى لتنفيذ التفتيش يعدّ باطلا⁽¹⁾، و الحكمة من ذلك هو صيانة عرض المرأة و احترامها لحياتها و كرامتها، لذا فإنّ كل تفتيش يتمّ بالمخالفة لهذه القاعدة المتصلة بالنظام العام لا يرتب البطلان فحسب، بل يقيم المسؤولية الجزائية للقائم بالتفتيش عن جريمة هناك العرض⁽²⁾.

فهذا الضابط مقصور على إجراء التفتيش ذاته في مواضع تعتبر من عورات المرأة أي الحالات التي يستطيل فيها التفتيش شخص المرأة، بحثا عن الدعامات الإلكترونية بتحسس ملابسها و أعضاء جسمها، و يجري التساؤل في ضوء ذلك فيما إذا كان تفتيش النظم المعلوماتية العائدة للأنثى المتهمة يمكن أن يؤدي إلى المساس بعورتها و خدش حياتها أم لا؟

(1) تنص المادة 46 من قانون الإجراءات الجنائية المصري على أنّه "إذا كان المتهم أنثى و يجب أن يكون التفتيش بمعرفة أنثى يندبها لذلك مأمور الضبط القضائي". و مراد القانون من إشتراط تفتيش أنثى بمعرفة أنثى عندما يكون مكان التفتيش من المواضع الجسمانية التي لا يجوز لرجل الضبط القضائي الإطلاع عليها و مشاهدتها هو الحفاظ على عورات المرأة التي تخدم حياءها إذا مُست. و لما كان ما قام به الضابط من إمساكه باليد اليسرى للمطعون ضدها و جذبها عنوة من صدرها إذ كانت تخفي فيه المخدر ينطوي بلا شك على مساس بصدر المرأة الذي يعتبر من العورات لديها لما يقتضيه ذلك بالضرورة من ملامسة هذا الجزء الحساس من جسمها. و من ثمّ فإنّ الحكم المطعون فيه إذ قضى بقبول الدّفع ببطلان تفتيش المطعون ضدها للأسباب السائغة التي أوردتها يكون قد طبّق القانون تطبيقاً سليماً). الطعن رقم 698 لسنة 34 جلسة 16/11/1964 مشار إليه لدى منى جاسم الكواري، المرجع السابق، ص 130.

(2) تنص المادة 1/335 من قانون العقوبات الجزائري "يعاقب بالسجن المؤقت من خمس إلى عشر سنوات كل من ارتكب فعلا مخلا بالحياء ضد إنسان ذكرا كان أو أنثى بغير عنف أو شرع في ذلك" و نلاحظ أنّ النسخة الفرنسية استعملت مصطلح *Attentat a la pudeur* التي تقابل هناك العرض في اللغة العربية و هو الأصح لأنّ جريمة الفعل المخل بالحياء نظّمته المادة 333 من قانون العقوبات. و قد ورد خطأ في النص الاصلي بالعربية، بغير عنف و الأصح هو بالعنف، أنظر : عبد الله أزهايبة، المرجع السابق، ص 278.

قدّمنا عند الحديث عن تقسيمات الأدلة المعلوماتية إلى أنّه من الضروري التمييز بين ثلاثة أنواع من المعلومات، المضمون الفعلي للاتصالات الإلكترونية، و بيانات حركة المرور، و بيانات المشتركين، و توصلنا إلى أنّ بيانات المحتوى تبعث على توقعات متميّزة من الخصوصية، لأنّها تؤدي إلى كشف مباشر و صريح لخصوصيات الأفراد و عوراتهم، و لما كانت الحكمة من قاعدة حظر تفتيش الأنثى بغير أنثى هي صون عرض المرأة و حياتها و لو كانت موضع إتهام، فإنّ هذا الحكم يدور مع علّته وجودا و عدما.

و لا مرأى أنّ النّظام المعلوماتي للمرأة يحتوي من حيث بيانات المضمون على معلومات تكشف في غالب الأحيان المواضيع الجسمانية للأنثى التي تعدّ من العورات التي لا يجوز للقائم بتنفيذ الإذن الإطلاع عليها و مشاهدتها لما في ذلك من خدش لحياء الأنثى، و الأمثلة الدارجة في هذا الإطار تلك الاتصالات التي تجريها المرأة مع أفراد أسرتها و أقاربها باستعمال خاصية الاتصالات المرئية و الصوتية عبر الأنترنت أو تصوير بعض وقائع الحياة اليومية التي تعيشها في محيط أسرتها دون ستر عورتها و دون حرج أو خوف باعتبار أنّ "مكان التصوير" أو "مكان التخزين" أو "نظام الإتصال" يفترض أن يجعل بياناتها في مأمن عن فضول الغير و إطلاعهم، و لا شك أنّ مشاهدة بيانات المحتوى من هذه الفئة من غير أنثى يتحقّق معه إنتهاك للأداب العامة خاصة بالنسبة للمجتمع العربي و الإسلامي المحافظ.

و تطبيقا للقاعدة الفقهية التي مؤداها أنّ "الحكم يدور مع علّته"، فإنّه حيثما توافرت العلة ثبت الحكم، و بناء عليه نرى ضرورة أن يتمّ تفتيش النّظام المعلوماتي الخاص بالأنثى بواسطة أنثى، لأنّ إطلاع القائم بالتفتيش على معلومات تكشف عورة المرأة قد يتمّ بقدر لا يقل إنتهاكا لحرمتها و حياتها عن مشاهدة جسم المرأة عند تفتيش جسدها، بل إنّ الحالة الأولى في اعتقادنا أخطر مساسا بالأداب العامة، من حيث نطاق كمّية المعلومات و من حيث النّطاق الزمني لتنفيذ التفتيش و الذي يتمّ في غياب هذه الأخيرة بمخابر التحليل الحاسوبي الشرعي، إذ قد يتناول القائم بالتفتيش إلى تكرار الإطلاع على ما يكشف عورتها، فيستطيل بنظره إلى ما يجاوز الغاية من التفتيش بجعله شاملا، دون أن يكون عليه رقيب في ذلك سوى ضميره.

أمّا خلو التفتيش الذي يطال النّظام المعلوماتي من المساس بعورة الأنثى فهو أمر نادر لأنّ الأنظمة المعلوماتية تفيض خصوصيتها عن خصوصية غرفة نوم هذه الأخيرة، كما أنّه من الناحية الفنية لا يمكن قصر تطبيق هذه القاعدة فقط على الحالات التي

يستهدف فيها التفتيش بيانات المحتوى العائدة للمتهم دون بقية البيانات، لأنه يستحيل فرز بيانات المحتوى عند ضبطها بحكم إختلاط البيانات و تشابكها، مع حجم هائل من البيانات. و هذا القصور التشريعي ليس حال التشريع الجزائري فقط، بل إنّ كافة التشريعات العربية لم تتطرق إلى وجوب تطبيق هذه القاعدة حال تنفيذ التفتيش عن الدليل المعلوماتي، و كان أولى بالمشرّع من باب سد الدرائع أن يقرّر بطلان التفتيش المعلوماتي الذي يكون محله نظام معلوماتي تابع للأنثى إذا تمّ تنفيذه دون الإستعانة بالأنثى، فهذا الفعل يعتبر في نظرنا مخالف لمبدأ الأمانة في الإثبات الجنائي و ينطوي على هدر للأخلاق.

إن هذا القيد يرتبط بكرامة العدالة لأنّ السعي إلى الحقيقة ليس كافيا إذا لم يلازمه الضمير الإنساني الذي يستلهم اعتبارات الأخلاق و يحميها، لذا نرى الإصرار على سن هذه القاعدة⁽¹⁾، و يكون مؤداها في اعتقادنا كما يلي "إذا كان المتهم أنثى و يجب أن يتمّ تفتيش أنظمتها المعلوماتية المحددة في الإذن القضائي بمعرفة أنثى تندب خصيصا لذلك تحت طائلة بطلان التفتيش مع استبعاد ما يسفر عنه من أدلة، و ذلك دون الإخلال بالعقوبات التي يمكن أن توقع على القائم بتنفيذ التفتيش وفقا ما هو مقرر بالقانون".

المبحث الثاني

حرية القاضي الجنائي في تقدير الدليل المعلوماتي المستمد من التفتيش

إذا كنا فيما سبق قد إنتهينا إلى أنّ القاعدة التي تحكم مقبولية الأدلة المعلوماتية المستمدة من التفتيش هي حرية القاضي من حيث المبدأ في قبول أيّ دليل يتقدّم به الخصوم متى إستوفى معايير المشروعية و النزاهة، فإنّ قبول هذه الأدلة يقرّر للقاضي سلطة تقدير قيمتها الإثباتية للحكم بما يثبت حقوق العدالة عموما، سواء حق المجتمع في الإدانة أو حقه في ثبوت براءة المتهم، و منطقيا و نحن نناقش مبدأ حرية القاضي في تقدير القيمة الإقناعية لهذا الدليل أن نبدأ بمناقشة ماهية هذا المبدأ (مطلب أول)، و نستطرد ذلك ببيان القيود الواردة عليه (مطلب ثاني).

(1) و هذه النتيجة تقودنا إلى القول بوجود تعديل أحكام المرسوم الرئاسي رقم 19-172 المؤرخ في 06 جوان 2019 يحدّد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها و تنظيمها و كفاءات سيرها، بالنص صراحة على أن تتكوّن تشكيلة المديرية التقنية المنصوص عليها بالمواد 11، 12، 13، 14 من خبراء إناث يناط بهم القيام تفتيش الأنظمة المعلوماتية المتعلقة بالأنثى، بناء على المهام المنوطة بهذه المديرية.

المطلب الأول: مبدأ حرية القاضي الجنائي في الإقتناع

إنّ مبدأ حرية القاضي الجنائي في تقدير القيمة الإقناعية لكلّ دليل يعرض عليه إنّما هو في حقيقته نتيجة من نتائج حرية الإثبات الجنائي بشكل عام، غير أنّ هذه الحرية قد تتراجع أمام قطعية الدليل المعلوماتي بحكم طبيعته العلمية، لذا يقع لزاماً علينا أن نعالج مضمون هذا المبدأ (فرع أول)، و نستعرض أثر الطبيعة العلمية لهذا الدليل في تكوين عقيدة القاضي و اقتناعه الذاتي (فرع ثاني).

الفرع الأول: مضمون حرية القاضي الجنائي في الإقتناع

لا مرأ أنّ الهدف الأسمى الذي ترنو إليه القاعدة الإجرائية هو الوصول إلى الحقيقة سواء بإدانة المتهم أو براءته، و ليس في وسع السلطة القضائية تحقيق هذا المسعى سوى عن طريق التوصل للإقتناع الذاتي للقاضي الذي ينظر الدعوى، ذلك ما يتطلب منا أن نحدّد المقصود بهذا المبدأ سواء في الفقه (أولاً)، و القانون (ثانياً)، و القضاء (ثالثاً).

أولاً: التّحديد الفقهي لمبدأ الإقتناع الذاتي للقاضي الجزائي

تتحد كلّ الإجراءات أو التشريعات الجنائية المختلفة في أن يصيب القاضي الحقيقة في إصدار الحكم الجنائي و لن يتمكّن من ذلك ما لم يتوفّر لديه اليقين الجازم، فاليقين إذن هو أساس العدالة الإنسانية و مصدر ثقة المواطنين⁽¹⁾، و من هنا فإنّ العملية القضائية التي يجريها القاضي الجنائي غايتها النهائية التّوصل إلى الحقيقة الواقعية، فكلّ نشاط أو جهد ذهني خلال إجراء هذه العملية يبغى من ورائها التّوصل إلى حقيقة الوقائع كما حدثت في العالم الخارجي لا كما يتصوّرها الخصوم، و لا يمكن أن تظهر الحقيقة الواقعية إلاّ بعد البحث عنها و ثبوتها بالأدلة، فإذا وصل القاضي إلى ذهنية إستجمع فيها كافة ملامح و عناصر الحقيقة الواقعية و استقرّت في وجدانه و ارتاح ضميره للصّورة الذهنية التي تكوّنت و استقرّت لديه عن تلك الحقيقة فهنا يمكن القول أنّ القاضي وصل إلى حد الإقتناع⁽²⁾.

لقد تناول الكثير من الفقهاء مسألة تحديد ماهية مبدأ الإقتناع الذاتي للقاضي الجنائي و جميعها لا يتعدّى القول بأنّه التّعبير عن عملية ذهنية وجدانية بمنطق و عقل و نتیجتها الجرم و اليقين، فالبعض يعرفه بكونه "التّقدير الحر المسبّب لعناصر الإثبات في الدعوى و هو

(1) هلاي عبد الله أحمد، المرجع السابق، ص 436.

(2) حازم محمد حنفي عثمان، المرجع السابق، ص 249.

البديل عن نظام الأدلة القانونية⁽¹⁾، و منهم من عرفه "بأنه تلك الحالة الذهنية و النفسية أو ذلك المظهر الذي يوضح وصول القاضي باقتناعه لدرجة اليقين بحقيقة واقعة لم تحدث تحت بصره"⁽²⁾.

و صفوة القول إذن أنّ الإقتناع الحر للقاضي لا معنى له أكثر من أنه "سلطة القاضي و واجبه في أن يستمدّ من أيّ مصدر وسيلة إثبات الوقائع و أن يقدرها دون أن يقيددها أو قيدها"⁽³⁾، فهذا المبدأ يعبر ببساطة عن الأثر الذي يحدثه في الذهن الدليل القاطع و الواضح و اليقين القاطع الذي يصل حتّى أعماق النفس⁽⁴⁾، لذا يكفي القضاء لكي يحكم بإدانة المتهم أن يقرّر إقتناعه بالإثم، فهو يركّز إنتباهه لفحص الظروف و يغفل إهتماماته و آرائه الشخصية، مع إستبعاد كل الأفكار المسبقة لديه، و يعمل مصادر الفهم و الإدراك في عقله و روحه و إدراكه و ضميره⁽⁵⁾.

و مما سبق نرى أنّ الفقه يكاد يجمع في تعريفه لمبدأ الإقتناع على أنه عملية ذهنية و نفسية و وجدانية تنشأ لدى القضائي أثناء ممارسة العملية الإثباتية بصدد خصومة جنائية من مراحلها الأولى و حتّى نهايتها، إذن فالإقتناع الشّخصي للقاضي الجنائي يمثّل الأثر النهائي لعملية الإستدلال و الإستنتاج تتلاقى فيها جميع الأدلة القضائية المطروحة بالدّعى و التي تصبّ في بوتقة واحدة هي ذاتية القاضي، دعائمها العقل و المنطق و الوجدان الحي للقاضي

(1) مفيدة سويدان، المرجع السابق، ص 175.

(2) محمد سيد حسن محمد، ضوابط سلطة القاضي في تقدير الأدلة، دراسة مقارنة بالشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 2008، ص 36.

(3) جيوفاني ليوني، مبدأ حزية الإقتناع و المشاكل المرتبطة به، ترجمة رمسيس بهنام، مجلة القانون و الإقتصاد، العدد الثالث، السنة الرابعة و الثلاثون، سبتمبر 1964، ص 934. مذكور لدى مستاري عادل، المنطق القضائي و دوره في سلامة الحكم الجزائي، رسالة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة بسكرة، 2011، ص 42.

(4) J. ZOLLINGER, L'intime conviction du juge dans l'innocence, Travaux de l'Institut de criminologie de Paris, 1977, p 33.

(5) Gorphe (François), La méthode générale d'examen critique des preuves, Revue de science criminelle et de droit pénal comparé, 1947, n° 1, p 69.

حيث يقوم فيها بالتمحيص و التقدير و الموازنة بين أكثر الأدلة عمقا أو إتصالا بالحقيقة فيحدّد الحكم على أساسها⁽¹⁾.

إنّ مبدأ حرّية القاضي في الإقتناع في سماحه للقاضي بأن يؤسّس إقتناعه و يبني حكمه على أية بيّنة أو قرينة يرتاح لها، يساهم و لا شك إلى حد كبير في تحقيق مصلحة المجتمع في التجريم لأنّه يزيل كثيرا من الصّعوبات العملية التي تحيط بعملية البحث عن الأدلة و إقامتها أمام القضاء، فالنيابة العامة التي تتحمّل عبء الإثبات ليست ملزمة بتقديم أدلة بعينها حتّى يقتنع القاضي طالما كانت كلّ عناصر الإثبات قابلة لأن تحقّق هذا الإقتناع، لكن الحقيقة أن مبدأ حرية القاضي في الإقتناع لم يهدر كلية مصلحة المتّهم و الموقف المتميّز الذي توفّره له قرينة البراءة، لأنّ هذه الحرّية الممنوحة للقاضي تخضع لعدد من القواعد القانونية و هو ما يشكل بطريقة غير مباشرة ضمانا للمتّهم و احتراماً لنتائج قرينة البراءة، و تجد هذه القواعد مصدرها فيما ما هو مشروط من أنّ إقتناع القاضي بالإدانة ينبغي أن يكون عقليا لا عاطفيا و على درجة معيّنة من اليقين الذي يخلو من الشكّ و الذي يعبر عنه القضاء بالجزم و اليقين⁽²⁾.

فهذا المبدأ يقوم على دعامين، الأولى تتمثّل في حرّية القاضي في الإستعانة بأيّ دليل يكون لازماً لتكوين قناعته، و الثانية تتمثّل في حرّيته في تقدير عناصر الإثبات تقديراً فعليا، فمبدأ حرّية القاضي في الإقتناع ينبسط على فكرتي: "قبول الدليل" و "تقييمه"، و بما يفيد أنّ مدلول "حرّية الإقتناع" هو بعينه مدلول "حرّية الإثبات"، و إنّ نظام الأدلة المعنوية و "الإقتناع القضائي" ماهي إلاّ تسميات لمبدأ واحد صادقة على حرّية القاضي في الإقتناع⁽³⁾.

ثانيا: المفهوم القانوني لمبدأ الإقتناع الذاتي للقاضي الجزائي

مبدأ قضاء القاضي بمحض إقتناعه بمفهومه المستقرّ عليه في مختلف الشرائع الجنائية يعني أنّ القاضي الجنائي يحكم في الدّعى المنظورة أمامه وفقا لما تكوّنت لديه من عقيدة و بحسب إقتناعه، و أن يقدرّ بكامل حرّية قيمة الأدلة، بمعنى آخر أن يكون للقاضي كامل

(1) مفيدة سويدان، المرجع السابق، ص 178.

(2) احمد زكي أبو عامر، المرجع السابق، ص 132.

(3) بدر الدين يونس، سلطة القاضي الجنائي في تقدير الدليل الجنائي، أطروحة دكتوراه، كلية الحقوق جامعة قسنطينة، 2014، ص 61.

الحرية في أن يستمد إقتناعه من أي دليل يطمئن إليه من الأدلة التي تقدّم في الدعوى دون أن يتقيّد في تكوين إقتناعه بدليل معيّن، إلا إذا نصّ القانون على غير ذلك⁽¹⁾.

فالقاضي الجنائي يقوم بتحقيق في الدعوى بالأسلوب الذي يراه موصلا للحقيقة، دون أن يتقيّد في اتباع وسائل إثبات معينة، إذ أنّ هذا المبدأ يعطيه الحرية الكاملة في تقدير الأدلة المتصلة بالدعوى فهو يقدر قيمة الدليل و يستطيع أن يستخلص منه إدانة المتهم أو برائته تبعا لإقتناعه الشخصي الداخلي، و لا يتدخل القانون في تحديد قيمة الأدلة أو قوتها في الإثبات، فكلّ الأدلة عند القانون سواء و لها نفس القوة الإقناعية، فله أن يأخذ بدليل دون الآخر و له أن يأخذ بجزء من الدليل و يطرح الجزء الآخر، و له أيضا أن يعزز دليلا معينا بقرينة أو بأكثر⁽²⁾.

لقد تمّ التعبير لأوّل مرة على مبدأ حرية القاضي في الإقتناع بموجب المادة 342 من قانون التّحقيقات الجنائية الفرنسي القديم، من خلال العبارات التي تتلى على مسامع المحلفين بمناسبة المداولات التي تخصّ إتهام شخص معيّن، ثمّ تم إقراره مجدداً بمقتضى المادة 353 من قانون الإجراءات الجزائية الذي جاء بعد إلغاء قانون تحقيق الجنايات بموجب قانون 25 نوفمبر 1941⁽³⁾.

و أخذ المشرّع الفرنسي بتعدّد الأساس القانوني لمبدأ حرية الإقتناع، فجعل مناط هذا التعدّد هو نوع المحكمة التي يطبّق أمامها هذا المبدأ⁽⁴⁾، فالمادة 427 من قانون الإجراءات الجزائية تتعلّق بتطبيق هذا المبدأ أمام محكمة الجنح، و التي تنصّ ما لم يرد نص مخالف يمكن إثبات الجرائم بكلّ الطّرق، و يحكم القاضي بناء على إقتناعه الشخصي، و أمّا المادة 436 من نفس القانون فتخصّ محكمة المخالفات، و التي تحيل إلى تطبيق المادة 427 المشار إليها أعلاه، أمّا المادة 353 من نفس القانون، فتتعلّق أساسا بمحكمة الجنايات و هي تنصّ "لا يطلب القانون من القضاة حسابا بالأدلة التي إقتنعوا بها و لا يفرض قاعدة خاصة

(1) فرج إبراهيم العدوي عبده، سلطة القاضي الجنائي في تقدير الأدلة، أطروحة دكتوراه، كلية الحقوق جامعة القاهرة، 1995، ص 25.

(2) المرجع نفسه، ص 26.

(3) إنّ إلغاء المادة 342 من قانون التّحقيقات الجنائية بمقتضى القانون 25 نوفمبر 1941 لم يحل دون تطبيق حكمها لأنّ هذه المادة نقلت حرفيا إلى المادة 353 من قانون الإجراءات الجزائية الحالي الصادر سنة 1958.

(4) بدر الدين يونس، المرجع السابق، ص 65.

تتعلق بتمام و كفاية دليل ما، و إنما يفرض عليهم أن يتساءلوا في صمت و تدبر و أن يبحثوا في صدق ضمائرهم أي تأثير قد أحدثته الأدلة الراجعة ضد المتهم و وسائل دفاعه...⁽¹⁾.

و فيما يخص القانون الجزائري فإنّ المشرع نص في الفقرة الأولى من المادة 212 من قانون الإجراءات الجزائية على أنه "يجوز إثبات الجرائم بأيّ طريق من طرق الإثبات ما عدا الأحوال التي ينص في القانون على غير ذلك و للقاضي أن يصدر حكمه تبعا لاقتناعه الخاص"، و النص على هذا المبدأ و في هذا الموضع بالذات من طرف المشرع الجزائري يجعل منه قاعدة عامّة تصلح أساسا له بالنسبة لجميع المحاكم و الجهات القضائية⁽²⁾. و مع ذلك نجد أنّ المشرع الجزائري أكد على هذا المبدأ مجددا أمام محكمة الجنايات بموجب المادة 307 من قانون الإجراءات الجزائية و التي هي في الأصل مستوحاة من المادة 353 من قانون الإجراءات الجزائية الفرنسي⁽³⁾.

الحقيقة أنّ مبدأ الإقتناع القضائي لم يقتصر على التشريعات اللاتينية فحسب بل يمتدّ أيضا إلى التشريعات الإنجلوأمريكية مع اختلاف طفيف في الصياغة فهي لا تعرف تعبير "الإقتناع الذاتي للقاضي الجنائي" و أنّها تستخدم ذات النظام القانوني بتعبير آخر و هو "ثبوت الإدانة بعيدا عن أيّ شك مقبول" **Proof beyond a reasonable doubt**⁽⁴⁾.

(1) L'Article 353 du CPP dispose que ; "La loi ne demande pas compte aux juges des moyens par lesquels ils se sont convaincus, elle ne leur prescrit pas de règles desquelles ils doivent faire particulièrement dépendre la plénitude et la suffisance d'une preuve ; elle leur prescrit de s'interroger eux-mêmes dans le silence et le recueillement et de chercher, dans la sincérité de leur conscience, quelle impression ont faite, sur leur raison, les preuves rapportées contre l'accusé, et les moyens de sa défense. La loi ne leur fait que cette seule question, qui renferme toute la mesure de leurs devoirs : " Avez-vous une intime conviction ? ". "

(2) بدر الدين يونس، المرجع السابق، ص 66.

(3) تنص المادة 307 من قانون الإجراءات الجزائية الجزائري على أنه : " يتلو الرئيس قبل مغادرة المحكمة قاعة الجلسة التعليمات الآتية التي تعلق فضلا عن ذلك بحروف كبيرة في أظهر مكان من غرفة المدولة: « إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين إقتناعهم، و لا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، و لكنه يأمرهم أن يسألوا أنفسهم في صمت و تدبر، و أن يبحثوا بإخلاص ضمائرهم في أيّ تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم و أوجه الدفاع عنها و لم يضع لهم القانون سوى هذا السؤال الذي يتضمّن كلّ نطاق واجباتهم: هل لديكم إقتناع شخصي؟ ». "

(4) John SPENCER, La preuve en procédure pénale, droit anglais, RIDP, V 63, 1er et 2eme trim, 1992, p 101.

و من هذا المنطلق فإنّ حجية الأدلة المعلوماتية المستمدة من التفتيش لا تثير صعوبات لمدى حرية تقديم هذه الأدلة لإثبات الجرائم سواء التقليدية أو المعلوماتية، و لا لمدى حرية القاضي الجنائي في تقدير هذه الأدلة ذات الطبيعة الخاصة باعتبارها أدلة إثبات في المواد الجنائية، و في فرنسا مشكلة حجية الأدلة المعلوماتية على مستوى القانون الجنائي ليست ملحة أو عاجلة في نظر الفقهاء، فالأساس هو حرية القاضي في تقدير هذه الأدلة، و يدرس الفقه الفرنسي هذه الحجية تحت نطاق قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية مثل أجهزة التصوير، و أجهزة التسجيل و أجهزة التتبع، و قد قضت محكمة النقض الفرنسية: "إنّ أجهزة التسجيل الممغنطة التي تكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي"⁽¹⁾.

حقيقة الأمر أنّ معظم التشريعات اللاتينية بما فيها التشريع الفرنسي و البلجيكي و الجزائري قد أبتت على هذا المبدأ كقاعدة عامة تنطبق على جميع الأدلة، و بالتالي لم تورد قيمة إقناعية معينة للدليل المعلوماتي المستمد من التفتيش الجنائي بل شأنه شأن باقي الأدلة، بحيث تخضع الأدلة المعلوماتية لحرية القاضي في الإقتناع الذاتي، حيث يكون بمقدوره أن يطرح مثل هذه الأدلة- رغم قطعيتها من الناحية العلمية- ذلك عندما يجد أنّ الدليل المعلوماتي لا يتسق منطقياً مع ظروف الواقعة وملابساتها⁽²⁾.

و إذا كان هذا حال التشريعات المقارنة بما فيها التشريع الجزائري، فإنّ التشريعات العربية لها موقف مغاير، إذ و رغم تبنيها صراحة لمبدأ حرية القاضي في تقدير قيمة الدليل الجنائي فما إطمأن إليه أخذ به، و ما لم يطمئن إليه أعرض عنه، دون أن يسأل حساباً عن ذلك في تشريعاتها التقليدية (قانون الإجراءات الجنائية)، إلا أنّها أفردت نصوصاً خاصة تطبيقاً لهذا المبدأ على الدليل الجنائي المعلوماتي المستمد من التفتيش.

حيث تنصّ المادة 24 من المرسوم التشريعي السوري رقم 17 لسنة 2012 المتعلق بتطبيق أحكام قانون التواصل على الشبكة و مكافحة الجريمة المعلوماتية على ما يلي: "حجية الدليل الرقمي: (أ) يعود للمحكمة تقدير قيمة الدليل الرقمي شريطة تحقق مايلي: 1- أن تكون الأجهزة الحاسوبية أو المنظومات المعلوماتية المستمد منها هذا الدليل تعمل على نحو سليم. 2- ألاّ يطرأ على الدليل المقدم إلى المحكمة أيّ تغيير خلال مدة حفظه (ب) يعدّ

(1) هلاي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص ص 721-722.

الدليل الرقمي المقدم إلى المحكمة مستجماً للشّروطين الواردين في الفقرة (أ) من هذه المادة ما لم يثبت العكس".

و نفس الموقف نلمسه لدى المشرّع المصري، حيث جاء بالمادة 11 من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات ما يلي: "في الأدلة الرقمية: يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدّات أو الوسائط أو الدّعامات الإلكترونية، أو النّظام المعلوماتي أو من برامج الحاسب، أو من أيّ وسيلة لتقنية المعلومات نفس قيمة و حجية الأدلة الجنائية المادية في الإثبات الجنائي، متى توافرت بها الشّروط الفنيّة الواردة باللائحة التنفيذية".

و هو المبدأ الذي أكّد عليه المشرّع اللبناني بموجب المادة 22 من القانون رقم 81 لسنة 2018 و المتعلّق بالمعاملات الإلكترونية و البيانات ذات الطّابع الشّخصي حيث نصّت على أنّه "يعود للمحكمة تقدير الدليل الرقمي أو المعلوماتي و حجبيته في الإثبات، و يشترط أن لا يكون قد تعرّض لأيّ تغيير خلال عملية ضبطه أو حفظه أو تحليله".

ثالثاً: التّحديد القضائي لمبدأ الإقتناع الدّاتي للقاضي الجزائي

إنّ مبدأ الإقتناع الدّاتي للقاضي الجنائي يعتبر قضاء مستقرّ في عقيدة المحكمة العليا الجزائرية فقد أوردت في أحد قراراتها "حيث أنّه من المقرّر قانوناً في باب تقدير كفاية أو تمام أدلة الإثبات التي يستند عليها قضاة الموضوع في المادة الجزائية لتكوين إقتناعهم، أنّ المسألة قد حسمها نص المادة 212 من قانون الإجراءات الجزائية التي أجازت إثبات الجرائم كقاعدة عامة بأيّ طريق من طرق الإثبات ما لم يوجد نص مخالف، و سمحت للقاضي بأن يصدر حكمه تبعاً لإقتناعه الخاص، شريطة أن يبني قراره على الأدلة المقدّمة له في معرض المرافعات و التي حصلت مناقشتها في الجلسة، فمحكمة الموضوع لها كامل الصّلاحيات للموازنة بين الحجج و تقدير أدلة الدّعوى و الأخذ بما تطمئن إليه ما دامت تستند على أسباب سائغة تؤدي إلى النتيجة التي إنتهت إليها"⁽¹⁾.

أمّا محكمة النقض المصرية فقد عبّرت على هذا المبدأ الهام في الشرائع الحديثة بقولها "إنّ أساس الأحكام الجنائية إنّما هو حرّية قاضي الموضوع في تقدير الأدلة القائمة في

(1) قرار صادر عن المحكمة العليا الجزائرية بتاريخ 2010/02/04 عن غرفة الجرح و المخالفات طعن رقم 530382 مشار إليه لدى بدر الدّين يونس، المرجع السّابق، ص 77.

الدّعى فما دام يبيّن من حكمه أنّه لم يقض بالبراءة إلّا بعد أن ألمّ بتلك الأدلّة و وزنها فلم يقتنع وجدانه بصحتها فلا يجوز مصادرتها في اعتقاده، و لا المجادلة في حكمه أمام محكمة النّقض، كما أنّه لا يحكم بالإدانة إلّا إذا إطمأن ضميره إليها، بشرط أن يكون الإطمئنان مستمداً من أدلّة قائمة في الدّعى يصحّ في العقل أن تؤدي إلى ما إقتنع به القاضي، و ما دام الأمر كذلك فلا تجوز المجادلة في حكمه أمام محكمة النّقض⁽¹⁾.

وقد أكّدت محكمة النّقض الفرنسية على تمسكها بهذا المبدأ في باب الأدلّة العلمية بشكل عام⁽²⁾، و بطبيعة الحال بما فيها الأدلّة المعلوماتيّة، حتّى في الأحوال التي يتمّ فيها الحصول على الأدلّة بطريق غير مشروعة من قبل طرف خاص، حيث أكّدت هذه الأخيرة على هذه السّابقة القضائية بخصوص الأدلّة المعلوماتيّة المستمدة من التفتيش الجنائي، مشيرة إلى أنّه لا يوجد في القانون ما يمنع المحكمة من اعتماد دليل تمّ الحصول عليه بطريقة غير عادلة من قبل الأفراد، فوفقاً للمادة 427 من قانون الإجراءات الجزائية تتمتع المحكمة بالسلطان المطلق في تقدير القيمة الإقناعية للدلائل المعروض عليها⁽³⁾.

كما قرّرت هذه المحكمة أنّ القاضي الجنائي حر في أن يستمدّ عقيدته من أيّ مصدر يشاء ما لم يقيد القانون بدليل معين، فله الإستدلال على إتيان جريمة الإغتصاب بالقوّة من القرائن المتسببة من الأدلّة المعلوماتيّة، كذلك التي أثبتت تحديد الموقع الجغرافي للمتّهم لحظة إرتكاب الجريمة و تواجده بمسرحها و أيضاً تطابق تصريحات الضّحية مع الدليل حين صرّحت بإقدام المتّهم على غلق الهاتف فترة تنفيذ الجريمة و توصّل الخبرة إلى الجرم بذلك⁽⁴⁾.

(1) الطّعن رقم 179 لسنة 44 جلسة 1993/12/14 مشار إليه لدى فرج إبراهيم العدوي عبده، المرجع السّابق، ص28.

(2) Cass Crim, 11 juin 2002, pourvoi n° 01-85.559, Bull. Crim. 2002, n° 131.

(3) Cass crim. 27 janvier 2010, no 09-83.395, Bull. Crim ,2010, n° 16 « Attendu qu'en cet état, et dès lors qu'aucune disposition légale ne permet aux juges répressifs d'écarter des moyens de preuve remis par un particulier aux services d'enquête, au seul motif qu'ils auraient été obtenus de façon illicite ou déloyale et qu'il leur appartient seulement, en application de l'article 427 du code de procédure pénale, d'en apprécier la valeur probante, après les avoir soumis à la discussion contradictoire, la cour d'appel a justifié sa décision ; ».

(4) تتلخّص وقائع القضية في توجيه الإتهام للسيد MX بجريمة الإغتصاب في حق الضّحية Y بالعنف و الإكراه مؤكّدة في شكواها أنّها قدمت إلى فرنسا بغرض متابعة دراستها في الفنون التشكيلية و أقامت في إحدى العمارات، و

و خلاصة ما تقدّم أنّ قبول الأدلة المعلوماتية المستمدة من التفتيش الجنائي تعتبر من أهمّ المنافع التي جلبها مبدأ الإقتناع الذاتي للقاضي الجنائي لنظام الإثبات الجنائي الحديث، فالأدلة العلمية بطبيعتها لا تقبل الخضوع لأيّ قيود بل ينبغي أن يترك الأمر في تقديرها لمحض إقتناع القاضي خصوصا و أنّها كثيرا ما تتضارب مع باقي أدلة الدعوى و ذلك فضلا عن إحتمال آراء المختصّين في شأنها⁽¹⁾.

الفرع الثاني: أثر القيمة العلمية للدليل المعلوماتي على إقتناع القاضي الجنائي

إنّ حجية الأدلة المعلوماتية المستمدة من التفتيش، هي قوتها الإستدلالية على صدق نسبة الفعل إلى شخص معيّن أو كذبه، أو هي قيمة ما يتمتّع به الدليل، بأنواعه المختلفة الورقية و الإلكترونية و المصغّرات الفيلمية، من قوّة إستدلالية في كشف الحقيقة و إقتناع القاضي بعناصرها التي تمتاز بالقطعية بحكم طابعها العلمي، غير أنّ الإشكالية المثارة في هذا الصدد تتعلّق بمدى تقيّد القاضي بهذا الدليل في أحكامه و بالتالي يخرج الدليل العلمي عن مبدأ قناعة القاضي إلى كونه دليل قانوني يقيّد القاضي؟

عند الحديث عن تأثيرات الإثبات العلمي على إقتناع القاضي لا بد من الإشارة إلى أنّ إقتناع القاضي في الأمور الجنائية يهيمن على مختلف وسائل الإثبات، بما فيها تلك القائمة

في أحد الأيام و أثناء سيرها في المرر المؤدي إلى المرسم الخاص بالجاني قام بإمسакها بالقوّة، و حقّق فعله الجرمي بعد رفع صوت الموسيقى منعا من سماع الجيران لصراخها بالتجدة، و قد أكّد أحد الجيران لسماعه صوت إستغاثة و لكنّه لم يستطع تحديد مصدرها مؤكدا وجود شكوى سابقة ضده بهذا الخصوص، و بعد عرض المجني عليها على الطيبب الشرعي أكّد هذا الأخير عدم إصابتها بجروح في جسدها غير أنّه أكّد وجود عملية وطأ بالقوّة و العنف، إلّا أنّ المتهم تمسك بإنكاره لما نسب إليه و ادعى بأنّه بتاريخ الواقعة لم يكن موجودا بالمرسم و الخاص به من الساعة 12 ظهرا إلى غاية الساعة 9 مساء في حين أكّدت الضّحية أنّ المتهم أغلق هاتفه عقب إدخالها إلى شقته بالقوّة فأمرت المحكمة بتفتيش هاتفه من خلال خبير تقني و كذلك أمرت مزوّد الخدمة بتمكين المحكمة من الدليل المعلوماتي المتعلّق بتحديد الموقع الجغرافي الخاص بالمتهم بتاريخ الواقعة و بالفعل أكّد هذا الدليل و أنّ المتهم كان متواجدا بهذه الشّقة زمن الوقائع بحكم أنّ الهاتف كان في مسرح الواقعة و ليس في المكان الذي صرّح به المتهم كما أكّد الخبير على واقعة أخرى بدّدت الشكّ و هي أنّ الهاتف فعلا كان مغلقا في تلك الفترة الزّمنية التي استغرقها تنفيذ الركن المادي للجريمة، أين إنهار المتهم عند مواجهته بهذه الأدلة و غير من تصريحاته، و من هنا كونت المحكمة عقيدتها بالإستناد إلى هذه الأدلة المعلوماتية إعمالا لمبدأ الإقتناع الشّخصي للقاضي الجزائي.

Cass Crim,5 août 2015, n° 15-82.830 Non publié au bulletin disponible a la dresse

<https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000031084331> (consulté le 10-01-2020).

(¹) هلاي عبد الله أحمد، حجّية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 39.

على أساس من العلم و التي إستلزمها ضرورة مواكبة التطور العلمي المستمر الذي يميّز به العصر الحديث، فالهدف من إقتناع القاضي الجنائي هو حماية العدالة من الشطط و الهوى، و بذات الوقت يصون القاضي نفسه من الآثار المترتبة على إستخدام الوسائل العلمية في الإثبات، لذا فإن إقتناع القاضي يشكّل السيادة التامة بعد تكوينه بحرية⁽¹⁾. و هكذا فإنّ الدليل المعلوماتي المستمد من التفتيش إنّما هو مجرد دليل لا تختلف قيمته و لا تزيد حجّته عن سواه من الأدلة، و هو لا يحضى أمام القضاء بقوة حاسمة في الإثبات، و على هذا الأساس يصحّ للقاضي أن يؤسس إقتناعه على الدليل المعلوماتي كما يصحّ له أن يهدره تبعاً لاطمئنانه، و بالتالي لا يجوز إلزامه بالإقتناع بهذا النوع من الأدلة و لو لم يكن في الدعوى أدلة سواه⁽²⁾، و أيّا كانت درجة خطورة الجريمة موضوع المتابعة الجنائية.

على أنّه ينبغي التّعرض إلى مسألة جوهرية، و هي تتعلّق بالطبيعة العلمية لهذا الدليل التي تجعله يميّز بالموضوعية و الحياد و الكفاءة، الأمر الذي يجعل إقتناع القاضي الجنائي أكثر جزماً و يقيناً، حيث يساعده على التقليل من الأخطاء القضائية و الإقتراب إلى العدالة بخطوات أوسع و التّوصل إلى درجة أكبر نحو الحقيقة⁽³⁾، و تلك هي السمات التي جعلت بعضاً من الفقه يعنقد بأنّه بمقدار إتساع الأدلة العلمية و من بينها الأدلة المعلوماتية، بمقدار ما يكون إنكماش و تضاول دور القاضي الجنائي في تقدير القيمة الإقناعية لها، خاصة أمام نقص خبرة القضاء من الناحية التّقنية و بالتالي تصبح مهمّة القضاء شبه آلية، حيث يكون الدور الأكبر للخبرة التي تسيطر على العملية الإثباتية، و لم يبقَ لدى القاضي سوى الإذعان لرأي الخبير دون أيّ تقدير من جانبه⁽⁴⁾.

و هذا الرّأي الفقهي و على وجاهته، إلّا أنّنا نعارضه فالدليل المعلوماتي يخضع إلى تقدير القاضي و بالتالي إقتناعه و في هذا الخصوص ينبغي أن نميّز بين أمرين: القيمة العلمية القاطعة للدليل المعلوماتي. ثانياً، الظروف و الملابسات التي وجد فيها هذا الدليل.

(1) محمد بركات فارس الطراونة، حجية الدليل العلمي في الإثبات الجنائي، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 2015، ص 61-61.

(2) نضال ياسين الحاج حمو، دور الدليل الإلكتروني في الإثبات الجنائي، مجلة جامعة تكريت للعلوم القانونية و السياسية، مجلد 1 السنة 5 العدد 19، 2013، ص 212.

(3) مفيدة سويدان، المرجع السابق، ص 163.

(4) عائشة بن قارة، المرجع السابق، ص 248.

فتقدير القاضي الجنائي لا يتناول القيمة العلمية للدليل المعلوماتي، و ذلك لأن قيمة الدليل تقوم على أسس علمية دقيقة، و بالتالي لا حرية للقاضي في مناقشة الحقائق العلمية الثابتة و التي تمتاز بالثقة في مصادرها العلمية، الأمر الذي يصعب معه بل قد يستحيل على القاضي أن يتناولها بالفحص و التقدير، أما الظروف و الملابسات التي وجد فيها الدليل فإنها تدخل في نطاق تقديره، فهي من صميم وظيفته القضائية بحيث يكون في مقدوره أن يطرح مثل هذا الدليل إذا تبين أنه لا يتفق مع ظروف الواقعة و ملابساتها⁽¹⁾.

و على ذلك فإننا لا نذهب مع الإتجاهات الفقهية القائلة بأن نظام الأدلة العلمية يكون نظام المستقبل و سيحلّ الخبير محلّ القضاء فيكون الدور له و ليس للقاضي، فيجعل رأي الخبير هو الحاسم لإقتناع القاضي، لكننا نقول أن التطور العلمي في مجال الأدلة لا يتعارض مع سلطة القاضي الجنائي في تقديرها، بل إنّ هذه الأدلة ستكفل للقاضي وسائل فعالة في كشف الحقيقة، و أنه لا يمكن للخبير مهما كانت دقة نتائجه و موضوعيتها أن يحتلّ مكانة القاضي في إيجاد العدالة، و التي يستلزم إيجادها حسًا مختصًا لا يدركه غيره، و يتمّ هذا الحس من خلال التكوين العلمي و القضائي الرفيع و الذي تنهض به المؤسسات القانونية و القضائية، ليشكّل أساسا رصينا في التقدير السليم للأدلة و الذي من خلاله يصل إلى قراره العادل الذي يكون عنوانا للحقيقة⁽²⁾.

فمجرد توافر الدليل العلمي لا يعني أن القاضي ملزم بالحكم بموجبه مباشرة سواء بالإدانة أو البراءة دون بحث الظروف و الملابسات، فالدليل العلمي ليس آلية معدة لتقرير إقتناع القاضي بخصوص مسألة غير مؤكدة⁽³⁾، لأنّ الدليل الجنائي و إن كان عليما يخضع دائما لتقدير القاضي و من ثمّ فلا تثريب على القاضي في استخدام الوسائل العلمية لإرساء و توضيح الحقيقة و لتسهيل تكوين إقتناعه و بنائه على الجزم و اليقين، لأنّ الغاية الحقيقية للإثبات هي الكشف عن الحقيقة الواقعية بالقطع و اليقين بحكم المنطق و العقل⁽⁴⁾.

(1) هلاي عبد الله أحمد، المرجع السابق، ص 48.

(2) فاضل زيدان محمد، سلطة القاضي في تقدير الأدلة، دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر و التوزيع، الأردن، 2006، ص 155.

(3) عائشة بن قارة، المرجع السابق، ص 248.

(4) لذا يرى جانب من الفقه أنه من قبيل المغالطة أن نقول أننا أصبحنا في نطاق نظام إثبات جديد إذا ما وجدت أدلة ذات دقة أكبر، فالعلم قد أثر على الطبيعة الذاتية للدليل نفسه من حيث مدى صحته أو عدم صحته، لا على

واقع الأمر أنه و مع الهيمنة من قبل مبدأ الإقتناع القضائي على الأدلة المعلوماتية إلا أنه يظل لهذه الأخيرة أثرها على القاضي و التي تفرضها طبيعتها العلمية، و لهذا قضت محكمة النقض المصرية في قضاء مستقر لها أنّ " لمحكمة الموضوع كامل السّلطة في تقدير القوة التّدلّيلية لعناصر الدّعى المعروضة على بساط البحث، و هي الخبير الأعلى في كلّ ما تستطيع أن تفصل فيه بنفسها، إلاّ أنّه من المقرّر أنّه متى تعرّضت المحكمة لرأي الخبير الفني في مسألة فنية بحثة فإنّه يتعيّن عليها أن تستند في تفنيده إلى أسباب فنية تحمله و هي لا تستطيع في ذلك أن تحلّ محلّ الخبير فيها" (1).

و إذا كان ذلك الذي سلف كذلك، فإنّ الإمتداد الطّبيعي لهذه النّتيجة هو نتيجة أخرى مؤداها تراجع مبدأ "القاضي خبير الخبراء"، فالحقيقة أنّ مؤشرا في عمل الخبير التّقني يوحي

منهج الأخذ به أو عدم الأخذ به و لا على النّظام أو المبدأ المتعلّق بالإقتناع الدّاتي من حيث أبعاده و عدم الأخذ به، و ليس معنى توضيح الرّؤية للقاضي و تقريب عناصر اليقين بتقريب عناصر التّقدير و دقّتها أنّنا تخلينا على هذا النّظام باللّجوء إلى نظام آخر طالما ما زالت تحكمه نفس المبادئ الأصلية، و من باب المغالطة أن نقول أنّنا إذا أصبحنا بوضع يجعل الأمر فيه يتّسم بالموضوعية أو شبه الموضوعية أنّنا أصبحنا خارجين عن النّطاق الذي نحن به فإنّ وضوح الرّؤية معناها ثقة أكبر في التّقدير و يقين ثابت و عدالة واضحة و رضا من النّاس بالأحكام و حتّى المتهمين يعطيهم ذلك صورة تجعلهم مطمئنين إلى عدالة القضاء.

لمزيد من التّفصيل حول موضوع أثر الدّليل العلمي على مبدأ إقتناع القاضي الجنائي راجع: مفيدة سعد سويدان، المرجع السّابق، ص 167 و ما بعدها و أنظر أيضا، ضياء الدّين خليل، المرجع السّابق، ص 48 و ما بعدها.

(1) و قد تردّد هذا المبدأ في سابقة قضائية لمحكمة النقض المصرية فأوردت في أحد أحكامها "إذا كان الحكم قد أسس إدانة الطّاعن على ما قاله من أنّه "ظاهر من الإطّلاع على الأوراق أنّ موضع المؤاخذه في هذه الدّعى هو إصابة الرّأس وحدها التي نشأت عنها الوفاة إذ أنّ الإصابات الأخرى التي وجدت بالجسم لم تحدث إلاّ كدمات لا تتصل مطلقاً بواقعة الوفاة" ثم قال: "إنّه لا محلّ البتّة لتعلّق إبداء الرّأي فيما يختص بهذه الإصابة على معاينة الملابس" بحجّة أنّ المجني عليه كان حاصر الرّأس و أنّ الإرتجاج نشأ عن إصابة الرّأس بالضربة التي أحدثتها الطّاعن - إذ كان ذلك و كان الواضح من الحكم أيضاً أنّ الطّبيب الشرعي و هو الخبير الفني لم يبد رأيه في سبب الإرتجاج الذي نشأت عنه الوفاة و أرجأ ذلك إلى ما بعد معاينة ملابس المجني عليه، و أنّ الطّاعن تمسك باستدعاء الطّبيب لمناقشته في هذا الأمر فرفضت المحكمة، فهذا منها إخلال بحقّ الطّاعن في الدّفاع إذ هي برفضها هذا الطّلب قد أحلتّ نفسها محلّ الخبير الفني في مسألة فنية علّق الطّبيب نفسه رأيه فيها على معاينة الملابس، و هذا لا يجوز".

أنظر الطّعن رقم 165 لسنة 21 جلسة 14/05/1951 و العديد من التطبيقات القضائية مشار إليهما لدى: طه أحمد طه متولي، الدّليل العلمي و أثره في الإثبات الجنائي، رسالة دكتوراه، كلية الحقوق جامعة طنطا، مصر، 2007، ص 383 و ما بعدها.

بوجود تطوّر على درجة من الخطورة هنا ممثلاً في مدى إستجابة القضاء لعمل الخبير التّقني على النّحو الذي يحقّق إستفاضة في فهم عمل تكنولوجيا الإعلام و الإتصال، و على النّحو الذي يجعل الخبير موجّها للقاضي، سيما إزاء عدم وجود قواعد تشكّل مقياس عام يعتمد عليه في تقنيات الإعلام و الإتصال يمكن إدراكها بالعلم العام الذي يملكه كلّ شخص؟

و مثل هذا الأمر يخشاه علماء القانون و تردّدت فيه الآراء بحيث يمكن القول، على الرّغم من وجود أنصار بين إتجاه و آخر، إنّ من الصّعوبة بمكان اللّجوء إلى الخبير قصد الحصول على نتائج توجيهية لقاضي الموضوع، بل إنّ مثل هذا الأمر إنّ حدث يضع الخبير فعلا في مرتبة قاضي الدّعوى و هو الأمر الذي -إن لم يكن قد عزل دور القاضي الجنائي- فإنّه يجعل للدّعوى قاضيا آخر غير مرئي⁽¹⁾.

في اعتقادنا إنّ كثيرا من الفقه يخلط بين مسألة اقتناع القضائي بمسألة علمية ذات جانب معلوماتي، و بين يقينية القاضي بنسبة الجريمة للمتّمم بارتكابها، فالحقيقة العلمية الأولى و إنّ إتسمت بالثّبات و الإستقرار لأنّها مستمدّة من أصول علمية بحيث تنطبق في جميع الحالات المتشابهة إلاّ أنّها لا تعدو أن تكون مجرد قرينة، قد تعزّز الإتهام و قد تتجرّد من أيّ قيمة متى تعارضت مع المنطق و العقل في ضوء ظروف القضية و ملابساتها، فيظل القاضي خبير الخبراء و لو أمكننا قول ذلك، لجاز القول إنّ إستناد القاضي إلى شهادة الشّهود يجعل الشّاهد محل القاضي و ذلك قول غير صحيح على الإطلاق فكلّ دليل يخضع للتّقييم و التّقدير في سياق الطّروف و ما تكشف عنه الملابس، و هذا يؤدي بالّلزوم العقلي إلى التّأكيد على أنّ كلّ ما يتعلّق بمآل الدّعوى ينتهي عند قاضي الموضوع سواء إستند إلى رأي الخبير أو طرحه، و من ثمّ فإنّ نظام الإثبات لا يزال يدور في فلك الإقتناع الدّاتي للقاضي أو بالأحرى نظام الإقتناع الدّاتي العلمي و المعلوماتي.

(1) محمد أبو بكر بن يونس، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السّابق، ص 1042.

المطلب الثاني: القيود الواردة على حرية القاضي الجنائي في الإقتناع بالدليل المعلوماتي المستمد من التفتيش

إذا كان المبدأ هو حرية القاضي الجنائي في الإقتناع بالدليل المعلوماتي المستمد من التفتيش في تكوين عقيدته بإدانة المتهم أو ببراءته، فإن هذه الحرية في التقدير و التقييم لا تخضع للسلطان المطلق لقاضي الموضوع، بل إنها تخضع لمجموعة من القيود التي تجعل كم المظهرية في هذا المبدأ أكبر بكثير من الحقيقة، فالمنطق يفرض أن يكون الدليل يقينياً لا يعتريه الشك (الفرع الأول) و أن يخضع هذا الدليل لمناقشة الخصوم (فرع ثاني)، و أن يكون صادقا في مضمونه أي موثوقا فيه (فرع ثالث).

الفرع الأول: مبدأ يقينية الدليل المعلوماتي المستمد من التفتيش

إن الهدف الأساسي الذي ترنو إليه التشريعات الإجرائية المختلفة هو أن يصيب القاضي الحقيقة في حكمه سواء بالإدانة أو البراءة، و لذا يجب على القاضي قبل أن يحزر حكمه أن يكون قد وصل إلى الحقيقة المؤكدة، و هو لا يصل إلى هذه الحقيقة ما لم يتكون لديه يقين بحدوثها، لذا يتعين علينا تحديد مفهوم هذا القيد على حرية القاضي في تقدير الدليل المعلوماتي (أولاً)، و بيان الحدود التي يملئها على القاضي للإلتزام به (ثانياً).

أولاً: مفهوم اليقين القضائي

يعتبر "اليقين القضائي" وحدة أساس كل العدالة الإنسانية، فهو مصدر ثقة المواطنين في هذه العدالة، إذ بدون هذا اليقين لا يمكن إدراك الحقيقة، فالحقيقة القضائية لا يمكن التسليم بوجودها ما لم يكن اليقين بها قد أصبح موجوداً⁽¹⁾، و على هدى من تلك الفكرة يعرف اليقين في القانون بأنه "تلك الحالة الذهنية أو العقلية التي تؤكد وجود الحقيقة و لا يتوصل إلى هذه الصورة إلا بواسطة الإستنتاج، و الوصول إلى ذلك اليقين يتم عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال وقائع الدعوى، و ما يرتبه ذلك في ذهنه من تصورات ذات درجة عالية من التوكيد تستبعد إمكانية أي شك أو ريب في تجاه تلك المحصلة النهائية التي وصل إليها القضائي في حكمه"⁽²⁾.

(1) هلاي عبد الله أحمد، النظرية العامة للإثبات الجنائي، المرجع السابق، ص 398.

(2) إيمان محمد علي الجابري، يقين القاضي الجنائي، رسالة دكتوراه، كلية الحقوق جامعة الإسكندرية، مصر، 2002، ص 101.

فاليقين إذن يمثل حالة ذهنية أو عقلية لدى القاضي محدثة إنطباعاً عن كيفية حدوث تلك الواقعة الإجرامية، و يتوقف تكامل هذا اليقين في ضمير القاضي على قدرة الأدلة المطروحة على توصيل القاضي إلى هذه الدرجة من الإقتناع فإذا حدث ذلك يكون هناك تطابق لديه بين "حالة الذهن و العقل" مع "حالة الحقيقة و الواقع"⁽¹⁾. فاليقين القضائي إذن هو "إقتناع القاضي"، و الذي لا يعني أكثر من إذعان هذا الأخير للتسليم بثبوت الوقائع كما دونها حكمه ثبوتاً كافياً⁽²⁾، و من ثمّ فإنّ اليقين الذي يصل إليه القاضي ليس هو اليقين المطلق و إنّما هو اليقين النسبي القائم على الضمير و الذي يكون راشده العقل و المنطق، إذ أنّ كشف الحقيقة أمر غير أكيد بالنسبة لإمكانات البشر و ذلك فإنّ القاضي لا يقول أنا أعلن أنّ هذا المتهم مدان لأنّ هذه هي الحقيقة المطلقة، و إنّما يكتفي بالقول إنّه في ضميري و بحسب مكنون نفسي و بمقتضى إقتناعي الداخلي و اطمئناني أنا على يقين من إدانته⁽³⁾.

إنّ مفهوم الجزم و اليقين المتطلب لبناء الحكم له معنى قضائي يختلف عن معناه الفلسفي أو اللغوي، فما يجري عليه إجتماع الفقه و القضاء أنّ إقتناع القاضي بثبوت الوقائع ينبغي أن يصل إلى درجة الجزم و اليقين يحتاج إلى بعض التأمل لأنّ الحكم "بالثبوت" أي بالوجود يتأسس على أسباب إمّا شخصية إذا حملت "ذهناً" على التسليم بوقوع الحدث و تكون هذه الأسباب موضوعية إذا كان من شأنها أن تحمل "كلّ ذهن" على التسليم بوقوع الحدث. و حين يذعن المرء للتسليم بثبوت الوقائع، فإنّ إذعانه هذا يشكّل "رأياً" إذا استقام حكمه بثبوت الواقعة على أسباب محتملة فيكون هذا الحكم محصلة لأسباب قاصرة من الناحيتين الشخصية و الموضوعية و يدع لذلك مجالاً للتحرز لافتقاره إلى الإقتناع التام و استقامة الحكم بثبوت الوقائع على مجرد "الرأي" محذور في القانون الجنائي، لأنّ الرأى ليس إقتناعاً فهو قاصر على أحداثه حتّى لدى القاضي نفسه و إذا كان الرأى على هذا النحو مرفوضاً، فهل تحقيق اليقين ممكناً؟⁽⁴⁾

(1) محمد زكي أبو عامر، المرجع السابق، ص 8.

(2) رمزي رياض عوض، سلطة القاضي الجنائي في تقدير الأدلة، بدون رقم الطبعة، دار النهضة العربية، مصر، 2010، ص 17.

(3) فرج إبراهيم العدوي عبده، المرجع السابق، ص 63.

(4) الواقع أنّ اليقين حالة ذهنية تلتصق بالحقيقة دون أن تختلط بأيّ شك فهي من الناحية الشخصية تتعارض مع الشك و من الناحية الموضوعية فوق الجهل و الغلط، و درجة اليقين تختلف حسب المكنات المعطاة و اليقين المادي

الحقيقة أنّ نتائج هذا اليقين تتسم بالنسبية، و مع ذلك فإنّ اليقين المطلوب من العدالة البشرية هو اليقين المعقول فضمير القاضي العادل يملئ عليه أحكاما أساسها العقل و المنطق لأنها مجردة من الأهواء و المصالح الشخصية⁽¹⁾، فهذه الحرّية في التّقدير و الإقتناع ليس معناها أن يؤسّس القاضي إقتناعه على عواطفه أو حدسه، و إنّما هو إقتناع عقلي مصدره في العقل لا في العاطفة باعتباره عملا ذهنيا أو عقليا⁽²⁾، فهو ملزم ليس فقط بـ "الإقتناع" بل أيضا بـ "الإقناع" من خلال ضمانته تسبب الأحكام القضائية.

و في قضاء مستقر لها أكدت محكمة النقض الفرنسية أنّ حرّية القاضي في التّقدير لا يقصد بها حرّية القاضي في أن يؤسّس إقتناعه على هوى عواطفه أو حدسه العاطفي و إنّما هو إقتناع عقلي **Une Conviction De Raison** يجد مصدره في العقل لا في العاطفة باعتباره

هو الدّرجة القصوى فيه و هذه الدّرجة من اليقين برغم ندرة تعلّقها بالقاضي في صدد نزاع ما من شأنها أن تمنعه من تولي القضاء في النزاع إحتراما لمبدأ الموضوعية و بين الرّأي و اليقين يمكن أن يتأسّس الحكم بثبوت الوقائع على مجرد الإعتقاد و هو يستقيم على أسباب شخصية تحمل المرء على التّسليم بثبوتها، لكن هذه الأسباب لو نظرنا إليها من النّاحية الموضوعية لجاز أن تكون غير كافية لهذا التّسليم و هي درجة مرفوضة على القاضي للإحتمالية اللانهاية لها و لا يبقى بين الإعتقاد و اليقين سوى الإقتناع و هو التّسليم الناتج من قوة التّدليل أو التّسبب، هذا الإقتناع لقيامه على التّسبب و قبوله أمر شخصي- تصاحبه بالضرورة بعض الإحتمالية و يشكّل في أعلى درجاته اليقين القضائي بالمعنى الدّقيق، و على هذا الأساس فإنّ الإقتناع هو إذعان حاد للتّسليم بثبوت الوقائع ما تثبت ثبوتا كافيا فهو يمثّل المنطقة الوسط بين "الإعتقاد الذي يبنى على أسبابا شخصية"، و اليقين الذي يبنى على أسباب شخصية و موضوعية أي ينطلق من الإعتقاد إلى اليقين، فإقتناع القاضي هو في حقيقته إعتقاد يقوم أساسا على أسباب شخصية صحّت لديه لكنها لا تصحّ لدى غيره و هذا ما يفسّر الإكتفاء بالأغلبية في إصدار الأحكام لكنه يتفوق على الإعتقاد في استقامته على أدلة موضوعية تدنيه من اليقين لكنه ليس يقينا لاستقامته على تسبب و قبول التّسبب هو بالأكثر أمر شخصي لا يتسم بصرامة اليقين و هذا ما يفسّر إقتناع قاضي الموضوع كافيا لحمل محكمة النقض على الإقتناع هي الأخرى و من هنا و لأنّ هذا الإقتناع لا يجري في فلك قانوني يفلت هذا الإقتناع تماما من رقابة محكمة النقض و هذا ما يسلم به الفقه و القضاء.

لمزيد من التّفصيل حول الفارق بين الإقتناع و اليقين راجع : محمد زكي أبو عامر، شائبة الخطأ في الحكم الجنائي، محاولة فقهية و نظرية لإرساء نظرية عامة، بدون رقم الطّبعة، دار الجامعة الجديدة، مصر، 2011، ص 320 و ما بعدها. و أنظر أيضا إيمان محمد علي الجابري، المرجع السّابق ص 103 و ما بعدها.

(¹) RACHED, ALY , De l'intime conviction du juge, Vers une théorie scientifique de la preuve, thèse Faculté de droit Université de Paris, 1942, p 143.

مشار إليه لدى فرج إبراهيم العدوي عبده، المرجع السّابق، ص 64.

(²) رمزي رياض عوض، المرجع السّابق، ص 29.

عملا ذهنيا *Un Travail Intellectuel* يحصّله القاضي في صمت و خشوع و مناخ من الصدق و سلامة الطّوية⁽¹⁾. و خلاصة القول في ذلك أنّ حرّية القاضي الجنائي في الإعتدال على الدّليل لتكوين عقديته مقيد بوجوب أن يكون هذا الدّليل يقينيا و غير قابل للشك، لكن هل القاضي مقيد بهذا الشرط حتى في حال الحكم بالبراءة؟

ثانيا: حدود التزام القاضي بقاعدة يقينية الدّليل المعلوماتي المستمد من التفتيش

يؤسس إفتراض البراءة على الفطرة التي جُبل الإنسان عليها، فقد ولد حرا مبرءا من الخطيئة، و يفترض على امتداد مراحل حياته أنّ أصل البراءة لا زال كامنا فيه، فهذه الحقيقة هي يقين لا يمكن إثبات عكسه إلاّ بدليل معلوماتي جازم و قاطع في نسبة الجريمة إلى المتهم (أ)، أمّا إذا تأرجح هذا الإقتناع بين ثبوت التّهمة و عدم ثبوتها كان لزاما على القضائي صيانة الأصل الإثباتي القائم على إفتراض البراءة لأنّ مجرد الشك يفسّر لصالح المتهم (ب).

أ - إشتراط يقينية الدّليل المعلوماتي المستمد من التفتيش للقضاء بالإدانة

إستقرّ الفقه و القضاء على وجوب أن يبلغ إقتناع القاضي بالإدانة درجة من اليقين، و اليقين المطلوب عند الإقتناع ليس هو اليقين الشّخصي للقاضي و إنّما هو اليقين القضائي الذي يمكن أن يصل إليه الكافة لاستقامه على أدلة تحمل بذاتها معالم قوتها في الإقناع⁽²⁾، إلى درجة أن تستقرّ هذه القناعة فتتميّز بنوع من بالثبات و لو تغير القاضي⁽³⁾، إذ لا محلّ لدحض قرينة البراءة و افتراض عكسها إلاّ عندما يصل إقتناع القاضي إلى حد الجزم و اليقين فالمطلوب أن يبني القاضي عقيدته على أساس احتمالات ذات درجة عالية من التّقة لا يهزها أو ينقضها احتمال آخر، فالإدانة لا يمكن إقامتها بأيّ شكل على مجرد ظنون أو تخمينات⁽⁴⁾.

(1) cass crim 12 mai 1971. b 153

مشار إليه لدى محمد زكي أبو عامر، المرجع السابق، ص 134.

(2) ياسر الأمير فاروق، المرجع السابق، ص 692.

(3) تعبّر محكمة النقض المصرية عن هذه الدّرجة من القناعة بقولها "أن يكون الحكم مبنيًا على الجزم و اليقين من الواقع الذي يثبت بالدليل المعتبر و لا يؤسس على الظنّ و الإحتمال من المفروض و الإعتبارات المجردة " ياسر الأمير فاروق، المرجع السابق، ص 692.

(4) هلاي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 740.

و التّقيّد بهيكلّة حكم الإدانة على الدّليل المعلوماتي اليقيني يهدف إلى الإقتراب أكثر نحو الحقيقة الواقعية بحيث لا تقبل الشّكّ و أن تتعد عن الظّنون و التّخمينات، و يترتّب على ذلك أنّ جميع الأدلّة المعلوماتيّة بمختلف أنواعها من مخرجات ورقية أو أقراص مغناطيسية أو مصغّرات فيليمية تخضع لتقدير القاضي الجنائي و يجب أن يستتج منها الحقيقة بما يتفق مع اليقين و يبتعد عن الشّكّ و الإحتمال⁽¹⁾.

و قد حرصت المحكمة العليا على التّأكيد على هذا المبدأ في كثير من قراراتها فقضت بأنّ "الأصل في الإنسان البراءة حتّى تثبت إدانته، و قد تبنى دستور 1996 هذا المبدأ في نص المادة 45 منه، إذ نصّ أنّ كلّ شخص يعتبر بريئاً حتّى تثبت جهة نظامية إدانته مع كلّ الضّمّانات التي يتطلّبها القانون. و ترتيباً على ذلك فإنّ الأحكام و القرارات لا تبنى على الشّكّ و الافتراضات و إنّما على الجزم و اليقين"⁽²⁾.

و تفرّيعاً على هذا، فإنّ القول بأنّ القاضي الجنائي يملك حرّية تقدير الأدلّة وفقاً لمبدأ حرّية الإثبات و الإقتران ليس معناه أنّه يملك الحكم بالإدانة على غير أساس من التّثبت و التيقّن، ذلك أنّ أكثر ما تكون حالات فساد الإستدلال عندما يتسرّع القاضي و يجزم بثبوت الإدانة مؤسساً هذا الجزم على دليل أو أكثر غير مباشر أو على قرينة من القرائن إذا كان ذلك لا يؤدي إلى الجزم بالتّثبت بحكم الضّرورة أو اللّزوم العقلي بل يصحّ أن يحمل على أكثر من وجه⁽³⁾، و بطبيعة الحال فإنّ شرط يقينية الدّليل في القضاء بالإدانة شرط عام سواء كانت الأدلّة التي يستسقى منها هذا اليقين تقليدية أو مستحدثة كالدّليل المعلوماتي و اليقين الذي يعوّل عليه في هذا الشّأن هو ما يتولّد لدى القاضي بأنّ ما وصل إليه هو الحقيقة⁽⁴⁾.

لكن هذا لا يمنع القاضي من أن يؤسّس قضاءه بإدانة المتّهم على ترجيح فرض على آخر إذ أنّ شرط القطع و اليقين لا يتعارض مع إمكانية إفتراض صور مختلفة لحصول الواقعة و إدانة المتّهم على أيّ صورة من الصّور التي إفترضها الحكم، فهنا يكون إقتران

(1) محمد أحمد المنشاوي، المرجع السّابق، ص 542.

(2) مشار إليه لدى: مستاري عادل، المنطق القضائي و دوره في سلامة الحكم الجزائي، رسالة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر بسكرة، 2011، ص 68.

(3) هلاّلي عبد الله أحمد، النّظرية العامة للإثبات الجنائي، المرجع السّابق، ص 407.

(4) مفيدة سويدان، المرجع السّابق، ص 183.

القاضي بوقوع الجريمة و نسبتها إلى المتهم يقينياً، و لا يقدح في هذا اليقين أن تستخلص المحكمة من الأدلة من مجموعها و من الأوراق إحتتمالات متعدّدة لكيفية وقوع الجريمة طالما أنّ جميع الإحتتمالات تؤدي إلى إدانة المتهم، أمّا إذا كان هناك إحتتمال واحد يفيد البراءة فلا يجب على المحكمة الحكم بالإدانة و إلاّ كان ذلك خطأ منها⁽¹⁾.

و إذا كانت هذه الأحكام العامة هي التي تحكم اليقين في الأدلة الجنائية، فإنّ الأمر لا يختلف بالنسبة للأدلة المعلوماتية المستمدة من التفتيش، إذ يُشترط في الأدلة أن تكون غير قابلة للشك حتّى يمكن الحكم بالإدانة، ذلك أنّه لا مجال لدحض قرينة البراءة و افتراض عكسها إلاّ عندما يصل إقتناع القاضي إلى حد الجزم و اليقين⁽²⁾.

و يمكن التّوصل إلى ذلك من خلال ما يعرض من الأدلة المعلوماتية، و غيرها من الأشكال الإلكترونية التي تتوافر عن طريق الوصول المباشر، أو كانت مجرد عرض لهذه المخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به أو على الطّرفيات، و هكذا

(1) هلاي عبد الله أحمد، النظرية العامة للإثبات الجنائي، المرجع السابق، ص 408.

(2) و في هذا تقوق المحكمة الدستورية العليا في مصر "حيث إنّ أصل البراءة يمتدّ إلى كلّ فرد سواء أكان مشتبهاً فيه أو متّهماً باعتباره قاعدة أساسية في النظام الإتهامي أقرتها الشرائع جميعها لا لتكفل بموجبه حماية المذنبين، و إنّما لتندراً بمقتضاها العقوبة عن الفرد إذا كانت التهمة الموجهة إليه قد أحاطتها الشبهات بما يحول دون التيقن من مقارفة المتهم للواقعة الإجرامية، ذلك أنّ الإتهام الجنائي في ذاته لا يزحزح أصل البراءة الذي يلزم الفرد دوماً و لا يزيله سواء في مرحلة ما قبل المحاكمة أو أثناءها و على امتداد حلقاتها و أيّا كان الزّمن الذي تستغرقه إجراءاتها، و لا سبيل لدحض أصل البراءة بغير الأدلة التي تبلغ قوتها الإقناعية مبلغ الجرم و اليقين بما لا يدع مجالاً لمعقولا لشبهة إنتفاء التهمة، و بشرط أن تكون دلالتها قد إستقرت حقيقتها بحكم قضائي إستنفذ طرق الطعن فيه... و إنّما يؤسس افتراض البراءة على الفطرة التي جبل الإنسان عليها، فقد ولد حراً مبرراً من الخطيئة أو المعصية، و يفترض على امتداد مراحل حياته أنّ أصل البراءة لا زال كامناً فيه، مصاحباً له فيما يأتيه من أفعال، إلى أن تنقض المحكمة بقضاء حازم لا رجعة فيه هذا الافتراض على ضوء الأدلة التي تقدّمها النيابة العامة مثبتة بها الجريمة التي نسبتها إليه في كلّ ركن من أركانها، و بالنسبة إلى كلّ واقعة ضرورية لقيامها بما في ذلك القصد الجنائي بنوعيه إذا كان متطلباً فيها. و بغير ذلك لا ينهدم أصل البراءة إذ هو من الرّكائز التي يستند إليها مفهوم المحاكمة المنصفة التي كفلها الدستور، و يعكس قاعدة مبدئية تعتبر في ذاتها مستعصية على الجدل، واضحة وضوح الحقيقة ذاتها، تقتضيها الشريعة الإجرائية، و يعتبر إنفاذها مفترضا أولياً لإدارة العدالة الجنائية، و يتطلّبها الدستور لصون الحرّية الشخصية في مجالاتها الحيوية و ليقوّف من خلالها كلّ فرد الأمن في مواجهة التّحكم و التسلط، بما يحول دون اعتبار واقعة تقوم بها الجريمة ثابتة بغير دليل، و بما يرد المشرّع عن افتراض ثبوتها بقريضة قانونية تحكيمية ينشؤها...". المحكمة الدستورية المصرية العليا، الطعن رقم 25، السّنة القضائية 16، تاريخ الجلسة 1995/07/03، الصّفحة 67، الفقرة 26.

يستطيع القاضي من خلال ما يعرض عليه من مخرجات إلكترونية، و ما ينطبع في ذهنه من تصوّرات و احتمالات بالنسبة لها، أن يحدّد قوّتها الإستدلالية على صدق نسبة الجريمة إلى شخص معيّن من عدمه⁽¹⁾.

هكذا فإنّ القاضي يصل إلى يقينية الأدلة المعلوماتية المستمدة من التفتيش عن طريق نوعين من المعرفة، أولهما المعرفة الحسية التي تدركها الحواس من خلال معاينة هذه الأدلة و تفحصها، و ثانيها المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل و الإستنتاج من خلال الرّبط بين هذه الأدلة و الملابس التي أحاطت بها⁽²⁾.

و في إطار هذه الضوابط يمكن للقاضي أن يصل إلى يقينية الأدلة المعلوماتية المستمدة من التفتيش عن طريق المعرفة الحسية التي تدركها الحواس من خلال معاينته لهذه المخرجات و فحصها عن طريق المعرفة العقلية من خلال ما يقوم به من إستقراء و إستنتاج ليصل إلى الحقيقة التي يهدف إليها و يجب أن يصدر حكمه إستنادا إليها، و هذا الأمر على إطلاقه محل نظر حيث أنّه إذا توافر للبعض من القضاة الحس اليقيني بما تكشفه حواسه الوجدانية فالبعض الآخر ليس لديه هذه الملكة، الأمر الذي يصبح معه التشكيك في وجهة نظر إقتناع القاضي الجنائي بيقينية الدليل المعلوماتي محل إعتبار⁽³⁾.

و مجمل القول أنّ اليقين الذي يجب أن يبني القاضي عليه إقتناعه ليس اليقين المطلق و إنّما اليقين الذي يولّد في نفسه عقيدة لا يزحزحها إحتمال آخر على إدانة المتّهم، و في هذا تقول محكمة النقض المصرية " و لا يقدح في هذا اليقين أن تستخلص المحكمة من الأدلة في مجموعها و من الأوراق إحتتمالات متعدّدة لكيفية وقوع الجريمة كاملا أنّ جميع الإحتتمالات تؤدي إلى إدانة المتّهم"⁽⁴⁾.

(1) Erman Sahir, les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Turquie, Revue international de droit pénale, Editions ERES, Paris, 1993,p 624.

(2) محمد سيد حسن محمد، المرجع السابق، ص 82.

(3) محمد أحمد المنشاوي، المرجع السابق، 544.

(4) المرجع نفسه، نفس الموضوع.

(ب) - إستثناء حالة البراءة من شرط يقينية الدليل المعلوماتي المستمد من التفتيش

إنّ الأصل في الإنسان البراءة و هذا يقين، و من ثمّ فإنّه لا يزول إلاّ بيقين مثله أو أقوى منه⁽¹⁾، و يترتب على هذه النتيجة لزوم بلوغ الإقتناع بالإدانة درجة اليقين أنّه إذا لم يدرك القاضي هذه الدرجة من الإقتناع كان معنى ذلك أنّ إقتناعه يتأرجح بين ثبوت التهمة و مسؤولية المتهم عنها و بين عدم ثبوتها أو عدم مسؤولية المتهم عنها، و هذا الإقتناع المتأرجح يعني الشكّ في ثبوت التهمة و مسؤولية المتهم عنها و الشكّ يفسّر لصالح المتهم (in dubio pro reo) مما يستوجب على القاضي أن يحكم بالبراءة⁽²⁾.

ففي حالة عدم قدرة أدلة الإدانة على إحداث اليقين يترتب عليه إستمرار حالة البراءة التي يكفي لتأكيد وجودها مجرد الشكّ في ثبوت تلك الإدانة، و ذلك إتباعاً لمبدأ البراءة المسلّم بوجوده بداءة، فإذا كانت المحكمة لم تنته من الأدلة التي ذكرتها إلى الجزم بوقوع الجريمة من المتهم بل رجّحت وقوعها منه فحكمها بإدانته يكون خاطئاً واجبا نقضه⁽³⁾.

فبخلاف حكم الإدانة فالحكم بالبراءة هو مجرد تأكيد لمبدأ البراءة الذي يتمتع به الفرد منذ ميلاده، و لذلك فإنّه يكفي لتقريره مجرد التشكيك في وقوع ذلك الأمر العارض و المتمثل في حالة الإدانة مما يفضي من ثمّ إلى إعادة تأكيد حالة البراءة الأصلية، إلاّ أنّ الإكتفاء بمجرد الشكّ في إثبات التهمة مشروط بأن يشتمل الحكم بالبراءة ما يفيد أنّ المحكمة قد أحاطت بظروف الدعوى و أدلة الثبوت التي قام عليها الإتهام عن بصيرة و زانت بينها و بين أدلة النفي فرجّحت دفاع المتهم أو داخلتها الرّيبة في صحّة أدلة الإثبات أمّا القضاء بالبراءة دون إحاطة بظروف الدعوى و تمحيص أدلتها فإنّه يعيب الحكم⁽⁴⁾.

(1) مأمون سلامة، المبادئ العامة للإثبات الجنائي في الفقه الإسلامي، مقال في دراسات في حقوق الإنسان في الشريعة الإسلامية، مجلة القانون و الإقتصاد، عدد خاص، س 50، 1980، ص 45 مشار إليه لدى إيمان محمد علي الجابري، المرجع السابق، ص 94.

(2) ياسر الأمير فاروق، المرجع السابق، ص 694.

(3) و تطبيقاً لذلك قضت محكمة النقض المصرية "إذا كانت الأدلة التي ساقها القاضي في حكمه إنتهت إلى ترجيحه وقوع الجريمة من المتهم فإنّ الحكم يكون خاطئاً و مخالفاً للقانون فأيّ شكّ يتطرّق إلى عقيدة المحكمة في ثبوت التهمة يجب أن تقضي معه بالبراءة مهما أنّ احتمال الثبوت و درجته متى أحاطت بالدعوى عن بصر و بصيرة" مشار إليه لدى ياسر الأمير فاروق، المرجع السابق، ص 694.

(4) هلاي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 741.

و هكذا فإنّ الفقه لا يَنزاع في اعتبار هذه القاعدة إحدى النَّتائج الإيجابية لقرينة البراءة و الوجه السَّلبي لاشتراط "اليقين القضائي" لسلامة إقتناع القاضي بالإدانة، و مع ذلك فإنّ هناك رأياً يقف دون أنصار يرى أنّ قاعدة الشكّ يفسّر لصالح المتّهم ليس سوى إسما و ليست مبدأً مسيطر على الإثبات، إنّما مجرد حكمة لا تلزم القضاة في شيء، و استقرارها في التّطبيق القضائي ليس أكثر من عرف مؤسف و غير قانوني *pratique illégale et malheureuse*، و هو رأي يتجاهل في واقع الأمر سائر الإعتبارات التي يقوم عليها نظام الإثبات الجنائي، و على الأخص مقتضيات الحفاظ على "الحرية الشخصية" و إحترام "إفتراض البراءة" فيه حتّى يثبت عكس ذلك يقيناً، فهذه القاعدة هي من غير شك ضمانات للمتهمين في مقابل حرية القاضي في الإقتناع⁽¹⁾.

فالشكّ يفسّر لمصلحة المتّهم و تفسير ذلك يكمن في أنّ عدم قدرة أدلة الإدانة على إحداث القطع أو اليقين يترتب عليه إستمرار حالة البراءة الثابتة يقيناً و في هذا تقول محكمة النقض السوريّة " أنّ القضاء مؤسّسة مهمتها الحكم بالعدل و لا يكون ذلك إلاّ بالعمل على إبراز الوقائع واضحة جلية لا لبس فيها تدعمها أدلة قاطعة و حاسمة لا يتطرق إليها الشكّ و الشبهة و لا يلتبس فيها الإحتمال و كلّ دليل يحمل بين طياته شكاً أو شبهة أو إحتمالاً يجب أن يكون مصيره الإهمال، لأنّ في ذلك فقط يسود الحق و يقوم العدل"⁽²⁾.

و رغم أنّه من المستقرّ عليه أنّ الحكم بالإدانة يجب أن يبنى على اليقين في صحّة أدلة الإثبات بينما حكم البراءة يكفي فيه أن يؤسّس على الشكّ في هذه الأدلة، إلاّ أنّ محكمة النقض الفرنسيّة لا تأخذ بمبدأ الشكّ يفسّر لصالح المتّهم إلاّ في نطاق ضيق، حيث إنّها تتشدّد في فحص أسباب الحكم بالنسبة لأحكام البراءة المبنية على الشكّ أكثر من تشدّدتها بالنسبة لأحكام الإدانة فمجرد التأكيد أنّه يوجد شكّ في الإدانة لا يكفي لتبرئة ساحة المتّهم بل يجب أن يستند هذا الشكّ على أدلة قاطعة⁽³⁾.

(1) محمد زكي أبو عامر، المرجع السابق، ص 172.

(2) نقض سوري بتاريخ 1968/05/23 رقم 15، مشار إليه لدى: ممدوح خليل بحر، المرجع السابق، ص 347.

(3) من التّطبيقات القضائية على هذا التّوجه قضت محكمة النقض الفرنسيّة "إذ أفصحت محكمة الإستئناف على أنّ وسائل دفاع المتّهم غير أكيدة فيتعين أن تقضي بالبراءة حتّى تمكّنه من الإستفادة من قاعدة تفسير الشكّ لصالح المتّهم إلاّ بعد أن يتعدّر أن تضاء أمام القضاء كافة الشّموع و أن يتعدّر عليه إزالة الغموض الذي دعا لقيام الشكّ و

و قد أكدت المحكمة العليا ذلك المبدأ في العديد من أحكامها موضحة أن "القرارات القضائية الصادرة بالبراءة مثلها مثل القرارات الصادرة بالإدانة يجب أن تعلل تعليلا كافيا حتى تتمكن المحكمة العليا من مراقبة صحة تطبيق القانون، فالقرار الذي يكتفي بالحكم بالبراءة بمقول أنه يوجد في الدعوى شك لصالح المتهم يعتبر ناقص السبب و يستوجب النقض"⁽¹⁾.

في اعتقادنا فإن تطبيق قاعدة الشك يفسر لصالح المتهم في الحقيقة هي تأكيد لقاعدة أخرى مؤداها "أنه من الأفضل تبرئة ألف مجرم من إدانة بريء واحد"، فهي ضمانات أساسية تحول دون تعسف القاضي، و بمثابة نقطة التوازن بين مبدأ حرية القاضي في الإقتناع و مبدأ إفتراض البراءة.

الفرع الثاني: مبدأ وضعية الدليل المعلوماتي المستمد من التفتيش

لا تكفي قاعدة يقينية الدليل المعلوماتي المستمد من التفتيش في بناء حكم الإدانة لأن الحقيقة قد تكون خلاف ما توصل إليها القاضي، فالتقدير السليم لقيمتها الإقناعية يوجب عرضها على المناقشة العلنية و تأمين حق الأطراف من تقديم دفاعهم لدحضها أو تأكيدها إذ أن قاعدة وضعية الدليل قد تفضي إلى إقناع المحكمة بحقيقة غير التي ثبتت في ذهنها مقدما، ما يجعل هذا الشرط جوهريا في تكوين القناعة القضائية و تأسيسا على ما تقدم نستعرض هذا المبدأ من حيث مفهومه و مبرراته (أولا) و كذا النتائج المترتبة عليه (ثانيا).

أولا: مفهوم مبدأ وضعية الدليل المعلوماتي المستمد من التفتيش

تتضاعف أهمية كشف الحقيقة في الخصومة الجنائية بالنظر لتعلقها بسلطة العقاب و هو أمر يمس حرية المتهم و يتعرض لحقوقه الأساسية، و لذلك فإن القاضي يجب أن يصل إلى معرفة الحقيقة دون الإكتفاء بما يقدمه الخصوم من أدلة، بل إن عليه القيام بدور إيجابي في إستقصاء الأدلة و تقديرها فلا يجوز له الإقتصاد في جمع الأدلة بحجة الإسراع في المحاكمة فقد يحول ذلك دون إنارة الطريق أمامه للوصول إلى الحقيقة⁽²⁾.

ذلك بقيامه بمزيد من التحقيقات"، راجع هذه التطبيقات القضائية و أخرى لدى هلاي عبد الله أحمد، المرجع السابق، ص 741، و أنظر أيضا ممدوح خليل بحر، المرجع السابق، ص 347.

(¹) قرار صادر بتاريخ 12/11/1981 عن القسم الثاني للغرفة الجزائية في الطعن رقم 22416، مذكور لدى بن الصادق أحمد، سلطة القاضي الجنائي في تقدير أدلة الإثبات، رسالة دكتوراه، كلية الحقوق جامعة الجزائر 1، الجزائر، 2017، ص 88.

(²) فاضل زيدان محمد، المرجع السابق، 268.

و الحقيقة التي ينشدها الحكم الجنائي إنما الحقيقة الواقعية، و هذه الحقيقة لا يمكن توافرها إلا باليقين القضائي لا بمجرد الظن و الإحتمال، فاليقين مناط الحقيقة القضائية و ليس هو الذي ينفرد به القاضي باعتباره يقينا شخصيا بل هو اليقين الذي يفرض نفسه على القاضي و على كافة من يتطلعون بالعقل و المنطق إلى الأدلة فيجب أن تخرج الحقيقة التي تلوح في ذهن القاضي لكي تنتشر في ضمير الكافة⁽¹⁾، و يأتي ضابط المواجهة كأهم ضمان يحقق هذا اليقين.

لذا بات من القواعد الأساسية الراسخة في الأنظمة القانونية أنه لا يجوز للقاضي الجنائي أن يبني حكمه على أدلة لم تطرح لمناقشة الخصوم في الجلسة و هو ما يعبر عنه "بوضعية الدليل"، و مقتضى ذلك أن يكون للدليل أصل ثابت في أوراق الدعوى و أن تتاح للخصوم فرصة الإطلاع عليه و مناقشته و الرد عليه و كلا الأمرين ينبغي توافرها⁽²⁾، و ذلك مفترض يتفرع عن الحق في المحاكمة العادلة و حق الدفاع، فإذا كان القاضي الجنائي يقضي باقتناعه هو و ليس باقتناع غيره، فإنه يجب عليه أن يعيد تحقيق كافة الأدلة القائمة في الأوراق لكي يتمكن من تكوين إقتناع يقربه نحو الحقيقة الواقعية التي يصبو إليها كل قاض عادل و مجتهد⁽³⁾.

مؤدى هذا القيد أن الأدلة المعلوماتية المستمدة من التفتيش الجنائي سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسوب، أم كانت بيانات مدرجة في حاملات البيانات، أم اتخذت شكل أشرطة و أقراص ممغنطة أو ضوئية أو مصغرات فيلمية، كل هذه ستكون محلاً للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة، و على ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات يجب أن يعرض في الجلسة ليس من خلال ملف الدعوى في التحقيق الابتدائي، لكن بصفة مباشرة أمام قاضي الموضوع، و هذه الأحكام تنطبق على كافة الأدلة المتولدة عن حاسبات الحواسيب⁽⁴⁾، و أيضاً بالنسبة لشهود

(1) المرجع نفسه، نفس الموضوع.

(2) ياسر الأمير فاروق، المرجع السابق، ص 696.

(3) حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2007، ص 476.

(4) هلاي عبد الله أحمد، المرجع السابق، ص 748

الجرائم المعلوماتية الذين يكون قد سبق أن سُمعت أقوالهم في التّحقيق الإبتدائي، فإنّه يجب أن يعيدوا أقوالهم مرة أخرى من جديد أمام المحكمة⁽¹⁾.

محصلّة القول أنّه ينبغي على قاضي الموضوع أن يفضّ حرز الأدلّة المعلوماتيّة التي إنتهى إليها التّفتيش، و أن يمحصّها في حضور الخصوم بالجلسة لكي تصبح معروضة على بساط البحث و المناقشة، و هذا الإجراء واجب سواء تمسك المتّهم بذلك أو سكت عنه لتعلّقه بقاعدة أساسية من قواعد الإجراءات الجزائية⁽²⁾، و لا يوجد أيّ إستثناء على هذه القاعدة فكلّ الأدلّة تخضع وجوبا للمناقشة الحرّة للأطراف، و بناء عليه "لا يمكن للقاضي أن يبني قراره إلاّ على الأدلّة المقدّمة إليه أثناء الإجراءات و التي تمّت مناقشتها حضوريا في الجلسة"⁽³⁾.

و قد حرصت التّشريعات الإجرائيّة على أن تنصّ صراحة على هذه القاعدة الهامة، و من ذلك على سبيل المثال ما تنصّ عليه المادة 302 من قانون الإجراءات الجزائية الفرنسي "لا يجوز للقاضي أن يؤسّس حكمه إلاّ على أدلّة طرحت بالجلسة أثناء المحاكمة و نوقشت أمامه في مواجهة الأطراف"، و قد أخذ بهذه القاعدة المشرّع الجزائري إذ تنصّ المادة 212 فقرة 2 من قانون الإجراءات الجزائية "و لا يسوغ للقاضي أن يبني قراره إلاّ على الأدلّة المقدّمة في معرض المرافعات التي حصلت المناقشة فيها حضوريا".

في الحقيقة ليس هناك من دليل لا يصلح للمناقشة العلنية قبل أن يوضع موضع الإعتبار عند الإدانة أو البراءة، لذا نجد أنّ قاعدة وجوب مناقشة الدليل الجنائي من القواعد الأساسية في جميع الأنظمة القانونية⁽⁴⁾، تقتضي مراعاتها تحت طائلة بطلان الحكم الجنائي، و تطبيقا لذلك قضت المحكمة العليا الجزائرية أنّه "لا يمكن لقضاة الموضوع أن يؤسّسوا

(1) الشّاهد المعلوماتي: هو الفني صاحب الخبرة و المتخصّص في تقنية و علوم الحاسوب و الذي تكون لديه معلومات جوهرية لازمة لولوج لنظام المعالجة الآلية للبيانات إذا كانت مصلحة التّحقيق تقتضي التّقيب عن أدلّة الجريمة داخله، لمزيد من التّفصيل في هذه المسألة راجع: هلاّلي عبد الله أحمد، إلّتزام الشّاهد بالإعلام في الجرائم المعلوماتية، الطبعة الثّانية، دار النهضة العربيّة، القاهرة، 2008، ص 23 و ما بعدها.

(2) ياسر الأمير فاروق، المرجع السّابق، ص 697.

(3) Cass Crim, 20 novembre 1984, pourvoi n° 84-91.332, Bull. crim. 1984, n° 361.

(4) هلاّلي عبد الله أحمد، النّظرية العامة للإثبات الجنائي، المرجع السّابق، ص 470 و ما بعدها.

قراراتهم إلا على الأدلة المقدّمة لهم أثناء المرافعات و التي تمّ مناقشتها حضوريا و لذلك عملا بالمادة 212 من قانون الإجراءات الجزائية⁽¹⁾.

و في قضاء مستقر لها قضت محكمة النقض الفرنسية بأنّه ينبغي إعلام الخصم بأدلة الدّعى قبل الجلسة و في وقت يسمح له بمناقشتها و إلا لزم تأجيل نظر الدّعى إلى جلسة لاحقة، فإذا إستعصى ذلك لسبب من الأسباب كان على المحكمة أن تقضي باستبعادها من ملف الدّعى⁽²⁾، بل حتّى في الأحوال التي يتقدّم فيها الأطراف بأدلة أثناء نظر الدّعى و لم يسبق إعلام الخصوم بها كان للمحكمة الإلتفات عنها⁽³⁾، و انطلاقا من هذه السّوابق القضائية قرّرت ذات المحكمة نقض الحكم الذي إعتد على أدلة تقدّم بها المتّهم في الجلسة دون إعلام النيابة العامة بفحواها سابقا و تقديمها للمناقشة بالجلسة⁽⁴⁾، كما قضت بنقض الحكم الذي إعتد على أدلة لم تراعى فيها قاعدة وجوبية مناقشتها من قبل أطراف الدّعى⁽⁵⁾، و ذات الجراء الإجرائية متى إعتد القضاة في تكوين عقيدتهم على أدلة ضمت إلى ملف الدّعى بعد غلق باب المرافعات⁽⁶⁾.

غير أنّ محكمة النقض المصرية و إن إستقرت على هذا المبدأ، إلا أنّه كان لها رأي آخر في الموضوع أفصحت عنه في أحكامها، إذ قضت بأنّه "متى كان الطّاعن لم يطلب من

(1) قرار بتاريخ: 1982/01/21 رقم 1982 ، مشار إليه لدى: مستاري عادل، المرجع السابق، ص 63.

(2) Cass Crim, 19 juin 1991, pourvoi n° 90-86.630, Bull. crim. 1991, n° 267.

(3) Cass Crim, 12 janvier 2005, pourvoi n° 04-81.982, Bull. crim. 2005, n° 17.

(4) Crim., 5 janvier 2010, pourvoi n° 09-85.819, cité par Céline Michta, L'administration de la preuve en droit pénal français : exemple et pratique judiciaire de la gendarmerie nationale, Thèse de doctorat , l'Université, Strasbourg, France, 2017, p 45.

و في هذا الصّدّد تنتقد الباحثة قرار محكمة النقض على أساس التناقض الحاصل في سوابقها القضائية بين اعتبار هذه القاعدة كقيد على حرّية القاضي في قبول الدّليل الجنائي و في قرارات أخرى تعتبره بمثابة قيد على حرّية القاضي في تقدير القيمة الإقناعية للدّليل الجنائي.

(5) Cass crim. 20 mai 1992, no 91-84.297, Bull. crim. 1992 N° 201 « Mais attendu qu'en se déterminant ainsi, alors que ce document, au demeurant imprécis, n'a pas été soumis à la libre discussion des parties, la cour d'appel a méconnu les textes susvisés».

(6) Cass crim. 24 novembre 1970, no 70-90.161, Bull. crim. no 312 P. 763 » Doit être cassé l'arrêt qui se fonde sur un élément de conviction parvenu à la connaissance des juges entre la fin de l'audience à laquelle ont eu lieu les débats et le prononcé de la décision, et n'ayant pas dès lors été soumis à la libre discussion des parties »

المحكمة أن تفض حرز التّسجيلات الصّوتية فليس له من بعد أن ينعى على الحكم على إطلاع المحكمة على التّسجيلات أو عرضها عليه⁽¹⁾، كما قضت أنّ "لما كان البين من محضر جلسة المحاكمة أنّ الطّاعن أو المدافع عنه لم يطلب أيّهما الإستماع إلى شريط تسجيل المحادثات فليس للطّاعن من بعد النّعي على المحكمة قعودها عن إجراء تحقيق لم يطلب منها و لم ترى هي من جانبها لزوما لإجرائه"⁽²⁾.

و ينتقد الفقه المصري هذا التّطبيق القضائي، ذلك أنّ عدم فض حرز الدّليل الجنائي (التّسجيلات الصّوتية) و الإستماع إليها مفاده عدم عرض تلك التّسجيلات على بساط البحث و المناقشة في حضور الخصوم و الحيلولة بين المحكمة و بين الإطلاع على تلك التّسجيلات مما يصمّ إجراءات المحاكمة بالبطلان لمخالفة قاعدتي "وضعية الدّليل الجنائي" و "شفوية الإجراءات"، و لا يشفع لمحكمة النّقض أن تقرّر أنّ الطّاعن لم يتمسك بفض حرز التّسجيلات أو الإستماع إليها أمام محكمة الموضوع لأنّ تمسّكه أو عدم تمسّكه لا تأثير له فيما هو واجب عليها إجراءه من التّحقيق، إذ أنّ الأصل في الأحكام الجزائية أنّها تبنى على المرافعات التي تحصل أمام نفس القاضي الذي أصدر الحكم⁽³⁾.

مجمل القول أنّ ظهور المعلوماتية و خصائصها لا يغيّر شيئا من مبدأ الإقتناع الدّاتي، فالإقتناع يدبّ أن يتولّد على أثر الدّليل المتولّد في نفس القاضي و الذي لا يترك أيّ مجال للشك، و حيث أنّ القانون لا يقدّم في المجال الجنائي نمودجا خاصا للإثبات فإنّ القاضي الجنائي تكون له حرّية التّقدير و له الهيمنة في الواقع على القيمة الدّامغة للعناصر الإثباتية التي يؤسّس عليها إقتناعه و التي يكون لأطراف حرّية الاعتراض عليها و مناقشتها في كافة مراحل الدّعوى⁽⁴⁾.

(1) الطّعن رقم 181 لسنة 39 جلسة 1988/12/01، مشار إليه لدى ياسر الأمير فاروق، المرجع السّابق، ص 697.

(2) الطّعن رقم 31 لسنة 42 جلسة 1991/02/04، مشار إليه لدى ياسر الأمير فاروق، المرجع السّابق، ص 697.

(3) ياسر الأمير فاروق، المرجع السّابق، ص 697.

(4) JAEGER (Marc), les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France Revue international de droit pénale, Editions ERES, Paris, 1993, p 464.

ثانيا: النتائج المترتبة على مبدأ وضعية الدليل المعلوماتي المستمد من التفتيش

توصلنا فيما سبق إلى أنّ ضابط المجابهة أو قاعدة وجوبية مناقشة الأدلة المعلوماتية المستمدة من التفتيش تعتبر عنصرا مضافا لما يتمتع به القاضي الجنائي من حيده في تقرير قيمتها الإقناعية حيث يعدّ وسيلة تساعد على فهم أدلة الخصوم على حقيقتها من خلال المجابهة التي تتمّ أمامه مباشرة، فهي بالإضافة إلى أنّها تشكل ضمانة أساسية للخصوم في تقدير مستلزمات حق الدفاع فلا نعدو الحقيقة إذا قلنا أنّها تمكّن القاضي من تقدير الأدلة تقديرا مستتيرا بهذه المجابهة⁽¹⁾.

و يجري السؤال في ضوء هذه النتيجة عن مدى تأهيل القاضي من الناحية التقنية لمناقشة هذا النوع من الأدلة العلمية؟

لا مرأ أنّ قاعدة وجوب مناقشة الأدلة المعلوماتية المستمدة من التفتيش الجنائي بوصفها إحدى الركائز الأساسية التي تقوم عليها المحاكمة العادلة يترتب على إغفالها بطلان إجراءات المحاكمة لما في هذا الإغفال من إهدار لحقّ الدفاع بحرمانه من الإلمام بالأدلة المقدّمة ضده، و بالتالي فإنّ القاضي الجنائي لا يمكن أن يؤسّس إقتناعه إلاّ على العناصر الإثباتية التي طرحت في الجلسة و تمت مناقشتها في مواجهة الأطراف، و حتّى يكون للقاضي الجنائي السيادة و الهيمنة على الدّعوى الجنائية فلا بد أن يكون متدرّبا تدريباً فنياً خاصا على كيفية التعامل مع تقنية المعلومات و أنظمة معالجة البيانات المعقّدة و مع الأدلة المعلوماتية بشكل واف و دقيق، فلا شك أنّ هذا التأهيل العلمي يضمن نجاح المهمة التي تتطاط بالقضاة و هو بصدد مناقشة مخرجات الأنظمة الحاسوبية على اختلاف عناصرها و صورها⁽²⁾.

فما دام الدليل المستمد من التفتيش قد طرح بالجلسة و جب على محكمة الموضوع أن تقول كلمتها فيه بأسباب سائغة و متوائمة مع الثّابت بالأوراق و إلاّ كان حكمها قاصرا⁽³⁾، و الأمية المعلوماتية التي تعاني منها كافة الأجهزة القضائية و أعوانها تعدّ فعلا إشكالا كبيرا

(1) فاضل زيدان محمد، المرجع السابق، 268.

(2) هلاي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، مصر، 2008، ص 115.

(3) مشار إليه لدى ياسر الأمير فاروق، المرجع السابق، ص 698.

يحول دون مناقشة الأدلة المعلوماتية بل التسليم بها، أو بالأحرى التسليم برأي الخبير الفني المنتدب و هو ما يُفرغ هذا المبدأ من محتواه و يجزّده من الغاية المرجوة منه.

و لهذه الأسباب أجمعت كافة التقارير المقدّمة للمؤتمر الدولي الخاص ببحث "جرائم الحاسب و الجرائم الأخرى في مجال تكنولوجيا المعلومات إلى ضرورة التأهيل الفني و التقني للقضاة لمواكبة المواكبة العلمية للأدلة المعلوماتية المستمدة من التفتيش⁽¹⁾، حتّى يتمكن القاضي من تشكيل إقتناعه اليقيني بارتكاب المتّهم للجريمة، و لا يكون بوسعه ذلك ما لم يستوعب الجوانب الفنية للدليل المعلوماتي خاصة بالنسبة للجرائم المعلوماتية التي يكون فيها التّعقيد التقني أكثر وضوحا و مرتبطا بركنيها المادي و المعنوي، بما يحتمّ على القضاء الإستعانة بالخبراء لحضور جلسة المناقشة و الحصول على إيضاحات بشأن العناصر الإثباتية التي تنطوي على غموض⁽²⁾.

و هذا ما يوقدنا إلى القول بأنّ تحري الحقيقة يتخذ له مكانا كبيرا في سير عمل الخبير لكي يستطيع قاضي الموضوع الردّ على دفوع قد يبديها مرتكب الجريمة و تُشكّل في ذاتها دفوعا مقبولة أمام القضاء، لكونها تتفق من حيث طبيعتها مع تكنولوجيا المعلومات و المدى الواسع التي هي عليه، و من ذلك الدّفع الذي يبديه المتّهم بكون ما تمّ ضبطه في حاسوبه ليس له به علاقة و لا يدري عنه شيئا، و إنّما من قام بذلك هو أحد الهكرة مثلا، أو أن يكون ذلك هو مأمور الضبط القضائي ذاته لأيّ سبب كان، و معلوم أنّ إنتهاك حاسوب الغير من الأمور الجائزة الحدوث في جرائم الأنترنت، فمثل هذا الأمر يحتاج بالضرورة إلى الخبير للردّ عليه، سيما و أنّه دفاع مقبول أمام المحاكم في القانون المقارن، فلا يجوز للمحاكم إنكار مثل

(1) Erman Sahir, op cit , p 623.

(2) في الحقيقة يرى جانب من الفقه، أنّ إجراءات سماع المتّهم و استجوابه يجب أن تخضع لأحكام خاصة، بحيث يجب أن تتيج النّظم الإجرائية السّماح للخبير التقني بحضور هذا الإجراء حتّى يستعان به في فهم الجوانب الفنيّة للجريمة، أو حتّى السّلطة الإجرائية من طرح الأسئلة ذات العلاقة بهذا الجانب، بل إنّ من الفقه من نادى بإيكال هذه المهمّة إلى بيوت خبرة متخصصة في هذا المجال، بينما هناك من يرى الخطورة في تخلي أجهزة العدالة عن دورها في هذا النوع من الجرائم، إذ أنّها تضع حقوق المجتمع تحت رحمة شركات همها تحقيق الكسب المادي.

لمزيد من التّفصيل حول هذه المسألة راجع: محمد الأمين البشري، بحث بعنوان (التّحقيق في جرائم الحاسب الآلي، مقدّم إلى مؤتمر القانون و الكمبيوتر)، المنعقد في الفترة بين 1 و 3 ماي 2000 جامعة الإمارات العربية المتحدة، كلية الشريعة و القانون، الطّبعة الثالثة، 2004، ص 1082.

هذا الدّفع عن المتّهم، لكونه دفعا جوهريا واقعيا يحتاج للردّ عليه من قبل محكمة الموضوع و إلا وقعت في محذور الخطأ في التّسبيب⁽¹⁾.

و الملاحظ في هذا الصّدّد أنّ القاضي و إن لم يطمئنّ إلى الأدلة المعلوماتية فإنّه لا يجوز له إستبعادها إعمالا لسلطانه في تقدير قيمتها الإقناعية، فقد إستقرّ قضاء المحكمة العليا أنّه إذا كان القضاة غير مقيّدين برأي الخبير فإنّه لا يسوغ لهم أن يستبعدوا بدون مبرر نتائج الخبرة الفنية⁽²⁾، و من ثمّ فإنّ إمكانية الإستعانة بخبير متخصص لا يمكن أن يجعل القاضي بمعزل عن المعرفة و الدراية الفنية البسيطة و إلا عجز عن فهم الأدلة المعلوماتية المطروحة للمناقشة و لو بحضور الخبير، و استعصى عليه الردّ عن كل الدّفع و أوجه الطّعن المقدّمة ضد الخبرة، فاكتفى القاضي بالإدانة باقتناع الخبير لا بإقتناعه هو، و في ذلك ما يخالف مبدأ عدم جواز قضاء القاضي بناء على رأي الغير⁽³⁾.

(1) محمد أبو بكر بن يونس، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص 1044.

(2) قرار المحكمة العليا صادر بتاريخ 2010/07/22 رقم 676593، المجلة القضائية، قسم المستندات و النّشر بالمحكمة العليا، الجزائر، عدد2، 2011 (الفقرة الأخيرة من القرار).

(3) و تطبيقا لذلك قرّرت محكمة النقض المصرية حديثا "لما كان من حق محكمة الموضوع أن تستخلص واقعة الدّعوى من أدلتها و عناصرها إلا أنّ ذلك مشروط بأن يكون إستخلاصها سائعا و أن يكون الدليل الذي تعول عليه مؤديا إلى ما رتبته عليه من نتائج من غير تعسف في الإستنتاج و لا تنافر مع حكم العقل و المنطق، و كانت الأحكام الجنائية يجب أن تبنى بالجزم و اليقين على الواقع الذي يثبتته الدليل المعتمد، و لا تؤسّس بالظنّ و الإحتمال على الفروض و الإعتبارات المجردة .. إنّ الأحكام يجب أن تبنى على الأدلة التي يقتنع منها القاضي بإدانة المتّهم أو ببراءته صادرا في ذلك عن عقيدة يحصلها هو مما يجريه من التّحقيق مستقلا في تحصيل هذه العقيدة بنفسه لا يشاركه فيها غيره، و لا يصحّ في القانون أن يدخل في تكوين عقيدته بصحة الواقعة التي أقام قضاءه عليها أو بعدم صحتها رأيا لسواه، لأنّه و إن كان الأصل أنّ للمحكمة أن تعول في تكوين عقيدتها على التّحريرات باعتبارها معرّزة لما ساقته من أدلة طالما أنّها كانت مطروحة على بساط البحث إلا أنّها لا تصلح وحدها لأن تكون دليلا أساسيا على ثبوت التّهمة، هذا إلا أنّه يتعيّن في أحكام الإدانة أن تبنى على الجزم و اليقين لا على مجرد الظنّ و التّخمين، فإنّ الحكم يكون قد تعيّب بالفساد في الإستدلال و القصور في التّسبيب، و لا يغيّر من ذلك أن يكون الحكم قد عول على ما ورد بتقرير المعمل الجنائي و الطّب الشرعي، لما هو مقرّر من أنّ التّقارير الفنية لا تنهض بذاتها دليلا على نسبة الإتهام إلى المتّهم، و إن كانت تصحّ كدليل يؤيد أقوال الشّهود". الطّعن رقم 23981 لسنة 86 جلسة 2017/02/01.

الفرع الثالث: مبدأ موثوقية الدليل المعلوماتي المستمد من التفتيش

لا تقف حرية القاضي في تقدير الدليل المعلوماتي عند شرطي يقينية الدليل و وضعه قيد المناقشة العلنية ما لم يكن صادقا في مضمونه، خاصة و أنّ القضاء توجّس منه خيفة نظرا لسهولة تغييره و التلاعب به، فاليقين لا يتحقّق إلاّ بعد الإستثبات من صحته طالما أنّ الدليل الذي يعرض عليه ليس سوى نسخة منه، و هو ما يثير إشكالية إرتباط موثوقية الدليل بأصلته (أولا)، و مدى حرية القاضي في أعمال سلطته في تقييمها (ثانيا)، و كذا المعيار المعتمد في تقدير تحقّق الموثوقية من عدمها (ثالثا).

أولا: إشكالية إرتباط موثوقية الدليل المعلوماتي بأصلته

هناك تميّز حقيقي بين الأصالة Authentication في طابعها المادي و بين الأصالة في طابعها الرقمي، من حيث أنّ الأولى هي سوى تعبير عن وضعية مادية ملموسة كما هو الشأن في الورق المكتوب أو بصمة الأصابع، في حين فإنّ الثانية لسيت سوى تعداد غير محدّد لأرقام ثنائية موحّدة في الصّف و الواحد (0-1) و هما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمدّ حيويتها و تفاعلها من الطاقة ما يجعل الأصالة حين التّعامل مع الدليل المعلوماتي لها طابع خاص إذ أنّ طبيعة هذا الدليل لا تعبّر عن قيمة أصلية بمجرد رفع محتواه من البيئة الرقمية (الأنترنت و غيرها) سيما إذا علمنا قدرة الجاني على حذف الدليل من حاسوبه و يكون ما تبقى منه نسخة فقط تمّ إستردادها عن طريق التفتيش عن بعد⁽¹⁾.

فهل يكفي ناتج التفتيش وحده للقول بأنّ الدليل المعلوماتي المستمد من هذا الإجراء هو دليل أصلي يقبل طرحه على القضاء ليقول فيه كلمته بالإدانة؟ أي هل هذه النسخ تحقّق اليقين القضائي؟

العقبة الكؤود في هذا الخصوص هو معرفة المقصود بالمستخرج الأصلي أو بالمستند الأصلي هل هو الناقل أو الوسيط المغناطيسي؟ أو هو المدخلات الخام؟ أم هو الذاكرة الداخلية للحاسوب؟ و بفرض إن كانت وسائل التخزين هي المستندات الأصلية فإنّ السؤال سيظل قائما ما هي العلاقة بين المتحصّلات المتكافئة لنفس وسائل التخزين؟ هل القرص

(1) محمد أبو بكر بن يونس، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص 971.

المنسوخ مباشرة من الذاكرة الداخلية يفصل عن ذلك المنسوخ للمرة الثانية؟ هل المخرجات المبكرة أفضل من المخرجات المتأخرة أو اللاحقة؟⁽¹⁾.

إنّ عملية ضبط الأدلة المعلوماتية المستمدة من التفتيش بقصد تقديمها كدليل في المحكمة تعدّ من أولى الموضوعات التي تعرّض لها الفكر القانوني سواء من حيث قابليتها القانونية أو من حيث منهجية الدليل الذي تم تخريجه، إذ يصحّ في القانون أن يكون هناك من الأدلة ما هو مخرج من مخرجات الحاسوب و الأنترنت، بحيث تعدّ هذه المخرجات أدلة أصلية على الرّغم من كونها نسخ من دليل أصله موجود في العالم الافتراضي أو في الحاسوب و هو الجواب الذي وضع حدا لكافة هذه التساؤلات.

و قد عبّر عنه المشرّع الجزائري ضمنا بموجب المادة 6 من القانون 04/09 حيث جاء فيها "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزّنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و أنّه ليس من الضروري حجز كلّ المنظومة يتمّ نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحرار ووفقا للقواعد المقرّرة في قانون الإجراءات الجزائية"⁽²⁾.

(1) هلاي عبد الله أحمد، المرجع السابق، ص 744.

(2) و هذه القاعدة أصبحت عامّة بين مختلف الأنظمة القانونية بما فيها النظم الإنجلوسكسونية التي تتبنى "قاعدة الدليل الأفضل" The Best Evidence Rule التي مؤداها عدم جواز قبول صورة من المحرّر في الإثبات الجنائي إلا إذا كان من الممكن الحصول على الأصل، فقد حاولت مواعة تشريعاتها مع الضّرورة التي أمثلتها ذاتية أصالة الدليل المعلوماتي، في طليعة هذه الدّول، بريطانيا، التي أصدرت قانون إساءة استخدام الحاسوب في عام 1990م، الذي لم يتناول الأدلة الناتجة عن الحاسوب، و ربما كان السبب هو وجود قانون البوليس و الإثبات الجنائي لسنة 1984، الذي حوى تنظيمًا محدّدًا لمسألة قبول نسخ من الأدلة المعلوماتية المستمدة من التفتيش، كأدلة إثبات في المواد الجنائية، و في الولايات المتحدة الأمريكية تناولت بعض القوانين حجّية النسخ، و من ذلك على سبيل المثال ما نصّ عليه قانون الحاسوب لسنة 1984م، الصّادر في ولاية (أيووا)، من أنّ مخرجات الحاسوب تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرامج و البيانات المخزّنة فيه (المادة 16/716/أ)، كما يتضح من قانون الإثبات الصّادر في عام 1983م في ولاية كاليفورنيا، من أنّ النسخ المستخرجة من البيانات التي يحتويها الحاسوب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه البيانات، و في كندا، يمكن قبول نسخ من السجلات النّاجمة عن الحاسوب، إذا توافرت شروط معيّنة، و تنص المادة (29) من قانون الإثبات الكندي على عدد من الشّروط التي يجب توافرها قبل عمل صورة (Copy)، من السّجل الذي يضاف إلى الأدلة، و من هذه الشّروط أن تكون الصّورة حقيقية من المدخل الأصلي، و تنص قواعد الإثبات الفيدرالية الأمريكية، المادة 1001 بند 3 قانون الإثبات الأمريكي على إستثناء بقول الدليل المعلوماتي باعتباره مستندا أصليا مادام أنّ البيانات صادرة من جهاز حاسوب أو جهاز مماثل و سواء أكانت

الملاحظ في هذه الحالة أنّ إقرار القانون بهذه الهيئة الأخرى (النسخ) يكون مؤسساً على طابع إفتراضي مبناه أهميّة الدليل المعلوماتي ذاته و ضرورته، إلاّ أنّه لكي يحدث تواصل بين القانون و بين الدليل المذكور فإنّه يلزم سلوك مسلك الإفتراض من حيث إعتباره دليلاً أصلياً، و مسألة الأصالة هذه أثارت العديد من المشكلات، فعند البحث في قيمة الدليل المعلوماتي المستمد من التفتيش يتردّد السؤال دوماً على لسان القضاة فيما إذا كان الدليل المستخرج هو نفس أصل البيانات التي ضبطت دون أن يلحقه تغيير سواء أثناء "إستخراجه" أم عند "صبطه" و "تحليله" و "حفظه" إلى غاية تقديمه إلى القضاء أم لا.

و في هذا الإطار تثار ثلاثة تحديات، قد يدفع أحد الخصوم بعدم صحّة السجلات المتوالدة و تلك المخزّنة في الأنظمة المعلوماتية بالتساؤل عما إذا كانت السجلات قد تمّ تعديلها أو العبث بها أو تدميرها بعد إعدادها، أو ربّما قد يثير المتهمّ دفعا مبناه التّشكيك في صحّة سجلات الحاسوب المتوالدة بتحدي قدرة برنامج الحاسوب الذي قام بتوليدها و ربّما يقوم الأطراف بالإعتراض على صحّة السجلات المخزّنة و ذلك بالتّشكيك في هوية القائم بإعدادها- التفتيق-(1).

و هكذا فإنّ الخلاف حول إستخدام الدليل المعلوماتي المستمد من التفتيش أمام المحاكم الجزائية عادة ما يتعلّق بالموثوقية، و مع أنّ الكثيرين يتقنون في موضوعية و دقّة الأدلة المعلوماتية و يعتبرونها أكثر موثوقية و ينادون باستخدامها، يرى آخرون أنّ عدم وجود وسائل للتّحقق من أنّها أصلية يجعلها أكثر عرضة للرّفص، و على ذلك فهي أقلّ موثوقية من الأدلة التقليديّة، و من غير الملائم بناء حكم الإدانة عليها، فأعطاء قيمة قانونية لهذا النوع من الأدلة أمر صعب بسبب الجهل بإجراءات معالجة البيانات، و تترجم هذه الصّعوبة في

هذه البيانات مطبوعة أو مسجّلة على دعامات أخرى و مقروءة بالعين المجزّدة و تعبّر عن البيانات الأصلية بشكل دقيق، حيث تنصّ "النسخة المطابقة للأصل تقبل كما الأصل إلاّ إذا: أولاً، أُثير حولها تساؤل جدي يتعلّق بجديتها و أصالتها. ثانياً، إذا كانت الظروف لا تسمح بقبول النسخة المطابقة للأصل لكي تحلّ محلّ الأصل".

لمزيد من التّفاصيل حول موقف مختلف الأنظمة القانونية من أصالة الدليل المعلوماتي راجع: علي حسن محمد الطوّالبة، المرجع السّابق، 191 و ما بعدها، هلالى عبد الله أحمد، المرجع السّابق، ص 743 و ما بعدها، و أنظر أيضاً محمد أبو بكر بن يونس، المرجع السّابق، ص 974 و ما بعدها.

(1) عمر محمد بن يونس، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي المرشد الفيدرالي الأمريكي لتفتيش و ضبط الحواسيب توصلا إلى الدليل الإلكتروني في التّحقيقات الجنائية، المرجع السّابق، ص 426.

عدم وجود لوائح منهجية محدّدة و كذلك عدم وجود تجانس بين الأجهزة القضائية في تقدير مدى صحّتها و أصالتها، لذا أبدى الشّراح تخوّفهم من ضعف الرّقابة و سهولة التّلاعب في هذه الأدلّة مما يؤدي إلى وجود درجة عالية من التّقلب و عدم اليقين من صحة الأدلّة الأمر الذي يصعب معه الإعتقاد عليها في الإثبات⁽¹⁾.

إنّ حقيقة إمكانية خضوع الدّليل المعلوماتي للعبث به على نحو يجعله يعبر عن واقعة يقصدها أحد الأطراف خلافا للحقيقة الواقعية، جعلت المشرّع يعبر عن هذه المخاوف من خلال إرساء شرط جوهرى كقيد على حرّية القاضي في تقدير قيمتها الإثباتية و هي التّأكد من "سلامتها" Integrity و "صحّتها" Authenticity و هو ما يستشفّ من الفقرة الأخيرة من المادة 6 من القانون 04/09 و التي جاء فيها "غير أنّه لا يجوز لها إستعمال الوسائل التّقنية الضّرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للإستغلال لأغراض التّحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات".

لاشك أنّ إجراءات الحفاظ على البيانات و الوثائق و سلامتها أو ما يعرف **The chain of Custody Proves The Integrity** يعدّ أمرا مهماً لإثبات أصلية الدّليل المعلوماتي و يتمّ إثبات الحفاظ على البيانات و سلامتها من خلال التّأكد بأنّها إستخرجت من جهاز أو موقع معيّن و أنّ هذه البيانات و الأدلّة المستمّدة منها ظلّت تحت المراقبة منذ لحظة تجميعها و لم يطلها أيّ تغيير أو تدمير، ذلك أنّه من خلال الحفاظ على هذه البيانات يمكن الرّبط بين الدّليل المعلوماتي المستمد من تفتيش و الجريمة المرتكبة، فإذا كانت هذه البيانات أو المعلومات لم يحافظ عليها و على سلامتها بشكل صحيح فإنّ ذلك يؤدي إلى نتيجة مربكة و تظهر الشكّ في موثوقية الدّليل المتحصّل عليه من خلالها⁽²⁾، مما يؤدي إلى استبعادها من الإثبات تطبيقاً لقاعدة الشكّ يفسّر لصالح المتّهم.

ثانياً: المعالجة الفقهية و القضائية لإشكالية موثوقية الدّليل المعلوماتي

يثير موضوع موثوقية و أصالة الدّليل المعلوماتي كقيد على حرّية القاضي في تقدير قيمته الإثباتية إشكالية معقدة فيما إذا كانت هذه الطّبيعة التي عليها الدّليل المعلوماتي توجب

(1) سالم محمد الأولجي، مقبولية الدّليل الرّقمي في المحاكم الجنائية، مجلة دراسات قانونية، كلية الحقوق، جامعة بنغازي، ليبيا، العدد 19، جانفي 2016، ص 30.

(2) سالم محمد الأولجي، المرجع السابق، ص 35.

إرساء قواعد جديدة للتأكد من موثوقيتها أم تكفي القواعد التقليدية المتعارف عليها لبناء الحكم عليها أو إستبعادها؟

واقع الأمر أنّ الحل إزاء هذه الإشكالية لا يلقى الإجماع، إذ يرى جانب من الفقه في الولايات المتحدة الأمريكية أنّ التأكيد من صحّة السجلات الإلكترونية لتقديمها للقضاء لبناء هيكلّة الإدانة و البراءة يخضع لنفس القواعد التي تتبعها المحاكم للتأكد من صحّة أيّ دليل معروض عليها، و لا حاجة لوضع قواعد جديدة للتأكد من صحّة الأدلة المعلوماتية بوجه خاص⁽¹⁾، إذ أنّ معيار الصحّة في سجلات الحاسوب هو ذات معيار الصحّة في سجلات الحواسيب الأخرى، ذلك أنّ درجة الصحّة لا تتنوّع ببساطة لمجرد أنّ السجل متواجد في شكل إلكتروني⁽²⁾.

و تطبيقاً لذلك قضت المحكمة العليا في ولاية بنسالفانيا الأمريكية أنّ التأكيد من صحّة الأدلة المعلوماتية يخضع لذات القواعد المعمول بها في مجال الأدلة التقليدية و ذلك بقولها "نحن لا نرى أيّ مبرّر لإنشاء قواعد فريدة أو متميزة لقبول الأدلة المستمدة من الإتصالات مثل الرسائل بحيث يتمّ تقديمها للمحكمة و تقييمها على أساس كلّ حالة على حدى، شأنها شأن أيّ وثيقة أخرى لتحديد ما إذا كان هناك أسس و شواهد كافية للتأكد من أصالتها و صحّتها"⁽³⁾.

في مقابل ذلك أبدى جانب آخر من الفقه تردّداً واضحاً حيال مسألة موثوقية الأدلة المعلوماتية، خاصة بعد إقرار القضاء في كثير من قراراته بأنّ مصادقة المعلومات المخزّنة إلكترونياً ينطوي على عدد كبير من المخاوف، بحسبان أنّ "التكنولوجيا تتغيّر بسرعة كبيرة" بل و غالباً ما تكون غير مفهومة من قبل الجهات القضائية، علاوة على ذلك فإنّ تعقيد " أو

(1) محمود عبد الغني فريد جاد المولى، المرجع السابق، ص 211.

(2) H. Marshall Jarrett, et al, op cit, p 197.

(3) In re F.P., 878 A.2d 91, 95-96 (Pa.Super.2005)"We see no justification for constructing unique rules for admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity."

"حادثة" المعلومات المخزنة إلكترونياً مع إمكانية التلاعب بها، يستوجب متطلبات تحصيل أكثر صرامة بخلاف تلك المتعارف عليها لدراسة صحة السجلات الورقية الأخرى⁽¹⁾.

و قد بدى تردد القضاء واضحاً خاصة في ما يتعلق بالأدلة المعلوماتية المستمدة من تفتيش المراسلات الإلكترونية التي تتم عبر مواقع التواصل الاجتماعي -على كثرتها و تنوعها- إذ يتطلب القضاء خاصة في هذه الأحوال إثبات "القائم بالتأليف" و "إثبات عدم حدوث تغيير في المراسلة" على حد سواء، و تؤكد هذا التطبيق القضائي في عديد من القضايا الحديثة التي تعرف تزايداً مذهلاً في الولايات المتحدة الأمريكية و من بين أشهرها قضية *STATE v. ELECK*⁽²⁾، و قضية *COMMONWEALTH vs. DWIGHT WILLIAMS*⁽³⁾.

(1) Stephen Mason , Daniel Seng, op cit, 285.

(2) في قضية *State v. Eleck* حاول دفاع المتهم أن يشكك في صدق الشاهدة من خلال الإدعاء بأن المتهم قد تلقى مجموعة من الرسائل من الشاهدة عبر موقع التواصل الاجتماعي فيسبوك ، لكن المحكمة قضت بأن المتهم قد أخفق في إثبات أصالة هذه الرسائل و بناء على ذلك لا يمكن قبول هذه الرسائل كدليل لاستبعاد شهادة الشاهدة على الزعم من أن هذه الأخيرة أكدت بأن هذه الرسائل أرسلت فعلاً من حسابها الشخصي لكنها أنكرت أنها من قام بإرسالها و ذلك لأن حسابها الشخصي قد تم إختراقه من قبل طرف غير معروف منذ مدة تقارب خمسة عشر يوماً و قام بتغيير كلمة المرور الخاصة بها و أن نظام الإتصال ذاته لم يكن آمناً. و أخيراً ، دفع المتهم بأنه يمكن مصادقة الرسائل وفقاً لمبدأ "خطاب الرد" doctrine "reply letter" غير أن المحكمة لم يتحقق لديها اليقين بأن تتم مصادقة الرسالة B فقط بالرجوع إلى محتواها و الظروف التي تشير إلى أنها كانت رداً على الرسالة السابقة A و تم إرسالها من قبل المرسل إليه في الرسالة معتبرة أن هذا الدافع غير سديد.

State v. Eleck, 130 Conn. App. 632, 23 A.3d 818 (2011), citing Graham, Michael H., Authentication Generally: Chain of Custody, Electronic Communications, CRIM.L.BULL. Vol 54, (2018), p 33.

(3) تؤكد هذا التطبيق القضائي من قبل المحكمة العليا في مساتشوستس و تحديداً في قضية *COMMONWEALTH vs. DWIGHT WILLIAMS*. عندما قضت بعدم قبول الرسائل الموجودة على موقع التواصل الاجتماعي المسمى Myspace لعدم التحقق من أصالتها على الزعم من أن هذه الرسائل قد أرسلت بالفعل من الموقع الخاص بالمتهم الذي أدين بجريمة قتل مع سبق الإصرار و قد علّلت المحكمة قضاءها بعدم وجود ما يثبت -بالشهادة أو غيرها- إلى أي مدى يعدّ هذا الموقع آمناً، و من الذي يستطيع أن يدخل إلى هذا الموقع و هل يحتاج إلى شيفرات للدخول إليه و على الزعم من أن الشاهدة الرئيسية تؤكد أن هذه الرسائل أرسلت من حسابها الشخصي للمتهم لكن لا يوجد ما يثبت من هو الشخص الذي قام بإرسالها بالفعل كما لا توجد خبرة تثبت أن هذا الموقع لا يستعلمه شخص آخر غير المتهم.

COMMONWEALTH vs. DWIGHT WILLIAMS. [Available online]. Retrieved December 10, 2019, from :<https://law.justia.com/cases/massachusetts/supreme-court/volumes/456/456mass857.html>.

إلا أنّ الملاحظ أنّ القضاء الأمريكي يتجه نحو الإعتداد بموثوقية الأدلة المعلوماتية المستمدة من التفتيش من خلال إقرار قرينة مؤداها أنّ الدليل المقدم إلى المحكمة يستوفي شرط الموثوقية و يقع على من يدعي خلاف ذلك إثبات العكس⁽¹⁾. و مفاد ما استقر عليه هذا القضاء أنّ مجرد الدّفع بإمكانية أو احتمالية التلاعب بالبيانات، لا يعتبر غير كافيًا تأخذ به المحكمة لاستبعاد الدليل المعلوماتي المستمد منها، بل هناك من الفقه من ذهب إلى أبعد مما ذهب إليه القضاء، حيث يرى تحقّق شرط الموثوقية في الدليل المعلوماتي و لو طال التّغيير و التعديل بعض عناصر هذا الدليل الجنائي متى أمكن التّحقق من أصالة الباقي⁽²⁾.

بيد أن هذا الموقف الفقهي و القضائي لا يزال لا يحضى بالاجماع او الاستقرار، إذ أنّه ما تزال هناك شكوك حول أصالة و موثوقية هذا النوع من السّجلات الحاسوبية مع أنّه قد توجد بها معلومات مهمّة، فالمحقّقون يعتمدون اعتمادًا كبيرًا على السّجلات و ما يرد بها إذ أنّهم قادرون على تعويض أي نقص في وجود الوثائق التي تثبت بأنّ الأدلة المعلوماتية التي قدّمت أصلية و موثوقة⁽³⁾.

ثالثًا: معيار تقييم موثوقية الدليل المعلوماتي المستمد من التفتيش

إذا كان ذلك الذي سلف، فإنّ الإمتداد الطّبيعي للتساؤل المثار حول موقف القضاء من شرط موثوقية الأدلة المعلوماتية يثير تساؤلًا آخر يتعلّق مضمونه بالمعيار الذي يهتدى به للتأكد من إستفاء الأدلة لشرط الموثوقية و الصّحة؟

(1) H. Marshall Jarrett, et al, op cit, p 202.

(2) سالم محمد الأولجي، المرجع السابق، ص 35.

(3) ففي الحالات التي يكون فيها جزء من الدليل المعلوماتي يختلف عن الأصل، فإنّه من الممكن عزل الأجزاء التي تختلف عن الأصل بحسب تغييرها و التأكيد من سلامة ما تبقى منها، فعلى سبيل المثال إنّ الجزء السيء الموجود على القرص الصّلب الذي يحدث سبب التكرار أو التّغيير في محرك الأقراص الذي يدخل ضمن البيانات المستخرجة يتمّ إستبعاده، فتحديد الأجزاء السيئة و توثيقها يساعد المحققين على معرفة و تخصيص الملفات و البيانات المهمة في القضية، إضافة إلى أنّ الملفات الممتزجة بأجزاء سيئة يمكن أن تكون مفيدة في القضية من خلال مقارنتها بالأصل الموجود على القرص الصّلب للتأكد من أنّ البيانات و الأدلة المستمدة منها لم تتأثر بالأجزاء السيئة و عندما تكون هناك مخاوف من أنّ الدليل المعلوماتي قد أسيء إستعماله مما يحتمل أن تكون معلومات البراءة قد دمّرت فإنّ ذلك لا يمنع المحكمة من اعتماد الدليل طالما رأت أنّ الأدلة ما زالت محل ثقة.

لمزيد من التّفصيل راجع: سالم محمد الأولجي، المرجع السابق، ص 35-36.

يتطلب تقييم موثوقية الدليل المعلوماتي المستمد من التفتيش أن يكون الدليل أصليا و حقيقيا، و يتبع أحد النهجين في تقييم ما إذا كان الدليل المعلوماتي يمكن الاعتماد عليه في المحكمة أم لا، يقوم النهج الأول على التأكد من أن الحاسوب الذي أنتج الدليل المعلوماتي يعمل بصورة عادية، و النهج الثاني يقوم على فحص الدليل المعلوماتي الحقيقي لمعرفة مدى وقوع عيب بهذه النسخ أم لا⁽¹⁾.

مقتضى النهج الأول (شرط سلامة الحاسوب) يعني صحة حركة القطع الصلبة Hardware فيه، بحيث يجب أن تعمل بطريقة عادية، مثلما هو الحال في أي حاسوب آخر من ذات التركيبة، بحيث يجب فحص حركة الحاسوب المذكورة لكي يمكن تجنب الوقوع في مأزق رفض المحكمة الإعتداد بالدليل المنبثق عنه، و في القضاء المقارن لا سيما الأمريكي فإن شرط سلامة الحاسوب مطعن رئيسي على كل دليل تم الحصول عليه، بحيث يجب الكشف على حركة الحاسوب بداية و الإقرار بسلامته، و ذلك منذ قضية *Rosenberg v. Collins* حيث قررت المحكمة قبول الدليل الرقمي إذا كان مستمداً من حاسوب سليم⁽²⁾.

و هذا النهج تم إعتماده في الماضي من قبل أغلب التشريعات المقارنة في الولايات المتحدة الأمريكية و المملكة المتحدة، و هو يمنح للمحاكم سلطة تقدير البيانات المستخرجة من الحاسوب على أساس موثوقية نظام الحاسوب و عملية إستخراج البيانات، فعلى سبيل المثال تنص المادة 9/6/901 من القواعد الفيدرالية الأمريكية للإثبات بعنوان متطلبات الأصلية و التطابق تقتضي بأن الدليل يصف العملية أو النظام المستخدم في إحداث النتيجة و يبين أن العملية أو النظام أحدث نتيجة دقيقة، و في بريطانيا ينص القسم 69 من قانون الشرطة و الأدلة الجنائية لسنة 1984 "في أي مرحلة من مراحل الإجراءات الجنائية، فإن أي بيانات موجودة في وثائق مخرجة من حاسوب لن تكون مقبولة كدليل عن أية واقعة ما لم يتبين أنه: أ- ليس هناك أي إدعاء يصلح كأساس للإعتقاد بأن البيانات غير دقيقة بسبب عدم دقة الحاسوب"⁽³⁾.

(1) Eoghan Casey, op cit , p 61.

(2) محمد أبو بكر بن يونس، المرجع السابق، ص 1015.

(3) Eoghan Casey, op cit , p 62.

أما بالنسبة للتشريع الجزائري فهو لا يعير إهتماماً لمدى سلامة الحاسوب لتحديد موثوقية الأدلة المعلوماتية المستمدة من التفتيش، بل يشترط صراحة عدم حدوث تغيير على الأدلة عند "ضبطها" كمعيار فاصل في تقدير مدى أصالتها، كما توحى بذلك الفقرة الأخيرة من المادة 6 من القانون 04/09، و هو نص يحتاج إلى الكثير من التأمل و إعادة النظر، إذ أنّ عملية حفظ الأدلة في العالم الرقمي بالغة الدقة بحكم سرعة و سهولة العبث بها، ما يجعل شرط الموثوقية لا يقف عند هذا الحد (مرحلة إستخراج الدليل و مرحلة الضبط) وفق منظور المشرع، إنّما يتسع إلى مدى أبعد، بحيث يشترط أن لا يكون قد تعرّض الدليل لأيّ تغيير خلال عملية "ضبطه" أو "حفظه" أو "تحليله". و مثل هذا الأمر يجعل شرط الأصالة لا يتوقف عند مرحلة التحقيق، بل الأهم من ذلك هو المحافظة عليه عند تقديمه للقضاء فيستمر لمرحلة المحاكمة و أحيانا لمرحلة ما بعد المحاكمة، كما هو الشأن حال عرض الدليل المقدم إلى محكمة الموضوع و أمام جهة قضائية أعلى كالإستئناف أو لدى هذه الجهة بعد النقض لمرة أو مرات عدة و إلاّ فقد أهميّة وجوده قانوناً.

في مقابل ذلك هناك من التشريعات من اعتمدت كلا الشرطين لتحقيق أصالة الدليل المعلوماتي (سلامة الحاسوب و عدم حدوث تغيير على الأدلة عند ضبطها)، و يأتي التشريع السوري في طليعة هذه التشريعات، حيث أشارت المادة 25 من المرسوم التشريعي السوري رقم 17 لسنة 2012 إلى وجوب تيقن المحكمة من سلامة الدليل المعلوماتي المقدم إليها و ذلك بتحقق شرطين، التأكيد من كون الأجهزة الحاسوبية أو المنظومات المعلوماتية المستمد منها هذا الدليل تعمل جزئياً أو كلياً على نحو سليم، و أنّه لم يطرأ على هذا الدليل أيّ تغيير خلال مدة حفظه من شأنه أن يغيّر من طبيعته أو من محتواه، و يعدّ الدليل المعلوماتي المقدم إلى المحكمة مستجعماً لهذين الشرطين ما لم يثبت العكس⁽¹⁾.

(1) تنص المادة 25 من المرسوم التشريعي السوري رقم 17 لسنة 2012 المتعلّق بتطبيق أحكام قانون التّواصل على الشبكة و مكافحة الجريمة المعلوماتية: "حجية الدليل الرقمي:

أ) يعود للمحكمة تقدير قيمة الدليل الرقمي، شريطة تحقّق ما يلي:

- 1- أن تكون الأجهزة الحاسوبية أو المنظومات المعلوماتية المستمد منها هذا الدليل تعمل على نحو سليم.
- 2- ألا يطرأ على الدليل المقدم إلى المحكمة أيّ تغيير خلال مدة حفظه.

ب) يعدّ الدليل الرقمي المقدم إلى المحكمة مستجعماً للشرطين الواردين في الفقرة (أ) من هذه المادة ما لم يثبت العكس".

و مثل هذا القول لا يمكن قبوله على الإطلاق، و إنما وفقا للحالة العادية التي يعمل بها الحاسوب، بحيث لا يتمّ التّعويل على الدّليل المستمد من حاسوب محاصر تماما بالعطب البرمجي، أمّا إذا كان العطب البرمجي يجعل الحاسوب مع ذلك مؤهلا للعمل عليه فإنّ مثل هذا العطب البرمجي لا يؤثّر في قيمة الدّليل و مدى قبوله أمام المحاكم في هذا الشأن⁽¹⁾.

لذا يرى الفقه أنّه في الأحوال التي يقوم فيها شك معقول فيما يتعلّق بموثوقية الأدلة المعلوماتية، فإنّ هذا لا يجعلها بالضرورة مجردة من القيمة الإثباتية، و لكن ذلك سيقال من مقدار الوزن الذي تعطيه المحكمة، على سبيل المثال إذا كان هناك قلق من أنّ الأدلة قد تمّ العبث بها قبل جمعها، فإنّ هذا الشكّ قد يقلّل من الوزن المخصّص للأدلة، ففي العديد من الحالات جادل المتهمون بأنّ الأدلة لم تكن جديرة بالثقة لمجرد وجود احتمال نظري بأنّه كان يمكن تغييرها أو إختلاقها، و مع ذلك و نظراً لكون القضاة أصبحوا أكثر دراية بالأدلة المعلوماتية، فإنّهم باتوا يطالبون أدلة لدعم مزاعم عدم الثقة أو وجود عبث بالأدلة⁽²⁾.

من المعلوم أنّ موثوقية نظام حاسوب معيّن أمر صعب في التقييم، فمن الناحية العملية فإنّ المحاكم ليست مجهزة بشكل جيّد لتقييم موثوقية أنظمة الحواسيب و عملياتها، كما أنّ زيادة التنوع و التعقيد في هذه التقنيات جعل من الصّعب فحص كلّ الأجهزة و الوقوف على كلّ تعقيدات تشغيلها، إضافة إلى ما يبديه المبرمجون و مصمّمو البرامج من تحفّظ على موثوقية الدّليل المعلوماتي، في أنّه لا يمكن أن يؤسّس على أدنى مستوى من فحص أجهزة الحاسوب و التّعرف على دقّتها، و لهذا نجد أعباء كثيرة على المحاكم و ازدحام العديد منها بشهود التقنية، كما أنّ صعوبة تصديق الحاسوب أو حتّى عملية معيّنة في عمومها يمكن أن يعطلّ الموثوقية في ظروف معيّنة، على اعتبار أنّ أنظمة الحاسوب توجد بها أخطاء تشغيل غير متوقّعة تؤدي في بعض الأحيان إلى تلف البيانات أو قد يحدث تعطلّ كارثي، لذلك فإنّ أجهزة الحاسوب ليست آمنة لكي نفترض أنّ الأدوات الميكانيكية منضبطة وقت العمل⁽³⁾.

و لهذا فإنّ مسألة موثوقية الدّليل وفقا للنهج الأوّل مسألة معقّدة و للخروج من هذا المأزق لجأ القضاة المقارن إلى إرساء معايير أخرى أكثر موضوعية، و هي مبدأ إفتراض

(1) محمد أبو بكر بن يونس، المرجع السابق، ص 1014.

(2) Eoghan Casey, op cit , p 63.

(3) سالم محمد الأولجي، المرجع السابق، ص 37.

صحة الدليل المعلوماتي و يقع على من يدعي عكس ذلك إثبات تعرّضه للتغيير، و في حالة وجود شك معقول كان لقاضي الموضوع الإعتقاد على الخبرة التقنية للتأكد من أصالة الدليل أو نفي إستفائه لهذا الشرط⁽¹⁾، أو بالإستعانة بشهادة الخبراء التقنيين⁽²⁾.

غير أنّ هذا المعيار و إن كان الأكثر إستعمالاً إلاّ أنّه ظلّ منتقداً بشدّة و أسباب ذلك ترجع إلى أنّ عملية التفتيش على الأدلة المعلوماتية أصلاً عملية جدّ معقّدة و تستغرق جهداً كبيراً و موارد بشرية و أموالاً طائلة و تستنفذ وقتاً طويلاً قد يتجاوز في بعض الحالات ستة أشهر و يحدث ذلك في الدّول الأكثر تقدّماً من الناحية التقنية، أمّا إذا تمّ تكرار هذه العملية في سبيل التّحقق من أصالة الدليل فإنّ ذلك يؤدي بلا شك إلى شلل عملية استخدام هذا النوع من الأدلة في الإثبات الجنائي خاصة و أنّ مجمل الأدلة تتعرّض للطّعن في موثوقيتها.

و إزاء هذا الوضع حاول القضاء البحث عن بدائل لهذه المعايير المكلفة، و لعلّ أهمّها أنّه في حالة الشكّ المعقول في موثوقية الدليل المعلوماتي المستمد من التفتيش، يتمّ إعتبار هذا الدليل مجرد قرينة تحتاج إلى دليل يعزّز مصادقيتها للإعتقاد عليها في بناء حكم الإدانة،

(¹) و هذا ما أقرّه القضاء الأمريكي في العديد من القضايا، و من قبيل ذلك ما تم تطبيقه في قضية *Finley v. United States*، تتعلّق وقائع القضية باتهام *Finley* بحيازة صور فاحشة للقصر و توزيعها و قد تمّ إكتشاف الواقعة من خلال احتفاظ سلطات الولاية بقاعدة بيانات للصور الإباحية للأطفال القصر و المنشورة على شبكة الأنترنت، و في هذه القضية تمّ إستعمال برنامج *SHA* و هو إحدى تطبيقات برنامج *hash value*، و من خلال قاعدة البيانات تمّ تحميل البرنامج و إثبات أنّ الصور الموجودة على *IP* الخاص بالمتّهم هي نفس الصور الإباحية التي تمّ ضبطها بواسطة الضبطية القضائية في ملف القضية، و بناء على ذلك اقتنعت هيئة المحلّفين بصحة الدليل المعلوماتي المستمد من التفتيش و اعتمد عليه في إدانة المتّهم. أنظر الحكم *United States v. Finley, 612 F.3d* (8th Cir. 2010)، 998، مشار إليه لدى: محمود عبد الغني فريد جاد المولى، المرجع السابق، ص 218.

(²) و قد إستند القضاء الأمريكي إلى هذا المعيار في قضية *United States v. Salcido* و تتلخّص وقائع القضية أنّه تمّ العثور على أحد المواقع و بالفعل قام المحقّق بتحديد موقع هذه الصور و كذلك *IP* الخاص بصاحب الموقع (المتّهم) و تمّ إستصدار إذن بتفتيش حاسوب المتّهم عن طريق إنتداب خبير تمكّن من إسترداد العديد من الصور و الفيديوهات و التي تمّ ضبطها و تحريزها و بعد عرضها على هيئة المحلّفين طعن المتّهم في سلامتها، أكّدت المحكمة قناعتها بصحة و موثوقية هذه الأدلة من خلال شهادة الخبير *expert testimony*. أنظر الحكم *United States v. Salcido, 506 F.3d 729, 733* (9th Cir. 2007); مشار إليه لدى: محمود عبد الغني فريد جاد المولى، المرجع السابق، ص 224.

كالإعتماد على شهادة الشهود⁽¹⁾، أو تصريحات الضحية إذا لم ينكرها المتهم⁽²⁾، أو إقرار المتهم ذاته، أو بالإستناد إلى شواهد أخرى تؤكد قيام العلاقة بين الدليل المعلوماتي المطعون في صحته و بين الوقائع المراد إثباتها (test of potential relevance)⁽³⁾.

(¹) طبّق القضاء الأمريكي هذا المعيار في قضية *United States v. Barlow* حيث تمت إدانة المتهم بتحريض فتاة قاصر على فساد الأخلاق (التحريض و إغراء قاصر للإخراط في علاقة جنسية من خلال إرسال صور فاحشة و تتعلّق وقائع القضية أنّه و خلال شهر أوت سنة 2006 قام المتهم البالغ من العمر 29 سنة بإجراء محادثة من خلال البريد الإلكتروني مع الضحية Rebecca و كان عمرها آنذاك حوالي 14 سنة و تواصلت هذه المحادثات بشكل منقطع أين تجرّأ المتهم على إرسال صور جنسية محاولاً من خلال فعله إقناع الفتاة القاصر بإقامة علاقة جنسية معه مطالباً منها مراسلته بصور مخلة بالأداب لشخصها، و قد وافقت الضحية بالفعل على لقاء المتهم في احد الحدائق المنزوية و وصل المتهم قبل الميعاد فوجد شخصاً بالغاً بمقر الحديقة ففرّ العدول عن فعله الجرمي منها خوفاً من ضبطه إلا أنّ السلطات ضبطت حاسوب المتهم و عند القيام بتفتيشه تمكّنت من استرداد الأدلة المعلوماتية المتمثلة في الرسائل و الصور المتبادلة بينهما أثناء المحادثات أين تقدّم المتهم بالطعن في موثوقية الدليل المعلوماتي، و للتأكد من مصداقية هذه المراسلات الرقمية تلقت المحكمة شهادة صديق الضحية الذي كان يجري أيضاً محادثات مع الضحية و استطاع أن يطلع فيما سبق على بعض تلك المراسلات المتبادلة بين الضحية و المتهم. أنظر الحكم: *United States v. Barlow, 568 F.3d 215, 220 (5th Cir. 2009)*، مشار إليه لدى: محمود عبد الغني فريد جاد المولى، المرجع السابق، ص 228.

(²) و من تطبيقات ذلك ما قضت به محكمة الاستئناف في *North Carolina*، تتلخّص وقائع القضية في أنّ الضحية Jennie إنقبت بالمتهم لأول مرة في صيف عام 2005 بكنيسة Baptist و الذي كان يزاول عمله بوزارة رعاية الطفولة و يبلغ من العمر 27 سنة في مقابل ذلك كان سن الضحية لا يتعدى 13 سنة و استهل التّواصل بينهما عبر رسائل البريد الإلكتروني للهاتف النقال و في 14 جانفي 2006 إتفق على الذهاب إلى الإجتماع في هذه الكنيسة و حضرت الضحية فعلاً إلى مسكن المتهم حيث يقيم و جلست مع والده لما يقارب الساعة إلاّ ربع من الزمن و بعد ذلك خرجا سوياً إلى الكنيسة بعدها إنتقلا إلى إحدى الغابات أين حقّق الجاني مشروعه الإجرامي ليكرّر هذه الواقعة الإجرامية مرات أخرى بمسكنه و كانت الأدلة المعلوماتية المقدّمة من والدة الضحية تتمثل في مراسلات تبادلها المتهم مع الضحية تتضمّن ما يوحي بإقناعها بإقامة علاقة جنسية، و كان عنوان البريد الإلكتروني في كلّ الرسائل واحداً أين أقرّ المتهم بأنّ هذا العنوان هو الخاص به و لم يقدم ما يؤدي إلى التّشكيك في صحة و موثوقية الأدلة المعلوماتية. أنظر الحكم: *Williams v. United States N.C. App. 254 (N.C. Ct. App. 2008)* مشار إليه لدى: محمود عبد الغني فريد جاد المولى، المرجع السابق، ص 230-231.

(³) في قضية *Griffin v. State* أبرزت المحكمة أهميّة الإستفسار عن المنشئ المزعوم لموقع التّواصل الإجتماعي فيما إذا كان يملك الحساب و هل قام بتحميل المعلومات ذات العلاقة على ذلك الموقع، و تتلخّص وقائع القضية في أنّ محكمة الدّرجة الأولى أدانت المتهم بجريمة قتل من الدّرجة الثانية و جرائم أخرى، و قد إعتمدت محكمة الموضوع في إدانة المتهم على جملة من الأدلة من بينها صفحات اخذت من حساب صديقة المتهم على أحد مواقع التّواصل الإجتماعي و التي تتضمّن عبارات تهديد وجهتها صديقة المتهم إلى الشّاهد الرئيسي في القضية و في مرحلة

الحقيقة إنّ مثل هذه المخاوف تجعل من الصّعوبة بمكان إمكانية الإعتماد على دليل معلوماتي لوحده لإدانة المتّهم، و إنّما يحتاج الأمر هنا إلى دليل مادي و مثابرة من جهات التّحقيق لكي يتوافر لها دليل تقليدي كإعتراف أو شهادة أو خبرة أو قرائن، بحيث ينبغي ينبغي ألاّ تتجاوز إلى تقرير المستحيل، ففي الحالات التي تمّت فيها إدانة أشخاص أمام القضاء المقارن كان هناك دائماً دليل مادي يتمّ الإستناد إليه إلى جوار الدّليل المعلوماتي⁽¹⁾.

خلاصة القول أنّ معيار تقييم موثوقية الدّليل المعلوماتي المستمد من النفتيش الأكثر فاعلية يكون من خلال التّركيز على الدّليل المعلوماتي ذاته في ضوء الظروف و الملابسات أكثر من التّركيز على العملية التي أنتجت الدّليل، كما أنّه من غير العملي و لا من الضّروري اللّجوء إلى الخبرة العلمية في كلّ قضية تعرض على القضاء، خاصة و أنّ هذا النوع من الأدلّة سيشتكّل حجر الزّاوية في الإثبات الجنائي مستقبلاً، لذا ينبغي معالجة كلّ حالة على حدى و أعمال أحد المعايير السّالفة في ضوء نوع الدّليل و مدى معقولية التّشكيك في صحّته للوصول إلى اليقين القضائي.

الاستئناف قضت محكمة الاستئناف في ولاية Maryland بعدم قبول الدّليل المعلوماتي لأنّ النّياية العامة لم تتحقّق من أصلاتها على الرغم من ان تلك الصفحات محل النفتيش تحتوي على صور صديقة المتهم و تاريخ ميلادها و مكان سكنها يضاف إلى ذلك كلّهُ أنّ النّياية العامة لم تسأل صديقة المتّهم إذا ما كانت تملك الحساب على موقع التّواصل الإجتماعي أم لا و هل أنّ محتواه تمّ إعداده من قبلها أم لا كما أنّه لا تعدّ الصّورة و تاريخ الميلاد و مكان الإقامة خصائص مميزة تؤيّد و تدعم أصالة الدّليل المعلوماتي كما قضت المحكمة أيضاً بأنّه يجب أن يؤخذ بعين الإعتبار احتمال سوء الإستخدام أو التّلاعب بموقع التّواصل الإجتماعي من شخص لآخر غير المالك أو المستخدم الحقيقي له و جاء في حيثيات قرار الاستئناف أنّه من الوسائل التي يمكن إستخدامها للتّحقّق من أصالة الدّليل هو سؤال صاحب الحساب المزعوم فيما إذا كان هو من أنشأ الحساب و أضاف البريد محل البحث الذي تمّ تحميله على الحساب الشّخصي على أحد مواقع التّواصل الإجتماعي، و إذ ادعى أحد الأطراف أنّ الدّليل الذي تمّ الحصول عليه من أحد مواقع التّواصل الإجتماعي تعزّزه الدّقة فيمكن الحصول على مزيد من المعلومات من الطّرف الآخر أو من موقع التّواصل الإجتماعي ذاته بصورة مثالية يتعيّن إجراء ذلك قبل المحاكمة و هو أمر يظهر أهميّة تحضير الدّعوى من قبل المحامين لأغراض الحصول على المعلومات و قبول الدّليل على سبيل المثال الإدعاء بأنّ شخصاً قام باستخدام موقع التّواصل الإجتماعي على نحو غير ملائم يمكن دحضه من خلال تتبّع إستعمال حاسوب أحد الأشخاص من خلال المعرّف الرّقمي للجهاز IP، إذا كان حكم الإدانة يعتمد على أصالة المطبوعات المأخوذة من الموقع فيجب على هيئة المحلّفين أن تتحقّق من موضوع أصالة الدّليل بصورة يقينية لا محل للشكّ فيها حتّى و لو ترتّب على ذلك إطالة أمد المحاكمة. أنظر الحكم: (Griffin v. State, 19 A.3d 415 (Md. 2011)، مشار إليه لدى: سامي حمدان الرّواشدة، المرجع السّابق، ص 23.

(1) محمد أبو بكر بن يونس، المرجع السّابق، ص 999.

الفصل الثاني

القيمة القانونية للأدلة المعلوماتية المستمدة من تفتيش غير مشروع

تعتبر الرقابة على مشروعية إجراءات استرداد الدليل المعلوماتي، جوهر الإشراف القضائي على كفالة الحرية الشخصية، إذ تفقد قاعدة مشروعية الدليل المعلوماتي قيمتها إذا لم تكن هناك رقابة فعالة على السلطة التي تباشر التفتيش، و لا معنى لهذه الرقابة إذا لم يكن هناك جزاء يتقرر جزاء مخالفة كل ما تفرضه هذه القاعدة، و لا سبيل إلى ذلك سوى بفرض جزاء يصيب التفتيش غير المشروع (مبحث أول)، و جزاءات أخرى تصيب مرتكب هذا الإجراء غير المشروع (مبحث ثاني).

المبحث الأول

جزاء التفتيش غير المشروع عن الأدلة المعلوماتية

يكفل القضاء حماية الشّرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش عن طريق إعمال راقبته على هذا الإجراء المتخذ صونا للحريات الفردية و منعا من إساءة إستعمال السّلطة، و وسيلته في ذلك تكمن في منع العمل الإجرائي الذي إتخذ بالمخالفة للقانون من ترتيب آثاره، و تلك نتيجة غاية في الأهمية قد تؤدي إلى إفلات المجرم من العقاب رغم تحقّق الإقتناع بالإدانة، لذا يقع علينا أن نحدّد هذا الجزاء الإجرائي (مطلب أول)، و آثاره (مطلب ثاني).

المطلب الأول: تحديد الجزاء الاجرائي للتفتيش غير المشروع

لما كان تفتيش نظم المعلومات بمختلف مراحلها هو مصدر الأدلة المعلوماتية التي تؤسّس عليها المحكمة إقتناعها بالإدانة، فإنّ قبول هذه الأدلة يتوقّف على مشروعية هذا العمل الإجرائي لهذا كان البطلان عنوانا لعدم المشروعية، و لا يتأتى إهدار هذا الدليل إلا في ضوء التّناسب بين المصلحة العامة و مصلحة الأفراد، لذا وجب بيان سياسة البطلان بشكل عام (فرع أول) و تحديد طبيعة البطلان الذي يلحق التفتيش عن الأدلة المعلوماتية (فرع ثاني) و أحكام الدّفع به (فرع ثالث).

الفرع الأول: قواعد البطلان بشكل عام

لا يمكن أن نرتّب أثرا قانونيا لإجراء غير قانوني، و في مقابل ذلك فإنّه ليست كلّ مخالفة لقاعدة ما تستوجب إهدار الدليل المستمد من هذا الإجراء المطلوب ما لم تبلغ المخالفة حدا من الجسامّة، و إلا طغى عنصر الشّرعية على الفعالية و شلّت يد الهيئة الإجتماعية في مواجهة الإجرام، لذا يتحتّم علينا أن نبيّن مفهوم البطلان (أولا)، و نحدّد مذاهبه (ثانيا)، و صورته (ثالثا)، و معياره (رابعا).

أولا: تعريف البطلان

أشرنا فيما سبق إلى أنّ الرّقابة القضائية تعتمد على سلطة القضاء في إلغاء الإجراء المخالف للقانون، و يتمثّل هذا الإلغاء في الجزاء الذي يرد على الإجراء غير المشروع فيهدر آثاره القانونية، و هو أكثر الجزاءات فاعلية كنتيجة تترتّب على مخالفة الضّمّانات، لأنّه يفسد

على المخالف قصدَه فيهدر الدليل الذي يسعى إليه من وراء هذه المخالفة، و يتخذ الجزاء الإجرائي بوصفه وسيلة للرقابة القضائية صورة البطلان، و هو يحمي بذلك الحرية الشخصية التي جاءت الشرعية الإجرائية لكفالة إحترامها⁽¹⁾.

و قد تعددت التعريفات التي أعطها الفقه للبطلان إلا أنها مع ذلك متقاربة للغاية⁽²⁾، و يمكن القول بأن البطلان هو "جزء إجرائي يلحق كل إجراء معيب وقع بالمخالفة لنموذجه المرسوم قانونا فيعيقه عن أداء وظيفته و يجردّه من آثاره القانونية التي لا يمكن ترتيبها فيما لو وقع صحيحا"⁽³⁾. و يُعرّف البطلان كذلك، بأنه "جزء إجرائي يترتب على عدم مراعاة أحكام القانون المتعلقة بأي إجراء جوهري و يستوي أن تكون الأحكام المتعلقة بالإجراء الجوهري تتعلّق بمضمون و جوهر الإجراء أو كانت تتعلّق بالشكل الذي يصاغ فيه، كما يستوي أن تكون هذه الأحكام قد وردت بقانون الإجراءات الجزائية أم بقانون العقوبات"⁽⁴⁾.

فبطلان العمل القانوني هو "إهدار لقيمته و استبعاد آثاره"، و الأصل فيه أنه نتيجة طبيعية لمخالفة العمل للشروط التي يستلزمها القانون لصحته، سواء إستمدت هذه الشروط من نص صريح أو من القواعد العامة، لأنّ العمل المخالف للقانون لا يجوز أن يكون له قيمة العمل الصحيح⁽⁵⁾.

- (1) أحمد فتحي سرور، الشرعية الدستورية و حقوق الإنسان في الإجراءات الجنائية، المرجع السابق، ص 394.
- (2) راجع في تعريف البطلان: أحمد الشافعي، البطلان في قانون الإجراءات الجزائية، دراسة مقارنة، الطبعة الثانية، دار هومة، الجزائر، 2015، ص 12- أنظر رمسيس بهنام، المرجع السابق، ص 74 إذ يرى أنّ البطلان معناه إعتلال الإجراء و قابليته للإنهيار في صورة تجاهل له و عدم إكتراث به، فيكون الوجود القانوني للإجراء مهتزاً و آيلاً للسقوط على الرّغم من وجوده المادي، و مع ذلك يترتب على عدم الإجراء أن يدب فيه ديبب الصّحة بعد أن كان معتلاً فيشندّ و تثبت له آثاره- أنظر إبراهيم التّجاني أحمد، نظرية البطلان و أثرها على الحقوق الشرعية في القوانين الإجرائية و الجنائية السودانية، الطبعة الأولى، مركز الدراسات و البحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2001، ص 21، حيث يرى أنّ البطلان هو جزء يترتب على عدم توافر العناصر اللازمة للعمل القانوني في ظل حماية الحريات و أمن و سلامة المجتمع.
- (3) ياسر الأمير فاروق، المرجع السابق، ص 702.
- (4) مأمون سلامة، الإجراءات الجنائية في التشريع المصري، الجزء الثاني، بدون رقم الطبعة، دار النهضة العربية، مصر، 1992، ص 335.
- (5) توفيق محمد الشاوي، المرجع السابق، ص 425.

و لعلّ أهم التعريفات التي قيلت بشأن البطلان هو ذلك الذي يبى أنّ البطلان هو "جزاء إجرائي لتخلّف كلّ أو بعض شروط صحة الإجراء الجنائي و يترتّب عليه عدم إنتاج الإجراء آثاره المعتادة في القانون"⁽¹⁾.

و نحن نرى أنّ أكثر الوسائل الإجرائيّة فعّالية في كفالة الحرّية الشّخصية أو بشكل عام كفالة إلترام السّلطة الإجرائيّة بما تفرضه قاعدة مشروعية الدّليل الجنائي و ما تستوجبه قرينة البراءة هي البطلان، و هو مفهوم يرتبط بشكل أساسي بالغاية من الإجراء الجنائي بحد ذاتها، و التي سبق أنّ أشرنا إليها و هي التّسيق بين الثّانية الفعّالية و الشّرعيّة في الوصول إلى الحقيقة الواقعية، فهو بهذا المعنى جزء إجرائي يترتّب على عدم مراعاة العناصر اللّازمة للعمل الإجرائي فيهدر آثاره و يجرها من قيمتها القانونية فيما لو صح العمل الإجرائي.

و هذه الوسيلة الإجرائيّة التي تمنع العمل الذي أتخذ بالمخالفة للقانون من ترتيب آثاره، تثير لدينا تساؤلا محدّدا مضمونه هل المشرّع الجزائري عدّد على سبيل الحصر الحالات التي يترتّب فيها هذا الجزء الإجرائي للدّليل غير المشروع؟ أم أنّه ترك هامشا من التّقدير للقاضي يستخلصه وفقا لجسامة المخالفة المرتكبة حتّى و إن لم يترتّب المشرّع البطلان جزء مخالفتها بنص صريح في القانون؟

ثانيا: مذاهب البطلان

لا مرأ في أنّ قد يتقرّر البطلان بنص قانوني جزء مخالفة لقاعدة نصّ عليها المشرّع صراحة، كما قد يترتّب أيضا لمجرد مخالفة قاعدة تعتبر جوهرية دون أن ينصّ المشرّع على البطلان كجزء تلك المخالفة، و هذه النتيجة تفيذ أنّ البطلان قد يكون قانونيا أو شكليا(أ)، و قد يكون ذاتيا يقدره القاضي دون أن يرد عليه نص في القانون و هو ما يطلق عليه بالبطلان الجوهرية أو الذاتي(ب).

(أ) - مذهب البطلان القانوني

يعني مذهب البطلان القانوني أو الشكلي (Nullité Textuelle) أنّه "لا بطلان بغير نص" Pas De Nullité Dans Texte، و مضمون هذا المذهب أنّ المشرّع هو الذي يتولّى بنفسه تحديد حالات البطلان، بحيث لا يجوز للقاضي أن يقرّر البطلان في غير هذه

(1) محمود نجيب حسني، المرجع السّابق، ص 394.

الحالات⁽¹⁾، و ميزة هذا المذهب أنّ المشرّع يتولّى بنفسه الإفصاح عن آرائه في تحديد الضّمّانات الجوهرية التي يترتّب على مخالفتها البطلان⁽²⁾، فالقاضي مقيدّ بنص القانون في تقرير هذا الجزاء من عدمه.

و يترتّب على ذلك أمران: أولهما، أنّه لا يكفي النصّ على إتباع إجراء معيّن حتّى ينتج البطلان عن إغفاله، بل لا بدّ أن يكون المشرّع قد فرض هذا الإجراء في حالة الخروج عليه، بعبارة أخرى لا يجوز الحكم بالبطلان دون نص صريح يقرّر بطلان كلّ إجراء على حدى عند عدم مراعاة القواعد القانونية المتعلقة به. و ثاني الأمرين، أنّ القاضي لا يملك أيّ سلطة تقديرية في هذا الشأن، فلا يملك أن يقضي بالبطلان ما دام المشرّع لم ينص عليه، كما لا يملك عدم القضاء به عند النصّ⁽³⁾، و معنى ما تقدّم أنّ هذا المذهب يتسم بالضبط و التّحديد، فلا مجال للخلاف في الرّأي حول نصيب الإجراء من الصّحة و البطلان، فقد استبعد المشرع ابتداء السّلطة التّقديرية للقاضي في هذا الشأن⁽⁴⁾.

بيد أنّ هناك من الفقه من ينتقد هذا المذهب بحجة أنّه يضيق من حالات البطلان باستلزامه نصاً تشريعياً في كلّ حالة، كما أنّه يستند إلى تنبؤ المشرّع سلفاً بأحوال البطلان، مع أنّه يتعدّر أن يوقّق المشرّع في تحديد أحوال البطلان في قائمة خالية من الإفراط أو التّقريط⁽⁵⁾. فالمشرّع و هو يضع قواعد قانونية مجرّدة لا يستطيع أن يحيط بكلّ الفروض الواقعية، فثمّة حالات يقتضي المنطق القانوني و المصلحة الإجتماعية تقرير البطلان فيها، فلا يجد القاضي وسيلة إلى ذلك، بالإضافة إلى ذلك فقد يقرّر القانون البطلان في حالة، و

(1) إبراهيم التّجاني أحمد، المرجع السّابق، ص 21.

(2) أحمد فتحي سرور، المرجع السّابق، ص 27.

(3) عادل عبد البديع آدم حسين، وسائل الرّقابة القضائية على مشروعية الدّليل الجنائي دراسة مقارنة، الطّبعة الأولى، دار النهضة العربية، مصر، 2015، ص 140.

(4) محمود نجيب حسني، المرجع السّابق، ص 396.

(5) جدير بالذّكر أنّ القضاء الفرنسي بمساعدة الفقه هو الذي أنشأ مذهب البطلان الدّاتي لمواجهة ما كان ينصّ عليه قانون تحقيق الجنايات قديماً من حالات قليلة للبطلان، و يلقي هذا المذهب سنده المباشر في القياس بمعنى مظاهاة إجراء لم ينص فيه البطلان بأخر أحاطه المشرع بهذا الجزاء أمّا سنده غير المباشر فيتمثّل في فكرة العدالة. لمزيد من التّفصيل حول نشأة هذا المذهب راجع: أحمد الشّافعي، المرجع السّابق، ص 35 و ما بعدها.

لكن يتبين للقاضي بالنظر إلى الظروف الواقعية لهذه الحالة أنه لا مقتضى لهذا البطلان، و أن ثمة جزء أقل منه يمكن الإكتفاء به⁽¹⁾، لذا بات من الضروري الإستعانة بمذهب آخر.

ب) - مذهب البطلان الذاتي

أمّا البطلان الذاتي أو الجوهرية (Nullité substantielle) فمقتضاه أن الوسيلة لتقرير البطلان ليست تشريعية بمعنى وجود نص صريح يوجبه، و إنما الوسيلة إلى ذلك قضائية⁽²⁾، فجوهر هذا المذهب هو اعتراف الشارع للقاضي بسلطة تقديرية في تحديد القواعد التي يترتب البطلان على مخالفتها، و تمييزها عن القواعد التي لا يبطل الإجراء المخالف لها، و يضع الشارع معيارا مجردا يستعين به القاضي على هذا التمييز، و يقوم هذا المعيار في الغالب من التشريعات على التفرقة بين القواعد الإجرائية الجوهرية، و القواعد الإجرائية غير الجوهرية و تقرير البطلان جزاء لمخالفة الأولى دون الثانية⁽³⁾.

و يتميز هذا المذهب بالمرونة حيث يستطيع القاضي و هو على اتصال بالوقائع في كل حالة أن يوازن بين أهمية المخالفة و الجزاء الذي يترتب عليها، فيترك لتقدير القضاة بالنسبة للإجراءات الجوهرية التي يجازى عليها البطلان.

على أنه يعاب على هذا المذهب صعوبة وضع معيار للتمييز بين "القاعدة الجوهرية" و "القاعدة غير الجوهرية" مما يفسح المجال للإجتهاادات الفقية و القضائية، و هذا الأمر سوف يدخل القضاء في حالة عدم اليقين، مما يجعل مخالفته للضمان الجوهري في إحدى القضايا سببا للبطلان و في غيرها من القضايا عديم الأثر، و لا شك أن افتقار الجزاء الإجرائي إلى التحديد يمس إحترام مبدأ الشرعية التي تقتضى اليقين، كما أنه يمس بمبدأ المساواة أمام الخصوم حيث يقضى بالبطلان لصالح البعض و لا يقضى به لصالح الآخرين طالما كان

(1) محمود نجيب حسني، المرجع نفسه، ص 394.

(2) مقتضى هذا المذهب وجوب القول بالبطلان كلما كان الإجراء المعيب منظويا على وجه عام على إهدار القواعد الجوهرية و خاصة ما تعلق منها بالإعتداء على الحريات الفردية و الإخلال بحقوق الدفاع و يطلق عليه أحيانا بالبطلان الأساسي أو الجوهري، و يجري عليه القضاء الفرنسي في اتجاهه الغالب بالنسبة لمخالفة قواعد الموضوع في الإجراءات فيقضى بالبطلان كلما كان الإجراء المعيب جوهريا بغير حاجة إلى نص صريح. أنظر: رؤوف عبيد، نوع بطلان التفتيش في القانون المصري، المرجع السابق، ص 25.

(3) محمود نجيب حسني، المرجع السابق، ص 396.

الأمر متروك لتقدير القاضي⁽¹⁾، فهي عقبة كؤود قد ينتج عنها اختلاف وجهات النظر و تضارب في الأحكام.

و إذا كان ذلك الذي سلف، فإنّ الإمتداد الطبيعي للتساؤل المثار حول مذاهب البطلان من حيث مقوماتها و مبادئها، يدفعنا إلى التساؤل في ضوء ذلك عن المذهب الذي إعتنقه المشرع الجزائري؟ و هل وضع فعلا تنظيما وافيا لأحكام البطلان؟

ثالثا: الموقف التشريعي من مذاهب البطلان

لم يضع قانون الإجراءات الجزائرية الجزائري نظرية عامة في شأن البطلان، و كلّ ما فعله أنّه أورد بعض نصوص متفرقة ترتب البطلان جزاء مخالفة ما استوجبته تلك النصوص من قواعد، فاعتنق المشرع نظريتي البطلان الذاتي و البطلان القانوني عندما نصّ في المادة 159 من قانون الإجراءات الجزائرية "يترتب البطلان أيضا على مخالفة الأحكام الجوهرية المقررة في هذا الباب خلاف الأحكام المقررة في الماديتين 100 و 105 إذا ترتب على مخالفتها إخلال بحقوق الدفاع أو حقوق أيّ خصم في الدّعى و تقرّر غرفة الإتهام ما إذا كان البطلان يتعيّن قصره على الإجراء المطعون فيه أو امتداده جزئيا أو كليا إلى الإجراءات اللاحقة له".

و يمكن القول أنّ أغلب التشريعات تميل إلى الأخذ بمذهب البطلان الذاتي كالتشريع المصري و التشريع الليبي (المادة 304 من قانون الإجراءات الجزائرية)، و التشريع المغربي (المادة 769) و التشريع الكويتي (المادة 146) و التشريع الإماراتي (المادة 221) و توجب هذه التشريعات خضوع العمل الإجرائي المعيب و المؤثر في الحكم و الضار بحقوق الدفاع أو مصالح الخصوم لجزاء تقرره الجهة القضائية التي يرفع إليها الطعن بالبطلان⁽²⁾.

أمّا المشرع الفرنسي فقد هجر تقريبا نظرية البطلان القانوني، و كرّس بصور القانون رقم 93-1013 المؤرخ في 24 أوت 1994 نظرية البطلان الذاتي، فوفقا للمادة 171 من قانون الإجراءات الجزائرية يتحقّق البطلان عندما يترتب على إغفال إجراء جوهري منصوص عليه في قانون الإجراءات الجزائرية، أو أيّ نصّ إجرائي آخر فيه مساس بحقوق الطّرف الذي

(1) أحمد فتحي سرور، الشريعة الدستورية و حقوق الإنسان في الإجراءات الجنائية، المرجع السابق، ص 371.

(2) علي حسن محمد الطّالبة، المرجع السابق، ص 169.

يتعلّق به الإجراء⁽¹⁾، و هذا لا يعني أنّه قد أهمل كلية نظرية البطلان القانوني فقد حافظ عليها في مواضع كثيرة من قانون الإجراءات الجزائية، و هو مفترض طبيعي أن يتدخّل بالنص على حالات البطلان جزاء مخالفة قواعد راسخة تتعلّق بالنظام العام.

و الجمع بين النظريتين في النظام القانوني الواحد هو محل إجماع بين الفقه، فإلى جانب النص تشريعياً على حالات معيّنة للبطلان يُترك لتقدير القاضي فرصة ترتيب هذا الجزاء على مخالفة يقدر القاضي أهميتها خاصّة في ضوء واقع الدّعى التي ينظرها، لكن السّؤال الذي يتبادر إلى الذّهن في هذا الصّدّد ما هو المعيار الذي يهتدي به القاضي لتفريق بين "الإجراء الجوهري" و "الإجراء غير الجوهري" كمعيار للحكم بالبطلان؟، لا شك أنّ السّؤال حاسم لأنّ الكشف عن هذا المعيار يعني تحديد نطاق البطلان و رسم الخط الفاصل بين الإجراءات التي تفضي مخالفتها إلى بطلانها و تجريدها من أثرها القانوني و بين تلك التي تبقى صحيحة منتجة لأثارها القانونية و لو تمت مخالفتها⁽²⁾.

الحقيقة أنّ الفقه اختلف بشأن وضع معيار دقيق للتفرقة بين القواعد الجهرية و غيرها، و قد تعدّدت الضّوابط التي يمكن الإستهداء بها بشأن معرفة ما إذا كان الإجراء جوهرياً يجازى عليه بالبطلان أم أنّه إجراء تنظيمي لا يترتّب مثل هذا الأثر.

فيرى جانب من الفقه أنّ شروط صحة العمل الإجرائي في الخصومة الجنائية ليست إلّا ضمانات لاحترام الحرّية الشخصية و غيرها من حقوق الإنسان للوصول إلى محاكمة قانونية منصفة، فهي الضّمانات التي يتطلّبها الدّستور و القانون لحماية هذه الحقوق و التي أكدتها الشّريّة الإجرائيّة باعتبارها الشّريّة الدّستورية في الإجراءات الجزائية، و قد ترجم القانون هذه الضّمانات في صورة شروط لصحة الإجراءات الجنائية سواء كانت شروطاً شكلية أو موضوعية، و هنا يجب التّمييز بين هذه الشّروط الجهرية التي هي في جوهرها ترجمة لهذه الضّمانات، و بين بعض القواعد الإرشادية التّظيمية التي لا تنطوي على حماية هذه الحقوق، بل لتنظيم الأمور و حسن سيرها و لا يترتّب عليها البطلان⁽³⁾.

(1) ياسر الأمير فاروق، المرجع السابق، ص 604.

(2) عادل عبد البديع آدم حسين، المرجع السابق، ص 147.

(3) و يلخص الفقيه أحمد فتحي سرور الفارق بينهما في قوله "أمّا ما عبّر عنه القانون بالإجراء الجوهري ينصرف مدلوله إلى الضّمان الجوهري، و هو الضّمان الذي يحمي الحرّية الشخصية و سائر حقوق الإنسان في الخصومة الجنائية وفقاً للشّريّة الإجرائيّة، أمّا الإجراء غير الجوهري فينصرف مدلوله إلى الضّمان غير الجوهري الذي يحمي تنظيم الدّليل دون قبوله أيّ مشروعيته"، أحمد فتحي سرور، المرجع السابق، ص 374.

بينما نجد أنّ المذكرة الإيضاحية لنص المادة 332 من قانون الإجراءات الجنائية المصري⁽¹⁾، قد بيّنت معيار البطلان فنصت "للتعرف على الأحكام الجوهرية يجب دائماً الرجوع إلى "علّة التشريع" فإذا كان الغرض منه المحافظة على مصلحة عامة أو مصلحة المتهم أو غيره من الخصوم فإنّه يكون جوهرياً و يترتب على مراعاته البطلان"، و جوهر هذه الفكرة هي الرجوع إلى علّة التشريع، أي أنّ هذا المعيار قوامه فكرة "المصلحة"، هل القاعدة تستهدف حماية مصلحة بحيث يترتب على مخالفتها إهدار تلك المصلحة، أم هي تستهدف مجرد الترتيب و الإرشاد من وجهة نظر الملائمة فحسب بحيث لا يترتب على مخالفتها تضييع مصلحة ما، و على هذا النحو كان ضابط القاعدة الجوهرية هو "المصلحة"، و ضابط القاعدة الإرشادية "الملائمة"⁽²⁾، أي إذا اعتبرنا أنّ غاية الإجراء هي تحقيق مصلحة فكان من شأن عيبه أن جعله لا يحقّق هذه الغاية⁽³⁾.

(1) تنصّ المادة 332 من قانون الإجراءات الجنائية المصري "إذا كان البطلان راجعاً لعدم مراعاة أحكام القانون المتعلقة بتشكيل المحكمة أو بولايتها بالحكم في الدّعى أو باختصاصها من حيث نوع الجريمة المعروضة عليها أو بغير ذلك مما هو متعلّق بالنظام العام، جاز التمسك به في أية حالة كانت عليها الدّعى، و تقضي به المحكمة و لو بغير طلب".

(2) محمود نجيب حسني، المرجع السابق، ص 399.

(3) و نفيها على ذلك يطرح الفقه تساؤلاً مؤداه هل يجب الحكم بالبطلان لمجرد مخالفة قاعدة تتعلّق بالإجراء الجوهرية المطلوب إتخاذه أم أنّ هذا الأثر لا يترتب إلاّ بالنسبة للقواعد الجوهرية للإجراء الجوهرية ذاته؟ في معرض الإجابة على هذا التساؤل يرى الفقه أنّ الضابط في ذلك يتوقّف على التفرقة بين "القواعد الموضوعية للإجراء" و "القواعد الشكلية" له. فالقواعد الموضوعية اللازمة لصحة الإجراء أو التي تعرف بالشروط اللازمة لنشوء "حق إتخاذ الإجراء" هي "السبب" و "المحل" و "أهلية" من يمارس الإجراء من حيث الإختصاص تعتبر جوهرية، فالقانون حين يستلزم لصحة الإجراء ضرورة وقوعه من شخص له صفة معيّنة و هو ما يعبر عنه بالأهلية الإجرائية و بتوافر سبب معيّن و ينصّب على محل معيّن و أن يباشر في ظروف معيّنة، فإنّ جميع هذه الإجراءات المتعلّقة "بالوجود القانوني للإجراء" تعتبر جوهرية، ذلك أن تخلف أحد هذه الشروط الموضوعية يؤثّر على الغاية المبتغاة من الإجراءات و بالتالي يترتب عليها البطلان، أمّا بالنسبة للقواعد الشكلية و هي تلك التي يصاغ فيها الإجراء الجوهرية فيثور بصددها كذلك أهمية التفرقة بين القواعد الجوهرية و القواعد التنظيمية، فالقانون يأخذ بمبدأ شرعية الأشكال الإجرائية و القصد من ذلك ضمان غاية معيّنة تتعلّق بالمصلحة العامة أو بمصلحة الخصوم و من هذه الأشكال ما هو جوهرية و ما هو إرشادي تبعاً لذلك، و يرجع في تحديد المقصود بالمصلحة العامة و مصلحة الخصوم إلى العلّة من التشريع، فعلة التشريع هنا هي الغاية من الشكل في العمل الإجرائي أي مقتضى معيار التقريب بينهما يكمن في مدى تأثير هذه القواعد الشكلية على الهدف الذي أراده المشرّع من النصّ على الإجراء، فإذا كانت الشكليات التي يتطلّبها القانون من شأن تخلفها أن يفقد فاعليته في تحقيق الهدف منه كان الشكل جوهرياً، أمّا إذا لم يكن لها هذا الأثر كانت القاعدة من القواعد التنظيمية التي يقتصر دورها على مجرد إرشاد القضاء أو أطراف الدّعى إلى الوضع أو

واقع الأمر أنّ ضابط "المصلحة" أو ضابط "الملاءمة"، هي ضوابط لا تضع تفرقة واضحة المعالم بين الإجراءات الجوهرية التي يجازى عليها بالبطلان، و تلك التي ينظر إليها على أنّها ثانوية أو غير جوهرية لا يترتب على مخالفتها أيّ بطلان، لذا ظلّ الاختلاف قائماً بهذا الشأن، مما دفع بعض الفقه إلى محاولة رصد معايير أخرى للتّمييز بين الإجراءات الجوهرية و الإجراءات الإرشادي كميّار "المصلحة العامة في حسن سير الجهاز القضائي" و معيار "مصلحة الخصوم" و معيار "إحترام حقوق الدّفاع" و معيار " الغاية من الإجراء"⁽¹⁾، أما الجانب الآخر من الفقه فهو ينتقد أصلاً مسألة التفرقة بين الإجرائين من المبدأ⁽²⁾.

رابعاً: تقسيمات البطلان

ليس للبطلان كجزء إجرائي نوع واحد سواء كان بطلانا قانونياً أو بطلانا ذاتياً، فهناك تقسيمات مختلفة لهذا الجزء وفقاً لمعايير مختلفة، حيث يتوقف على تحديد نوع البطلان اللاحق بالعمل الاجرائي تحديد ما يترتب عنه من آثار تنعكس بشكل مباشر على القيمة القانونية للأدلة الجنائية المستمدة و هي مسألة غاية في الأهمية، ما يستوجب منا بيان صور هذا الجزء الإجرائي (أ)، و رصد معايير التّمييز بينهما (ب)، و أهميته (ج).

الأسلوب الملائم أو الأفضل من الوجهة العملية لنظر الدّعوى و بالتالي لا يترتب على مخالفتها البطلان. لمزيد من التّفصيل: راجع: مأمون سلامة، المرجع السّابق، ص 341، و أنظر أيضاً: هلاي عبد الله أحمد، النّظرية العامة للإثبات الجنائي، المرجع السّابق، ص 592.

(1) راجع تفصيلاً في هذا الموقف الفقهي: مأمون سلامة، المرجع السّابق، ص 238-247.

(2) تعرّضت الفرقة بين الإجراءات الجوهرية و الإجراءات التّنظيمية كأساس للحكم بالبطلان إلى النّقد، على سند من القول بأنّ جميع ما نصّ عليه من قواعد في قانون الإجراءات الجنائية قد إبتغى به المشرّع غرضاً معيّناً يهدف به في النّهاية إلى تحقيق العدالة الجنائية بين أفراد المجتمع، فهو لم يضمن نصوصه قواعد للعبث و إنّما لإعمالها في الواقع و إذًا فالقول بأنّ من بين قواعد الإجراءات الجنائية ما هو غير جوهرية و لكن قصد به التّنظيم فقط و لا يترتب على مخالفتها أيّ بطلان هو أمر ينبغي إطراحه إطلاقاً، و لا جدال في أنّه من غير الميسور النّص بكلّ قاعدة إجرائية على إثر مخالفتها و لذا ينبغي وضع قواعد عامة لتنظيم البطلان، و هي تقتضي بداءة تقسيم الإجراءات لتتنوّي تحت كلّ نوع منها ما يتحد في الأثر عند مخالفتها. لمزيد من التفصيل حول هذه المسألة راجع: حسن صادق المرصفاوي، المرجع السّابق، ص 764.

أ- أنواع البطلان

يمكن التمييز بين نوعين من البطلان، البطلان المطلق (1)، و البطلان النسبي (2).

1- البطلان المطلق

يجري العمل على إطلاق وصف "المطلق" على البطلان المتعلق بالصالح العام أو النظام العام، و وصف "النسبي" على البطلان المتعلق بمصلحة الخصوم، و هو أمر لا ضرر منه في النهاية رغم عدم دقته، حيث إنّ معيار النظام العام هو السائد في تمييز البطلان المطلق من النسبي، كما أنّ البطلان المطلق يلتقي مع البطلان المتعلق بالنظام العام في خصائصه الرئيسية⁽¹⁾.

و البطلان المطلق هو البطلان الذي يتقرر جزاء لمخالفة قاعدة إجرائية تتعلق بالنظام العام أي تستهدف بالدرجة الأولى تحقيق مصلحة عامة⁽²⁾، و لم يكن الغرض منها إبتداء مصلحة الخصوم حتى و لو أسفر مراعاة تلك القاعدة عن تحقيق مصلحة لأحد الخصوم في الدعوى، طالما أنّ هذه المصلحة لم تكن الهدف الأساسي للقاعدة، و إنّما تأتي في المرتبة الثانية تبعا لمصلحة المجتمع⁽³⁾.

الحقيقة أنّه بتأمل نصوص قانون الإجراءات الجزائية الجزائري فإننا نجده يخلو من الإشارة إلى البطلان المطلق أو البطلان المتعلق بالنظام العام، في حين فإنّ قضاء المحكمة العليا يستعمل في قراراته مصطلح البطلان المتعلق بالنظام العام، بدلا من البطلان المطلق⁽⁴⁾، في حين إستعمل القانون المدني لفظ البطلان المطلق.

أمّا المشرع المصري فقد حاول أن يحدّد مفهوم و معنى هذا البطلان و خصائصه، فأورد بعض الحالات المتعلقة بذلك، على سبيل المثال بموجب المادة 332 من قانون الإجراءات الجنائية المصري التي جاء فيها: "إذا كان البطلان راجعا لعدم مراعاة أحكام

(1) هلاي عبد الله أحمد، المرجع السابق، ص 610.

(2) فوزية عبد الستار، المرجع السابق، ص 39.

(3) سامي حسني الحسيني، المرجع السابق، ص 403.

(4) قرار المحكمة العليا صادر في 2005/12/21 عن الغرفة الجنائية طعن رقم 391134 المجلة القضائية للمحكمة العليا العدد 02 سنة 2006. "يعتبر أداء الشاهد اليمين، في حالة عدم وجود مانع قانوني من آدائها، من النظام العام، و يؤدي إغفال ذلك إلى بطلان الإجراءات و بالتالي الحكم".

القانون المتعلقة بتشكيل المحكمة أو بولايتها بالحكم في الدّعى أو باختصاصها من حيث نوع الجريمة المعروضة عليها أو بغير ذلك مما هو متعلّق بالنّظام العام، جاز التّمسك به في أيّة حالة كانت عليها الدّعى، و تقضي به المحكمة و لو بغير طلب".

(2) - البطلان النسبي

إذا كان البطلان المطلق يتعلّق بالنّظام العام و يرمي إلى حماية المصلحة العامة في المجتمع، فإنّ البطلان المتعلّق بمصلحة الأطراف قد وضع لحماية مصلحة أطراف الدّعى و المحافظة عليها و تقرير ضمانات لها، و عليه فإنّ كلّ بطلان لا يتعلّق بالنّظام العام هو بطلان نسبي⁽¹⁾، أي أنّ البطلان النسبي هو البطلان الذي يقع نتيجة عدم مراعاة الأحكام الإجرائيّة المتعلّقة بمصلحة الخصوم⁽²⁾، و يستخلص من ذلك أنّ الضّابط في البطلان النسبي أنّه البطلان الذي ينال الإجراء المخالف لقاعدة تحمي مصلحة يقدر القضاء أنّها أقلّ أهميّة من أن تبرّر البطلان المطلق⁽³⁾.

و إذا عدنا إلى التّشريع الجزائري، فإنّه حدّد حالات البطلان النسبي بأنّها ما ليست من البطلان المطلق و يتجلّى ذلك من خلال نص المادة 159 من قانون الإجراءات الجزائية - المقابل لنص المادة 172 من قانون الإجراءات الجزائية الفرنسي⁽⁴⁾ - الذي جاء فيه "يترتب البطلان أيضا على مخالفة الأحكام الجوهرية المقرّرة في هذا الباب خلاف الأحكام المقرّرة في المادتين 100 و 105 إذا ترتّب على مخالفتها إخلال بحقوق الدّفاع أو حقوق أيّ خصم في الدّعى..."، و هو موقف محل نقد لأنّه ضيق نطاق دائرة البطلان النسبي على مخالفة الأحكام الجوهرية المقرّرة في باب التّحقيق، و كان الأولى بالمشرّع ترتيب البطلان متى وقعت

(1) أحمد الشّافعي، المرجع السّابق، ص 61.

(2) محمد أمين الخرشنة، مشروعية الصّوت و الصّورة في الإثبات الجنائي، الطّبعة الثّانية، دار النّقافة للنّشر و التّوزيع، الأردن، 2015، ص 232.

(3) محمود نجيب حسني، المرجع السّابق، ص 404.

(4) Article 172 Modifié par Loi n°93-2 du 4 janvier 1993 - art. 71 JORF 5 janvier 1993 en vigueur le 1er mars 1993 : " Il y a également nullité lorsque la méconnaissance d'une formalité substantielle a porté atteinte aux intérêts de la partie qu'elle concerne.

La partie envers laquelle une formalité substantielle a été méconnue peut renoncer à s'en prévaloir et régulariser ainsi la procédure. Cette renonciation doit être expresse. Elle ne peut être donnée qu'en présence de l'avocat ou ce dernier dûment appelé. »

مخالفة للقواعد الجوهرية خلال كافة المراحل الإجرائية دون قصرها على مرحلة التحقيق القضائي و قد إستدرك المشرع الفرنسي ذلك من خلال التّعديل الملحق على النصّ. و ظاهر من خلال أحكام البطلان التي تضمّنها قانون الإجراءات الجزائية الجزائري أنّه لم يساعد كثيرا في حل مشاكل البطلان بقدر ما زادها تعقيدا، و السّؤال الذي يظلّ باقيا إذا كانت أغلب حالات البطلان سواء المطلق أو النسبي ترجع إلى مذهب البطلان الدّاتي أي لتقدير القاضي، فما هو المعيار الذي يهتدي به هذا الأخير في التّمييز بين النوعين طالما أنّ المشرّع لم يرصد معيارا ثابتا؟

ب)- معيار التمييز بين البطلان المطلق و البطلان النسبي

الحقيقة أنّ الجواب على هذا التساؤل ليس محل إجماع بين الفقه⁽¹⁾، و يمكن إجمال آراء الشراح حيال هذه المسألة في موقفين:

الإتجاه الأوّل: معيار نوع المصلحة التي تحميها القاعدة القانونية

يعتمد هذا المعيار على أساس نوع المصلحة التي تحميها القاعدة الإجرائية لتحديد نوع البطلان، فإذا كانت القاعدة الإجرائية تهدف إلى حماية مصلحة عامة، فالبطلان المترتب على مخالفتها مطلق، أمّا إذا كانت تهدف إلى حماية مصلحة الخصوم، فإنّ البطلان المترتب

(1) هناك رأي ينتقد أصلا التّمييز بين النوعين من البطلان حيث يرى أنّ تقسيم البطلان إلى بطلان مطلق و بطلان نسبي ليس له ما يبرّره في مجال الأعمال الإجرائية، بل إنّ التفرقة ذاتها بين البطلان المطلق و البطلان النسبي عدت تفرقة تقليدية في نطاق القانون المدني و استعارة هذا التقسيم و إعماله في قانون الإجراءات الجزائية يؤدي إلى نتائج لا تستقيم مع فكرة بطلان العمل الإجرائي. فالبطلان المطلق وفقا لهذا التقسيم التقليدي يعني بطلان العمل في ذاته و حكم القاضي بالبطلان ليس إلّا حكما كاشفا و مقرّرا عن هذا العيب الذي إعتري الإجراء منذ البداية، أمّا البطلان النسبي أو كما يقال "قابلية الإجراء للبطلان" فيعني صيرورة الإجراء صحيحا منتجا لآثاره حتّى يحكم القاضي بهذا البطلان فالحكم بالبطلان هو حكم منشئ، و لعلّ أهم نتيجة تترتب على هذا التصور التقليدي، أنّ البطلان المطلق لا يجوز تصحيحه، بينما يقبل البطلان النسبي التصحيح و هذه الأحكام لا تستقيم مع فكرة بطلان الإجراء الجنائي، فبطلان الإجراء الجنائي يجوز تصحيحه بحجية الأمر المقضي فيه، و بالتّالي يصعب نعت مثل هذا البطلان بالمطلق. أنظر تفصيلا: عادل عبد البديع آدم حسين، المرجع السّابق، ص 162.

على مخالفتها هو بطلان نسبي⁽¹⁾، و مثال ذلك القواعد المتعلقة بسرّية التحقيق لا تتعلّق بالنّظام العام بل بمصلحة الأطراف⁽²⁾.

فيرى هذا الجانب من الفقه أنّ المعيار الذي يحتذى به في ذلك هو بالمصلحة التي أراد المشرّع تحقيقها بالقاعدة الإجرائيّة، ذلك أنّ كلّ قاعدة إجرائيّة إنّما ينص عليها المشرّع حماية لمصلحة معيّنة، و هكذا فإنّ الضّابط السّليم في هذا المجال هو الإعتداد بالمصلحة المبتغاة من القاعدة، فإذا كانت هذه المصلحة تتعلّق بضمان حسن سير و فاعلية الجهاز القضائي لتحقيق العدالة الجنائية كانت القاعدة متعلّقة بالنّظام العام، و يندرج تحت تلك القواعد ما يتعلّق بعنانية الجلسات و القواعد الخاصة بتسبيب الأحكام و طرق الطّعن فيها⁽³⁾.

الإتجاه الثاني: معيار أهمّية المصلحة التي تحميها القاعدة الإجرائيّة

يرى جانب من الفقه أنّ "نوع المصلحة" ليس معيارا حاسما للتمييز بين نوعي البطلان، بل إنّ الضّابط الصّحيح في التّمييز بينهما هو "أهمّية المصلحة" التي تحميها القاعدة الإجرائيّة و ليس نوعها، و قاضي الموضوع هو الذي يناط به تحديد هذه الأهمّية، فالقاعدة التي تحمي مصلحة قدرّ القاضي أهميتها يترتّب على مخالفتها البطلان المطلق⁽⁴⁾، و يستوي أن تكون مصلحة عامة في تنظيم القضاء و حسن سيره، أو مصلحة هامة للمتهم أو غيره من الخصوم أو يرمي إلى حسن سير العدالة⁽⁵⁾.

(1) حسن صادق المرصفاوي، المرجع السّابق، ص 824.

(2) Cass Crim, 27 avril 2000, n° 00-80.420, Bull. Crim 2000, n° 170.

(3) هلاي عبد الله أحمد، المرجع السّابق، ص 614.

(4) إنّ العبرة في تحديد نوع البطلان ليس بنوع المصلحة التي تحميها القاعدة الإجرائيّة - مصلحة متعلّقة بالنّظام العام أو مصلحة متعلّقة بالخصوم - و إنّما العبرة بأهمّية المصلحة المحمية، ذلك أنّ أغلب قواعد الإجراءات الجنائية تستهدف في ذات الوقت تحقيق كلا المصلحتين - المصلحة العامة و مصلحة الخصوم - و لذلك يتعدّد عندئذ تحديد ما إذا كانت مخالفة القاعدة الإجرائيّة ترتّب البطلان المطلق أو البطلان النسبي، أمّا إذا كان الضّابط في تحديد نوع البطلان هو أهمّية المصلحة المحمية فإنّه يكون من اليسر أن نقرّر أنّ البطلان يكون مطلقا إذا كانت القاعدة تستهدف بالدرجة الأولى المصلحة العامة، و يكون نسبيا إذا كان هدفها الأول تحقيق مصلحة الخصوم. أنظر محمود نجيب حسني، المرجع السّابق، ص 403 - فوزية عبد السّتار، المرجع السّابق، ص 41.

(5) قرار المحكمة العليا صادر في 1983/11/29 عن الغرفة الجنائية الأولى طعن رقم 34094 المجلة القضائية للمحكمة العليا، العدد الرابع، سنة 1989 - قرار المحكمة العليا صادر في 1987/03/10 عن الغرفة الجنائية الأولى طعن رقم 4881 المجلة القضائية للمحكمة العليا، العدد الثّالث، سنة 1989 - قرار المحكمة العليا صادر في

يمكن القول بشكل عام أنّ حقوق الدّفاع الأساسية و ما تستوجبه قرينة البراءة من ضمانات للمتهم في حفظ حقه في الخصوصية و الكرامة البشرية و ما يتفرّع عنها من حقوق لصيقة بالشّخصية الإنسانية هي قواعد هامة و ينبني على مخالفتها البطلان المطلق و مثال ذلك القواعد المتصلة بحقوق الدّفاع أو المتعلقة بإجراء الحبس المؤقت⁽¹⁾، أو إجراءات تمديده⁽²⁾.

في ضوء ذلك فإننا نؤيّد مذهب بعض الفقه الذي ينادي بوجود تبني معيارا مزدوجا يجمع بين نوع "المصلحة" و "أهميتها"، و يتمّ التّوصل إلى ذلك من خلال أمرين. الأمر الأول، ضرورة أن يكون هدف القاعدة الإجرائيّة يتصل إتصالا مباشرا إمّا بالضمانات الأساسية المتعلقة بحماية الإنسان في جسده أو حياته الخاصة أو حرّيته الشّخصية أو في الدّفاع عن نفسه، و إمّا بالضمانات التي تتعلّق بالتنظيم القضائي. أمّا الأمر الثّاني، فهو أن يكون قصد المشرّع من وضع القاعدة الإجرائيّة هو المحافظة على هذه الضمانات تحقيقا للصّالح العام و يستوي في تحقيق الصّالح العام أن تكون المصلحة المحمية تتعلّق بالتنظيم القضائي أم تتعلّق بمصلحة هامة و أساسية للمتهم كما هو الحال في وجوب تعيين محام للمتهم في جناية و أيضا الإستجواب قبل الحبس المؤقت⁽³⁾.

و إذا فرغنا من تحديد معايير التّفريق بين البطلان المطلق و البطلان النسبي فإنّ أهمّ سؤال يطرح في هذا الصّدّد يتعلّق بالأهميّة العملية المرجوة في التّفريق بين هذين النوعين من البطلان؟

(ج) - أهمية التّمييز بين البطلان المطلق و البطلان النسبي

إنّ التّمييز بين البطلان المطلق و البطلان النسبي هو تمييز هام يرتّب آثارا عملية خطيرة في إجراءات التّقاضي الجنائي، و تختلف تلك الآثار من الوجوه الأربعة الآتية:

1987/03/10 عن الغرفة الجنائية الأولى طعن رقم 4881، المجلة القضائية للمحكمة العليا، العدد الثّالث، سنة 1989. مشار إليهم لدى: أحمد الشّافعي، المرجع السّابق، ص 39.

(1) Cass Crim, 4 janv. 1996, n° 95-84.330, Bull. crim 1996, n°5.

(2) Cass Crim, 30 janv. 2001, n° 00-87.155, Bull. crim 2001, n°26.

(3) هلاي عبد الله أحمد، المرجع السّابق، ص 612.

1- من حيث صاحب الحق في التمسك بالبطلان:

فلكلّ ذي مصلحة أن يتمسك بالبطلان المتعلّق بالنظام العام أمّا البطلان المتعلّق بمصلحة الخصوم فلا يجوز لغير ذي الشأن التمسك به.

2- من حيث التنازل أو التمسك بالبطلان:

لا يجوز التنازل عن التمسك بالبطلان المتعلّق بالنظام العام و لا يصحّ رضا الخصوم بالإجراء الباطل أمّا البطلان المتعلّق بمصلحة الخصوم فلصاحب الشأن أن يتناول صراحة أو ضمنا.

3- من حيث سلطة القاضي في تقرير البطلان:

فالقاضي يملك القضاء بالبطلان من تلقاء نفسه و لو بغير طلب، متى تعلّق ذلك بالبطلان من النظام العام و لا يميل هذا في شأن البطلان المتعلّق بمصلحة الخصوم إذ هو لا يستطيع تقريره إلّا إذا تمسك به من تقرّر لمصلحته.

4- من حيث الوقت الذي يجوز فيه التمسك بالبطلان:

يجوز التمسك بالبطلان المتعلّق بالنظام العام و لو لأوّل مرة أمام محكمة النقض ما دام ذلك لا يتطلّب تحقيقا موضوعيا و لا يجوز ذلك في شأن البطلان المتعلّق بمصلحة الخصوم فما لم يتمسك صاحب الحق فيه أمام محكمة الموضوع سقط حقه في إبدائه⁽¹⁾.

و إذ إنتهينا من بيان مذاهب البطلان في التشريعات الإجرائيّة المختلفة فإنّ السؤال المطروح يتعلّق بطبيعة البطلان الذي يلحق إجراء التفتيش عن الأدلة المعلوماتيّة؟

(1) و هذه الفروق ليست مسائل خلافية بل تجدها في كلّ فقه و قضاء يعرف التفرقة بين البطلان النسبي و البطلان المطلق سواء في نطاق الإجراءات الجنائية أم المرافعات المدنية، فكلّ بطلان منهما يرتب تلقائيا آثارا منها معنية بالذات على النحو الذي وضحناه ويرتّب عكسها تماما بغير تدخل بين النوعين و قد نصّت على هذه التفرقة صراحة بعض الشرائع كقانون الإجراءات الإيطالي و إنّما الأمر الوحيد الذي يصح أن يكون مثار خلاف بين الشرائع و الشراح هو في تعيين نوع البطلان الذي يصحّ أن يلحق مخالفة إجراء معيّن سواء مسّت هذه المخالفة نفس مشروعيته L'égalité أم طريقة القيام به Régularité أمّا تعيين آثاره فلم يكن يوما محل خلاف.

لمزيد من التفصيل حول معايير التفرقة بين البطلان النسبي و البطلان المطلق راجع : رؤوف عبيد، المرجع السابق، ص ص 26-27.

الفرع الثاني: طبيعة بطلان التفتيش عن الأدلة المعلوماتية

قدّمنا أنّ البطلان قد ينصّ المشرّع على تقريره صراحة جزاء مخالفة قاعدة معيّنة و قد يتقرّر دون نص إذا ما انصبّت المخالفة على قاعدة جوهرية، و قد يتعلّق أحدهما بالنظام العام و يتعلّق الثاني بمصلحة الخصوم، إزاء ذلك كلّه لابد من تحديد أحوال بطلان التفتيش عن الأدلة المعلوماتية في ضوء موقف التشريع (أولاً)، و الفقه (ثانياً)، و القضاء (ثالثاً).

أولاً: موقف التشريع من طبيعة بطلان التفتيش عن الأدلة المعلوماتية

سبق و أن توصلنا إلى أنّ البطلان معناه حرمان الإجراء المخالف للقانون من قيمته القانونية و إهدار جميع آثاره و إزالتها، لأنّ ما يخالف القانون لا يجوز أن تكون له قيمة في نظر القانون⁽¹⁾، إلّا أنّ هذا الأثر الإجرائي لا يترتب إلّا في حالة "البطلان المطلق" أو "البطلان النسبي" عند إثارته ممن تقرّر لمصلحته، و يجري التساؤل في ضوء هذه القاعدة عن طبيعة البطلان الذي يلحق التفتيش عن الأدلة المعلوماتية حال مخالفة أحكامه، هل هو بطلان مطلق أم بطلان نسبي؟

إنّ المتأمّل لنصوص القانون 04/09 المتضمّن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها يجده يخلو من الإشارة إلى البطلان الذي قد يترتب على مخالفة أحكام التفتيش عن الأدلة المعلوماتية، و هو موقف التشريع المقارن كالتشريع الفرنسي و التشريع البلجيكي، و كذا التشريعات العربية باستثناء التشريع اللبناني⁽²⁾،

(1) توفيق محمد الشاوي، المرجع السابق، ص 488.

(2) تنص المادة 127 من القانون اللبناني رقم 81 لسنة 2018 و المتعلّق بالمعاملات الإلكترونية و البيانات ذات الطابع الشخصي " تكون باطلة الأدلة المضبوطة أو المحفوظة خلافاً للأصول المحددة في هذا الفصل. تبطل تبعاً له إجراءات التحقيق المستندة إليه. إنّ البطلان لا يحول دون الأخذ بما توافر من معلومات تفيد التحقيق، بنتيجة الضبط أو المعالجة، إذا توافرت معها أدلة تؤيدها". و في الحقيقة فإنّ حكم هذه المادة يحتاج إلى تأمل قانوني ذلك أنّ الغاية من التشريع حين أوجب المحافظة على الأدلة المعلوماتية المضبوطة منعا من وقوع تغيير أو تعديل عليها إنّما قصد تنظيم العمل و المحافظة على الدليل لعدم تهوين قوّته في الإثبات، فالأمر مرجعه إلى إطمئنان المحكمة إلى سلامة هذا الدليل كغيره من عناصر الدّعى أي أنّ هذا الشرط وفق ما سبق التطرّق إليه هو شرط من شروط تقدير القيمة الإقناعية للدليل و ليس قيمته القانونية (المشروعية)، و الفرق بينهما يترتب عليه مسائل هامة في القانون كما سبق مناقشته في الفصل الأول من هذا الباب.

و مفاد موقف المشرع إذن أنّ التفتيش عن الأدلة المعلوماتية يخضع للأحكام العامة لبطلان التفتيش التقليدي و ليس له أحكام مستقلة يخضع لها.

بالرجوع الى نص المادة 159 من قانون الإجراءات الجزائية فإننا نجد أنّ المشرع قد حسم الخلاف نهائيا بشأن طبيعة بطلان التفتيش، بحيث ورد فيها: "يترتب البطلان أيضا على مخالفة الأحكام الجوهرية المقررة في هذا الباب خلاف الأحكام المقررة في المادتين 100 و 105 إذا ترتب على مخالفتها إخلال بحقوق الدفاع أو حقوق أيّ خصم في الدعوى و تقرّر غرفة الإتهام ما إذا كان البطلان يتعيّن قصره على الإجراء المطعون فيه أو امتداده جزئيا أو كليًا إلى الإجراءات اللاحقة له... و يجوز للخصم دائما التنازل عن التمسك بالبطلان المقرر لمصلحته وحده".

و صراحة هذا النص تقيّد على وجه الجزم أنّ بطلان التفتيش بصورتيه مادي و معلوماتي هو بطلان نسبي لا يتعلّق بالنظام العام، و ليس للمحكمة أن تقضي به من تلقاء نفسها، فالتنازل عن بطلان التفتيش يصحّحه، فأحكام التفتيش وردت في الباب الثالث من الكتاب الأول من قانون الإجراءات الجزائية التي نظّمها المشرع في المواد 44 إلى 49 و من 79 إلى 85 من قانون الإجراءات الجزائية، أي أنّ حكم المادة 159 من هذا القانون نطبق على جميع أحكام التفتيش بما فيها حالة تفتيش نظم المعلومات، و بالطبع فإنّ هذا البطلان هو بطلان قانوني كون المشرع حدّد حالات البطلان صراحة بمقتضى هذه النصوص التشريعية.

و بالعودة إلى المادة 48 من قانون الإجراءات الجزائية نجدها تنصّ على أنّه "يجب مراعاة الإجراءات التي استوجبها المادتان 45 و 47 و يترتب على مخالفتها البطلان"، و الضمانات المقررة بالمادة 45 من هذا القانون تتعلّق بحضور المتّهم أو تعيين من ينيبه في حالة غيابه عندما يتعلّق الأمر بتفتيش المساكن، و هذه الضمانة الإجرائية يجمع الفقه على اعتبارها مجرد إرشاد⁽¹⁾، الهدف منها هو زرع الثقة في الإجراء⁽²⁾.

(1) أحمد فتحي سرور، المرجع السابق، ص 374.

(2) توفيق محمد الشاوي، المرجع السابق، ص 449.

بل إنّ أحكام محكمة النقض المصرية تكشف أنّ القانون لم يجعل حضور المتّهم الذي يجرى التفتيش في مسكنه شرطاً جوهرياً لصحته، فهي لا ترتّب البطلان أصلاً جزاء هذه المخالفة⁽¹⁾.

أمّا الضّمّانات المقرّرة بنص المادة 47 من نفس القانون فتتعلّق بحظر تفتيش المنازل ليلاً، و رغم صراحة نص المادة 159 في تحديد طبيعة البطلان المترتّب جزاء مخالفة أحكام التفتيش بصفة عامة دون أن يردّ استثناء عليها، إلّا أنّ هناك من الفقه من يرى أنّ عدم مراعاة الأحكام المنصوص عليها بالمادتين 45 و 74 من قانون الإجراءات الجزائية ينجر عنه بطلان التفتيش بطلاناً مطلقاً، و حجته في ذلك أنّ نص المادة 48 من هذا القانون صريحة في تقريره⁽²⁾، و إن كنا نؤيد هذا الرّأي في توجيهه إلّا أنّنا نبدي قدراً من التّحفظ على مبرراته، ذلك أنّ صراحة النصّ على البطلان ليست معياراً للقول بكون القاعدة تتعلّق بالنظام العام، بل كلّ ما في الأمر أنّ البطلان في هذه الحالة هو بطلان قانوني.

إنّ موقف المشرّع الجزائري في الحقيقة مستوحى من التشريع الفرنسي، فهذا الأخير يعتبر قواعد التفتيش مقرّرة لحماية مصلحة الخصوم، و من ثمّ فإنّ مخالفتها يترتّب عليها البطلان النسبي تطبيقاً لنص المادة 59 من قانون الإجراءات الجزائية⁽³⁾، و هو أيضاً حال التشريع المصري التي تجسّده المادة 333 من قانون الإجراءات الجزائية⁽⁴⁾.

(1) الطعن رقم 209 لسنة 47 قضائية الصادر بجلسة 1977/06/5 مكتب فنى سنة 28، قاعدة 145، ص 691.

(2) عبد الله أوهابيه، ضمانات الحرّية الشخصيّة أثناء مرحلة البحث التمهيدي "الإستدلال"، رسالة دكتوراه، معهد الحقوق، جامعة الجزائر، 1992، منقول عن: أحمد الشّافعي، المرجع السابق، ص 103.

(3) Article 59 Modifié par Loi 93-1013 1993-08-24 art. 20 JORF 25 août 1993 en vigueur le 2 septembre 1993 « Sauf réclamation faite de l'intérieur de la maison ou exceptions prévues par la loi, les perquisitions et les visites domiciliaires ne peuvent être commencées avant 6 heures et après 21 heures.

Les formalités mentionnées aux articles 56, 56-1, 57 et au présent article sont prescrites à peine de nullité. »

(4) تنص المادة 333 من قانون الإجراءات الجزائية المصري " في غير الأحوال المشار إليها في المادة السابقة يسقط الحق في الدّفع ببطلان الإجراءات الخاصة بجمع الاستدلالات أو التّحقيق الإبتدائي أو التّحقيق بالجلسة في الجرح و الجنايات إذا كان للمتّهم محام و حصل الإجراء بحضوره بدون اعتراض منه. أمّا في مواد المخالفات فيعتبر الإجراء صحيحاً، إذا لم يعترض عليه المتّهم و لو لم يحضر معه محام في الجلسة. و كذلك يسقط حق الدّفع بالبطلان بالنسبة للنيابة العامة إذا لم تتمسك به في حينه".

ثانيا: موقف الفقه من طبيعة بطلان التفتيش عن الأدلة المعلوماتية

في حدود البحث الذي أجريناه فإنّ الفقه إلى غاية اليوم لا يزال يرجع أحكام بطلان التفتيش عن الأدلة المعلوماتية إلى أحكام بطلان التفتيش المادي لاسيما وأنّ المشرع لم يفرد أحكاما خاصة لبطلان التفتيش المعلوماتي، على نحو لا يزال الخلاف بين الفقهاء قائما الى غاية اليوم حول طبيعة البطلان في التفتيش عموما، فذهب رأي إلى القول بأنّ أحكام التفتيش تتعلق بمصلحة الخصوم (أ)، و ذهب البعض إلى القول بأنّ بطلان التفتيش يتعلّق بالنظام العام أي أنّه بطلان مطلق (ب)، و ذهب رأي آخر إلى أنّ بطلان التفتيش يتعلّق بالنظام العام عند مخالفة القواعد الموضوعية للتفتيش بينما هو نسبي عند مخالفة القواعد الشكلية (ج).

أ- الرأي القائل بالبطلان النسبي

غالبية الفقهاء من يذهب إلى القول بأنّ القانون قد إعتبر أحكام التفتيش من القواعد الأساسية المتعلقة بمصلحة الخصوم، و أنّ مخالفة تلك الأحكام يترتب عليه بطلان نسبي سواء تعلّق الأمر بمخالفة القواعد الشكلية للتفتيش أو القواعد الموضوعية. و من مبررات أصحاب هذا الرّأي أنّ الشّروط الخاصة بالتفتيش وضعت لحماية مصلحة الخصوم في عدم إنتهاك حرّيات مساكنهم و أشخاصهم و مراسلاتهم⁽¹⁾، فهي اذن غير مقررة لحماية المصلحة العامة.

و يضيف أنصار هذا المذهب أنّه إذا كانت هذه الحماية تتعلّق بالنظام العام إلا أنّ ذلك يأتي تبعا لحماية مصلحة الخصوم، و من ثمّ فإنّ رضا الشخص الذي تعرض للتفتيش يصحّ التفتيش الباطل⁽²⁾، و في نظر الفقه فإنّ هذا الموقف ينطبق على التفتيش عن الأدلة المعلوماتية أيضا من منطلق أنّ التفتيش المعلوماتي يخضع إلى النّظرية العامة للبطلان⁽³⁾.

(1) لمزيد من التفصيل حول هذا الخلاف الفقهي راجع: سامي حسني الحسيني، المرجع السابق، 411 و ما بعدها.

(2) فوزية عبد الستار، المرجع السابق، ص 308-309، أنظر أيضا: علي حسن الطّوالبة، المرجع السابق، ص 177

(3) هلاي عبد الله أحمد، تفتيش نظم الحاسب الآلي و ضمانات المثّم المعلوماتي، المرجع السابق، ص 234، و أنظر أيضا أسامة بن غانم العبيدي، المرجع السابق، 104.

و نحن من جانبنا لا نؤيد هذا الإتجاه على إطلاقه بل هناك قدر من التّحفظ لابد من إيراده، إذ من غير المعقول أن نجعل قواعد التفتيش كلّها من طبيعة واحدة، فإذا كان المشرع لم يحدّد القواعد التي ينجّر عن مخالفتها البطلان المطلق، فإنّه من غير المعقول إعتبار التفتيش المعلوماتي الذي يجرى بغير إذن من السّطة المختصة باطلا بطلانا نسبيا لأنّه يشكّل تعديا واضحا على الحريات الفردية مما تتأذى به المصلحة العامة، خاصة وأنّ عدا الضمان الإجرائي من الضمانات الدستورية، أو أن يجرى التفتيش دون أن ينهض سبب يبرّره، أو أن يرد على محل غير معيّن و غير قابل للتعيين، أو يجرى التفتيش بعد الميقات، أو تتجاهل السّطة حدود الإذن تجاهلا واضحا بتجاوز نطاق الإذن بشكل كبير فيصبح التفتيش المصرّح به حملة صيد لبيانات الفرد المستهدف⁽¹⁾، ففي كلّ هذه الفروض لم يراع المشرع مصلحة خاصة بالمتهم لضمان حرياته الفردية فحسب، فهذه الضمانات أيضا تهّم المصلحة العامة التي يضيرها إهدار ما تستوجبه قرينة البراءة و ما يتفرّع عنها من حقوق.

(ب) - رأي يعدّد حالات البطلان المطلق

و من بين الشّراح من ذهب إلى أنّ بطلان التفتيش يتعلّق بالنّظام العام إلاّ في حالة واحدة، و هي حالة عدم حضور شاهدين في التفتيش الذي يجريه مأمور الضبط القضائي إذا لم يمكن حضور المتهم أو من ينيبه، و ذلك على أساس أنّ القواعد المتعلقة بالنّظام العام هي تلك التي تتعلّق بالتنظيم القضائي و الأصول التي يقوم عليها النّظام الإجرائي و التي تحدّد شرعية الأعمال الإجرائية، فالقواعد الموضوعية هي من النّظام العام دائما أمّا القواعد الشكلية فهي تعتبر من النّظام العام متى كان النّظام الإجرائي يقتضي توفّرها و منها هذه القاعدة⁽²⁾.

(1) إنّ تجاوز نطاق التفتيش المعلوماتي أمر لا مفر منه لأسباب سبق الإستفاضة في شرحها، غير أنّ إستغلال سلطة التفتيش هذه الطبيعة التي عليها البيانات المخزّنة بتجاوز مستهدف التفتيش و استغلال هذه البيانات بسوء نية للتّوصل إلى أدلة أخرى تجعل التفتيش باطلا بطلانا مطلقا، و لا توجد في التشريع الأوروبي قاعدة تحضر هذا التّوسع، و عندما واجهت المحكمة الأوروبية هذا التّحدي قرّرت بطلان التفتيش المعلوماتي في هذه الحالة و وصفته بأنّه "مجرد حملة صيد fishing expedition"، و قد إستندت في قضائها على مبدأ استثناء الرّؤية الكاملة المقرّرة في القضاء الأمريكي لمزيد من التّفصيل راجع الحكم:

CEDH, Arrêt VINCI CONSTRUCTION ET GTM GÉNIE CIVIL ET SERVICES c.

FRANCE, 2 avril 2015, n° 63629/10 et 60567/10.

(2) أحمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجزائية، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، مصر 1959، ص 170-171، نقلا عن سامي حسني الحسيني، المرجع السابق، 411 و ما بعدها.

و قد إنتقد هذا الرأى لانتفاء أساسه في التشريع، بل إنتفاء حكمته، فلماذا يتعلّق بطلان التفتيش بالنظام العام في كلّ ضوابطه و أحكامه إلاّ في حالة واحدة، هي حالة عدم حضور الشاهدين في التفتيش الذي يجريه مأمور الضبط القضائي إذا لم يتم حضور المتهم أو من ينيبه؟ و ما علّة تخصيص هذه القاعدة الشكلية بحكم خاص من بين القواعد الشكلية الأخرى؟ و لماذا لا تخضع القواعد الشكلية برمتها لقاعدة موحّدة، مع لزوم هذا التّحديد و قيامه على منطوق واحد و حكمة مشتركة⁽¹⁾، و بناء عليه يمكن القول أنّ هذا الرأى أيضا فشل في إرساء ضابط مجرد لتحديد طبيعة بطلان التفتيش.

(ج) - الرأى الذي يفرّق بين القواعد الموضوعية و القواعد الشكلية

ذهب رأى من الفقه إلى أنّ البطلان الذي يلحق التفتيش هو بطلان يتعلّق بالنظام العام متى كان مترتّباً على مخالفة القواعد المتعلقة بتشكيل الهيئات القضائية و اختصاصها، و القواعد المتعلقة بحالات التفتيش (الشروط الموضوعية للتفتيش) بينما هو يتعلّق بمصلحة الخصوم إذا ما ترتّب على مخالفة القواعد الشكلية⁽²⁾.

ففي نظر هذا الجانب من الفقه فإنّ القواعد الموضوعية مقرّرة لمصلحة العدالة ذاتها لا لمصلحة الفرد و مخالفتها تشوب العمل بعدم المشروعية، و من الطّبيعي أن يعتبر البطلان المتعلّق بها من النظام العام، أمّا القواعد الشكلية فهي قواعد تنظيمية مقرّرة لمصلحة الخصوم و مخالفتها تشوب العمل بمجرد عدم الملاءمة، و من ثمّ ينبغي أن يكون البطلان المترتّب على تلك المخالفة نسبياً⁽³⁾.

(1) سامي حسني الحسيني، المرجع السابق، ص 415.

(2) توفيق محمد الشاوي، المرجع السابق، ص 447.

(3) ومن بين الحجج التي ساقها هذا الجانب من الفقه أنّ بطلان التفتيش لا يتعلّق بالنظام العام في كلّ الأحوال و الحالات لتعارض ذلك مع نص القانون، و لا يتصور أنّ مخالفة القواعد التي وضعت لحماية حرّيات عامة كفلها الدستور، كالحريّة الشخصية و حرمة المسكن و الرسائل ترتّب بطلاناً نسبياً في كلّ الأحوال، وإلاّ فمتى يترتّب البطلان المتعلّق بالنظام العام؟ إنّما ينبغي التفرقة بين القواعد الموضوعية للتفتيش و القواعد الشكلية له، فالأولى يترتّب على مخالفتها بطلاناً متعلّقاً بالنظام العام لأنّها تفقد الإجراء مقومات الحق في مباشرته، و يكون بالتّالي إعتداء غير شرعي على الحرّيات العامة. بينما مخالفة الثانية ترتّب بطلاناً يتعلّق بمصلحة الخصوم، لأنّها تشوب العمل بعدم الملاءمة فحسب مع قيام الحق في مباشرته، ثمّ إنّ هذا هو ما يوجب المعيار المعتمد في شأن تمييز قواعد النظام العام عن غيرها، فالقواعد الموضوعية للتفتيش إنّما تهدف إلى تحقيق مصلحة الجماعة في الوصول إلى الحقيقة بطريق عادل لا تحكم فيه و لا تعسف، طريق تحترم فيه كرامة الإنسان و الحرّيات الأساسية للفرد، التي لا

فالبسببة للقواعد الأولى، فإنّ المشرّع نفسه صريح في تشكيل الهيئات القضائية و ولايتها و اختصاصها متعلّق بالنظام العام، و لذلك فإنّ التفتيش الذي يخرج عن حدود القواعد المتعلقة بالإختصاص يكون باطلا بطلانا مطلقا، يضاف إلى قواعد الإختصاص الشّروط الموضوعية للتفتيش، و هي المتعلقة بركني "السبب" و "المحل"، إذ أنّ وظيفة هذه الشّروط هي تحديد حالات مشروعية التفتيش، و في غير هذه الحالات المشروعة يكون التفتيش مجرد عمل عدواني غير مشروع و هو ما يجعلها من النظام العام، لأنّ من قام به لم يكن يستعمل حقه القانوني بل تعدى حدود هذا الحق و أصبح معتديا، و قد يعاقب على ذلك لأنّه عمل "غير مشروع" و ليس عمل "غير صحيح" فحسب⁽¹⁾، كما هو الحال في التفتيش الذي لا يخالف الشّروط الشكلية التي تحدّد حالات التفتيش و إنّما تحدّد طريقة تنفيذه و من بين أمثلة عدم توفّر شروط المحل كون المحل غير قابل للتفتيش كالبيوت المسكونة أثناء الليل.

واقع الأمر أنّ هذا الرأى كسابقه لا يخلو من النقد، فأصحاب هذا الرأى اختلفوا في مسألة جوهرية تتعلّق أساسا بالتفريق بين "الشّروط الشكلية" و "الشّروط الموضوعية" للتفتيش، و قد سبق و أن أشرنا إلى أنّ الشّروط الموضوعية للإجراء هي التي يلزم توفّرها مسبقا لنشوء حق الهيئة الإجتماعية في اتخاذ العمل الإجرائي، و متى نشأ هذا الحق حدّد القانون الشّروط الشكلية التي تمثّل الإطار الذي يتحرّك داخله الحق⁽²⁾.

فمهمات تنفيذ التفتيش مثلا هو ظرف شكلي يتصل بزمان تنفيذ الإجراء و لا يعتبر شرطا موضوعيا، و هكذا اعتبره رأى من الفقه من القواعد الموضوعية التي يترتّب على مخالفتها بطلان الإجراء بطلانا مطلقا⁽³⁾، بينما إعتبره جانب آخر من الفقه من الشّروط

تقوم الدّولة المتمدينة و لا ينتظم سير الحياة فيها دونها، أمّا القواعد الشكلية فهي تهدف بالدّرجة الأولى إلى تمكين المتهم من مراقبة سلامة الدّليل و رعاية مصلحته في مباشرة الدّفاع عن نفسه غير أنّ هناك قاعدة شكلية ينبغي القول بأنّ مخالفتها ترتّب بطلانا من النظام العام تلك هي قاعدة تفتيش الأنثى بمعرفة أنثى و العلة في تخصيص هذه القاعدة من بين القواعد الشكلية بحكم خاص أنّ مخالفتها تعدّ في ذات الوقت مخالفة للآداب العامة التي يحرص المشرّع على صيانتها.

أنظر تفصيلا: سامي حسني الحسيني، المرجع السابق، ص 416 و ما بعدها.

(1) توفيق محمد الشاوي، المرجع السابق، ص 448.

(2) راجع ما سبق، بشأن معيار التفريق بين الضوابط الشكلية و الموضوعية للتفتيش الجنائي المعلوماتي.

(3) توفيق محمد الشاوي، المرجع السابق، ص 448.

الشكلية المتصلة بمصلحة المتهم التي يترتب على مخالفتها بطلان نسبي⁽¹⁾، و مثل هذا القول غير صحيح ، لأن إجراء تفتيش المنازل ليلا يشكل جريمة إنتهاك حرمة المسكن، و من ثم فالبطلان المنجر جزاء هذه المخالفة يتعلّق بالنظام العام لأنّ هذه المخالفة معاقب عليه قانونا. و إذا سايرنا مذهب الفقه - الذي أصاب في نظرنا في التفريق بين الشّروط الشّكلية و الموضوعية للإجراء- فإنّ النّطاق الزّمني لتنفيذ إذن التفتيش هو من الشّروط الشّكلية لتعلقه بظرف زمني للتّفيذ، ينجر عن مخالفته وفقا لهذا الرّأي بطلان نسبي، و هو أمر غير صحيح في جميع السياقات، ففي الأحوال التي يتم فيها تنفيذ التفتيش بعد انقضاء مدة سريان الإذن به، يكون حينها العمل الاجرائي قد تمّ بدون إذن قضائي لأنّ الإذن الأول يكون قد فقد معناه و بات في حكم العدم، و لا شك أنّ انتهاك ضمان الإشراف القضائي على الإجراءات الماسة بالحرية الشخصية مما يتعلّق بالنظام العام، و تلك مسألة محل إجماع بين الفقهاء⁽²⁾.

ثالثا: موقف القضاء من طبيعة بطلان التفتيش عن الأدلة المعلوماتية

أبانت المحكمة العليا الجزائرية عن موقفها إزاء طبيعة بطلان التفتيش فيما إذا كان متعلقا بالنظام العام أو بمصلحة الخصوم بشكل صريح و لذلك بموجب قرارها الصادر بتاريخ 27 جانفي 1987 رقم 22174، حين قضت بأنّ الدفع ببطلان التفتيش هو من المسائل الموضوعية التي يجب عرضها على قضاء الموضوع، و إلا سقط الحق في إثارتها لأول مرّة أمام المحكمة العليا⁽³⁾.

أمّا بالنسبة لمحكمة النقض المصرية، فقد اعتقدت في البداية نظرية موحدة كانت في مبدأ الأمر نظرية البطلان المطلق دون النسبي، و تُرتب على هذا البطلان جميع آثاره الطبيعية و كان ذلك على وجه خاص بالنسبة لدعم قاعدة موضوعية من قواعد التفتيش و هي إيجاب

(1) سامي حسني الحسيني، المرجع السابق، ص 415.

(2) و مما يؤسف له أنّ محكمة النقض الفرنسية في أحدث قراراتها قرّرت رفض طلب بطلان التفتيش الذي تأخر تنفيذه لمدة 6 أشهر كاملة على تاريخ صدور الإذن به و جاء في قرارها أنّه إذا لم يحدّد إذن التفتيش أجلا لتنفيذ الإذن الذي أصدره قاضي الحريات و الحبس فإنّ هذا الإذن يعتبر قائما و يكون التفتيش الذي حصل بمقتضاه صحيحا و لو مرّت ستة أشهر على صدوره عند تنفيذه طالما لم يسبق إتخاذ إجراءات بهذا الخصوص لأنّه لا يوجد أيّ نطاق زمني مقرّر لمباشرة تنفيذ التفتيش.

Cass Crim, 16 mai 2018, n° 17-84909. Bull. Crim 2018 ,n° 05.

(3) مشار إليه لدى: أحمد الشافعي، المرجع السابق، ص 104.

الرجوع الى سلطة التحقيق للحصول على إذن منها به عندما تنفي الأحوال التي تجيز لمأمور الضبط القضائي إجراءه بغير إذن، فكّما إنتفى هذا الإذن من سلطة التحقيق أو بطل لوجود عيب فيه أعدم آثاره، كّما كان التفتيش باطلا بطلانا مطلقا (1).

و بعدها ظهر تردّد لدى هذا القضاء بالتّحول و لو بشكل غير صريح إلى إعتبار بطلان التفتيش بطلانا نسبيا، فقضت بأنّ حصول التفتيش بغير حضور المتهم لا يترتب عليه قانونا بطلانه، فالقانون لم يجعله شرط جوهريا لصحة التفتيش، و إنّه إذا كان يجب على من يقوم بإجراء التفتيش أن يحرر محضرا يبيّن فيه المكان أو الشخص الذي حصل تفتيشه و اليوم و السّاعة اللّذين حصل فيهما التفتيش، إلّا أنّ ذلك إنّما وضع لحسن سير الأعمال و تنظيم الإجراءات و لا يترتب على مخالفته بطلان، و أن القانون حين أوجب المبادرة إلى وضع المضبوطات في أحرار مغلفة إنّما قصد تنظيم العمل و المحافظة على الدّليل لعدم توهين قوّته في الإثبات، لكنّه لم يترتب على مجرد الإهمال في ذلك أي بطلان (2).

و بخصوص محكمة النقض الفرنسية فإنّ موقفها لم يختلف كثيرا عن موقف محكمة النقض المصرية، فقد قرّرت أنّ بطلان التفتيش يتعلّق بالنّظام العام كّما تعلّق الأمر بالإعتداء على حقوق الدّفاع، كأن ينجر عنه ضبط رسائل متبادلة بين المتهم و محاميه (3)، أو عدم مراعاة قواعد الإختصاص (4).

و ظاهر من خلال أحكام محكمة النقض المصرية و الفرنسية أنّه يصعب مقدما تحديد حالات بطلان التفتيش المتعلّقة بالنّظام العام و تلك المتعلّقة بمصلحة الخصوم، و إن كان يمكن القول بأنّ مخالفة قواعد الإختصاص ترتّب بطلانا من النّظام العام، إذ ليست هناك مغايرة في موقف القضاء بشأنها، بل إنّ محكمة النقض مستقرّة على اعتبار قواعد الإختصاص عموما من النّظام العام فهي تتّصل بحسن إدارة العدالة، و كذلك حقوق الدّفاع

(1) و من هذا القضاء نسوق المثال "أن بطلان محضر التفتيش الحاصل بغير إذن من السلطة المختصة مما يمس بالنظام العام، فالتمسك به جائز في أي مرحلة كانت عليها الدعوى أما محضر التفتيش الذي يقوم به وكيل النيابة بدون أن يستصحب معه كابتا فبطلانه نسبي و لا يمس النظام العام في شيء، و لذلك يسقط حق التمسك به ما لم يطعن عليه أمام محكمة الدرجة الأولى" (نقض 1933/12/27 رقم 178)، مشار إليه لدى: رؤوف عبيد، المرجع السابق، ص 27.

(2) سامي حسني الحسيني، المرجع السابق، ص 421.

(3) Cass Crim, 12 mars 1992, n° 91-86.843, Bull. Crim 1992, n° 112.

(4) Cass Crim, 18 mai 1983, n°1983, 82-93.410, Bull. Crim, n° 148.

تتعلّق بالنظام العام، و يصح التمسك بالبطلان النَّاجم عن الإعتداء عليها و لو لأول مرّة في النَّقض⁽¹⁾.

صفوة القول أنّ سبب عدم تمكن الفقه و القضاء من إرساء ضوابط التّمييز بين حالات البطلان المطلق و البطلان النسبي للتفتيش، هو عدم وجود معيار ثابت للتفرقة بين القواعد المتصلة بالنظام العام و تلك المتصلة بمصلحة الأطراف، على أنّه ينبغي أن تشير إلى أنّ كافة الشّروط الموضوعية للتفتيش ينجزّ عن مخالفتها البطلان المطلق لانها تشكل عدونا صارخا على الحريات الشخصية كان يتم التفتيش من طرف سلطة غير مختصة، او بدون سبب، أو من غير تحديد محل التفتيش و تلك مسائل لا خلاف بشأنها بين الفقه.

في مقابل ذلك فإننا نعتقد أنّ الشّروط الشكلية التي ينجزّ عن مخالفتها قيام جريمة فهي مخالفة متعلّقة بالنظام العام، و مثال ذلك كتفتيش المساكن ليلا أو تفتيش أنثى بغير الإستعانة بأنثى، كما تعتبر جميع الضمانات الشكلية التي أصبغ عليها المشرّع الطابع الدستوري متعلّقة بالنظام العام حتّى و لو تعلّقت بمصلحة الأفراد لأنّ هذه الضمانات الدستورية تترعّ على قمة النظام العام، و أما ما عدا هذه الأحوال فهي قواعد يترتب على مخالفتها بطلان نسبي.

الفرع الثالث: أحكم الدفع ببطلان التفتيش عن الأدلة المعلوماتية

التفتيش كما قدّمنا من إجراءات إسترداد الأدلة المعلوماتية المخزّنة، لذلك فإنّ الدفع ببطلان هذا الإجراء هو من الدفع الموضوعية (أولا)، و إن كان المظهر السلبي لحق الحرمة يمنح لصاحبه السماح للغير بالإطلاع عليها، فإنّ هذه الموافقة تفقده الحق في الدفع بالبطلان (ثانيا)، كما أنّه ليس لغير من وقع التفتيش على أنظّمته المعلوماتية أن يطعن بالبطلان (ثالثا).

أولا: الدفع ببطلان التفتيش من الدفع الموضوعية

القاعدة العامة في الدفع الموضوعية أنّه يجوز التمسك بها في جميع مراحل الدعوى، سواء أمام جهة التحقيق أو الإحالة أو المحاكمة الابتدائية أو الأستئنافية، أمّا أمام محكمة النَّقض فلا يقبل من الخصم أن يتمسك بدفع موضوعي إلاّ إذا كان قد دفع به أمام محكمة الموضوع، و في هذه الحالة قد ترد المحكمة على هذا الدفع ردا صحيحا مقنعا فلا محل

(1) سامي حسني الحسيني، المرجع السابق، ص 432.

لإثارته أمام المحكمة العليا، أمّا إذا ردت ردا خاطئاً أو أغفلت الردّ عليه، فإنّ لصاحب الشّأن أن يطعن في الحكم على أساس الخطأ في تطبيق القانون أو الإخلال بحق الدفاع و كلها دفوع قانونية (1).

و كما سبق بيانه، فإن المحكمة العليا الجزائرية قد إعتبرت أن الدفع ببطلان التفتيش من الدفوع الموضوعية، و لذلك تسري القاعدة التي أشرنا إليها، بل إنّ هذه القاعدة تسري حتّى في الأحوال التي يعتبر فيها بطلان التفتيش متعلّق بالنظام العام. و مفاد ذلك أنّه يجوز الإحتجاج بالبطلان في أي مرحلة كانت عليها الدعوى العمومية، و مع ذلك لا يجوز الإحتجاج به لأوّل مرّة أمام المحكمة العليا عند سلوك طريق الطعن بالنقض، ذلك أنّ هذا الدفع من الدفوع التي يختلط فيها القانون بالواقع، و تقتضي تحقيقاً موضوعياً لا تختص به محكمة النقض (2).

بيد أنّنا نجد أنّ بعض أحكام محكمة النقض المصرية قد ذكرت أن الدفع ببطلان التفتيش هو دفع متعلق بالقانون - و ليس بالواقع - لتعلّقه بصحة الأخذ بالدليل هو النتيجة التي أسفر عنها التفتيش، فيجوز التمسك به لأوّل مرّة أمام محكمة النقض، إلّا أنّ هذا الدفع ببطلان التفتيش في هذه الحالة معلق على شرط أن يكون سبب البطلان يستند إلى وقائع ثابتة في نفس الحكم أو القرار المطعون فيه بالنقض، أو إذا جاء في الحكم من وقائع دالة بذاته على وقوعه، و لا يحتاج الحكم فيه إلى تحقيق موضوعي (3).

و نجد أيضاً في القضاء المقارن تطبيقاً متواتراً لهذه القاعدة ، ففي احد قرارات الدائرة الاستئنافية قرر القضاء الأمريكي لأنّه إذا كان صحيحاً أن التعديل الدستوري الرابع يحمي الأشخاص و الممتلكات من التفتيش غير المشروع، فإنّه صحيح كذلك أن من يطالب بالحماية التي يقرها هذا الدستور أن يثير الدفع بالبطلان في حينه، و إلّا عدّ متنازلاً عن التمسك به (4).

(1) توفيق محمد الشاوي، المرجع السابق، ص 458.

(2) محمود نجيب حسني، المرجع السابق، ص 544.

(3) نقض 28 ديسمبر 1937 رقم 141 مشار إليه لدى: توفيق محمد الشاوي، المرجع نفسه، ص 458.

(4) Mason W. White, Appellant, v. United States of America, Appellee, 235 F.2d 221 (D.C. Cir. 1956).

ثانياً: لا محل للبطلان في حالة الرضا

تبيّن لنا عند دراستنا لخصائص التفتيش، أن هذا الإجراء يمثل إطلاع على محل يمتع بالحرمة، و أنّ رضا صاحب الشأن بهذا الإجراء يجعل عمل الإطلاع صحيحاً لا لبس فيه، و يصبح حينئذ العمل الإجرائي مجرد معايينة لا يخضع للضمانات المقررة للتفتيش، فالقواعد الموضوعية للتفتيش هي مما يتعلق بالنظام العام و لا يصحّ التنازل عن مراعاتها، و لا يجوز القول بأنّ الرضا يصحح التفتيش الباطل، إذ لا تفتيش أصلاً حتى يمكن الحديث عن صحته أو بطلانه⁽¹⁾.

و هذا الأمر ينطبق أيضاً على جميع البيانات التي تنازل فيها صاحب الشأن عن حقه في الحرمة بجعلها متاحة للجميع، و إذ هو تنازل مسبقاً عن هذا الإمتياز القانوني، الذي قرره التشريع لصالحه، فليس له بعد ذلك أن يدفع بعدم صحة التفتيش.

لكنّ هذا الوضع على بساطته قد يثير بعض الإشكاليات في الواقع العملي، فقد يعترف المتهم فعلاً بالجريمة التي يراد أن يجرى التفتيش بسببها، قبل ان يدصر القضايا اذنا بالتفتيش و ذلك تقادياً منه للتفتيش حتى يحفظ لنفسه الحق في خصوصية نظامه المعلوماتي و يمنع لسلطة التحقيق او من تندبه من الاطلاع على اسراره التي يخزنها بنظام المعلوماتي، فيدركاً بواسطة هذا الاعتراف المسبق الإعتداء على أسرار يراها أولى بالحماية.

راجع هذا التطبيق القضائي و غيره مشار إليها لدى: سامي حسن الحسيني، المرجع السابق، ص 446.

(1) من التطبيقات القضائية لهذه القاعدة ما قرره محكمة النقض المصرية في عدد كبير من قراراتها من أنّ تفتيش المنازل أو الأشخاص هو بحسب الأصل إجراء من إجراءات التحقيق لا تأمر به إلا سلطة من سلطاته لمناسبة جريمة ترى أنها وقعت و صحت نسبتها إلى شخص معين و أن هناك من الدلائل ما يكفي للتعرض لحرية المتهم الشخصية أو لحرمة مسكنه -ذلك هو حكم التفتيش الذي نظم القانون قواعده و ضبط حالاته و جعل لرجال الضبط القضائي و لمن خولهم سلطة التحقيق حق مباشرته في حدود القانون، و التفتيش بهذا المعنى القانوني هو بطبيعة الحال غير التفتيش الذي يجريه الأفراد على من تلحقه شبهة الإتهام بحياسة شيء حيابة إجرامية غير مشروعة، فهو ليس تفتيشاً ينتزل منزلة التفتيش الذي خاطب الشارع المحقق بأحكامه و إنما هو نوع من البحث و الإستقصاء أو هو نوع من التقيب عن الأشياء الخاصة بجريمة تحقق وقوعها، و إذا رضى به المتهم كان دليلاً يصح إستناد قضاء الإتهام و قضاء الحكم إليه على السواء ، فإذا ثبت لمحكمة الموضوع سلامة هذا الإجراء جاز لها أن تأخذ بنتيجة هذا التقيب كدليل من أدلة الإثبات في الدعوى". الطعن رقم 1484 لسنة 29 قضائية الصادر بجلسة 1960/01/18، مشار اليه لدى: سامي حسن الحسيني، المرجع نفسه، ص 451.

فهل يجوز في هذه الحالة بناء على إقرار المتهم إجراء التفتيش عن الأدلة المعلوماتية بدون الإلتزام بالضمانات المقررة قانوناً؟

عُرِضَتْ هذه الحالة على القضاء المصري في إطار التفتيش التقليدي، و إنتهى فيها إلى أنّ صدور الإقرار من المتهم بإرتكابه للجريمة يعتبر بمثابة إذن منه بالتفتيش⁽¹⁾، و بطبيعة الحال فإننا لا نوافق على هذا القضاء نهائياً، فطالما أنّ المتهم قد استسلم للقضاء و أيقن بالعقوبة، فقد تحقّق الهدف من التحقيق الذي يسعى لإظهار الحقيقة بأقلّ التدابير القسرية التي يمكن أن تحقّق نفس الهدف، على نحو لم يعد من سائغ لإتخاذ إجراءات أخرى أكثر إنتهاكاً للحريات الفردية، لغياب ما يبررها.

و من ثم فإننا نرى أنّ إقرار المتهم بالجريمة لا يعتبر بمثابة رضا منه بالتفتيش، و كل تفتيش لا يراعي الضمانات الإجرائية المقررة قانوناً يقع باطلاً و عديم الأثر، بل إننا نذهب أبعد من ذلك، فحتّى في الأحوال التي يكون فيها التفتيش قد استكمل شروطه الموضوعية، و نشأ للسلطة الحق في التفتيش عن الأدلة المعلوماتية فإنّ إقرار المتهم بالجريمة يعتبر مانعاً من إجراء التفتيش، و حال تنفيذه رغم الإقرار المسبق للمتهم يعتبر سلوكاً غير مشروع، لا يؤدي فقط إلى بطلان الأدلة المعلوماتية المكتشفة بشكل عرضي، بل لقيام مسؤولية القائم بالتفتيش أيضاً طبقاً للمادة 4 فقرة ج من القانون 09-04.

و قد جاء قانون الإجراءات الجزائية الفرنسي فنص صراحة على جواز مباشرة تفتيش الأنظمة المعلوماتية بمعرفة الضبط القضائي بناء على رضا صريح من صاحب الشأن، و بموجب الفقرة الأولى من المادة 76 من قانون الإجراءات الجزائية التي تحيل بدورها على المادة 56 من نفس القانون التي تنظم التفتيش في صورته المادي و المعلوماتي، مع وجوب إثبات هذا الرضا كتابة بخط يد صاحب الشأن، فإن تعذرت عليه الكتابة يشار إلى ذلك في المحضر.

(1) نقض 9 ديسمبر 1947 قضية رقم 2025 لسنة 1946 السنة القضائية 17 ورد بالحكم "إن المتهم اعترف بالسرقة و بإقتسام المسروقات مع بقية المتهمين فكان من واجب المحقق أن يستمر في إجراءاته و أن يبادر إلى إتخاذ ما فيه تأييد لهذا الإقرار ففتش منزله باحثاً عن جسم الجريمة المعترف بها، و لإفماداً يكون الحال لو أن المسروق كان شيئاً ثميناً غير كمية زهيدة من التبغ و أقر المتهم بالسرقة فأرجأ البوليس امر التفتيش الى حين الحصول على إذن من النيابة فإستطاع المتهم بوسائله في تلك الأثناء نقل الشيء الثمين المسروق إلى مكان آخر فأخفاه ... إن الإقرار بمثابة إذن بالتفتيش". مشار إليه لدى: توفيق محمد الشاوي، المرجع السابق، ص 464.

أما بالنسبة للقضاء الأمريكي فقد أستقر في نظامه منذ أمد طويل على جواز الرضا بالتفتيش، فقضت المحكمة العليا الفيدرالية بأن الموافقة على التفتيش تفقد المتهم حقوقه المنصوص عليها بالتعديل الدستوري الرابع⁽¹⁾، بحيث يجوز للضبطية القضائية القيام بتفتيش أي مكان أو شيء بدون إذن قضائي، بل حتى دون قيام السبب المعقول متى أبدى الشخص الذي له سلطة على محل التفتيش موافقة طوعية على هذا الإجراء⁽²⁾.

غالباً ما يفرض التفتيش عن الأدلة المعلوماتية تساؤلاً حول ما إذا كانت الموافقة على تفتيش مسكن معين أو سيارة ما يحوزها المتهم تشمل بشكل ضمني الموافقة على تفتيش الأنظمة الحاسوبية الموجودة بهذه الأماكن؟

إن القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها قد رفض الجواب عن هذا التساؤل، إلا أن المتأمل لنص المادتين 46 و 47 من الدستور يجد أن المشرع قد قرّر حماية للنظم المعلوماتية بمقتضى نص مستقل عن الحماية المقررة للمسكن رغم وحدة الضمان الاجرائي المقرر لهما يقضى هاتين المادتين و هو الاذن القضائي المسبق لمباشرة تفتيشها، و في ذلك - كما سبق و أن أشرنا- دلالة على أن إذن تفتيش المسكن لا يجيز للسلطة الإجرائية تفتيش النظم المعلوماتية ما لم تحصل على إذن خاص بالتفتيش المعلوماتي زيادة على إذن بتفتيش المسكن، و لأن الرضا بالتفتيش إنما هو بمثابة تنازل طوعي عن اقتضاء الإذن القضائي المسبق لمباشرة التفتيش، فإننا نجزم بكون الرضا بتفتيش المسكن لا يبيح تفتيش الأنظمة المعلوماتية المتواجدة به، بل يشترط قيام الرضا بتفتيش الأنظمة المعلوماتية علاوة عن تحقق الرضا بتفتيش المسكن، فيستلزم لصحة الإجراء قيام الرضا كلما تطلب القانون الإذن القضائي.

أما بخصوص المشرع الفرنسي فقد أجاب ضمن نص المادة 76 من قانون الإجراءات الجزائية على هذا التساؤل بشكل صريح، حيث يستفاد منه أن الموافقة على التفتيش المادي ممثلاً في تفتيش المساكن يحتاج إلى موافقة صريحة و مكتوبة، ثم أشار إلى وجوب مراعاة هذه الضمانة الإجرائية حال تفتيش الأنظمة المعلوماتية، و مؤدى ذلك أن الموافقة على

(¹) Bolger v. United States, 189 F. Supp. 237 (S.D.N.Y. 1960) "Consent to a search may constitute a waiver of the rights secured by the Fourth Amendment".

(²) H. Marshall Jarrett, et al, op cit, p 15.

التفتيش المادي لا يمكن أن تفسر على أنه رضا بالتفتيش المعلوماتي، بل تتوقف مشروعية هذا العمل الإجرائي على موافقة مستقلة بهذا الخصوص تحت طائلة البطلان⁽¹⁾.

و في عدة أحكام حديثة متعاقبة واصل القضاء الأمريكي إتجاهه نحو تقوية الضمانات المقررة في التعديل الدستوري الرابع، بخصوص نطاق الرضا بتفتيش الأنظمة المعلوماتية الذي وجب أن يفسر بشكل دقيق وفقا للظروف، فإن تجاوز التفتيش نطاق الرضا وقع باطلا⁽²⁾، و هو نفس الجزاء الإجرائي الذي يرتبه القضاء في الأحوال التي يكون فيها رضا الشخص بالتفتيش يستند إلى سبب معين في حين يكون مستهدف التفتيش راجع إلى سبب آخر.

حيث قرر القضاء الأمريكي في العديد من أحكامه بطلان إجراءات التفتيش عن الأدلة المعلوماتية و استردادها، و المتمثلة في الصور الرقمية الخاصة بدعارة الأطفال القصر بعد الحصول على موافقة على تفتيش الحواسيب بحثا عن أدلة مغايرة لتلك التي حصلت لأجلها الموافقة على التفتيش، فاستقر هذا القضاء على أن تحويل التفتيش عن الأدلة المادية إلى التفتيش عن الأدلة المعلوماتية يجاوز نطاق إرادة الخاضع للتفتيش بما يبطل الدليل المتحصّل عليه⁽³⁾.

(1) Article 76 du Code de procédure pénale français Modifié par Loi n°2004-204 du 9 mars 2004 - art. 79 JORF 10 mars 2004 en vigueur le 1er octobre 2004 dispose que : **Les perquisitions, visites domiciliaires et saisies de pièces à conviction ne peuvent être effectuées sans l'assentiment exprès de la personne chez laquelle l'opération a lieu. Cet assentiment doit faire l'objet d'une déclaration écrite de la main de l'intéressé ou, si celui-ci ne sait écrire, il en est fait mention au procès verbal ainsi que de son assentiment.**

Les dispositions prévues par les articles 56 et 59 (premier alinéa) sont applicables."

(2) حيث قرّرت الدائرة الإستئنافية العاشرة في قضية *United States v. Carey* "أنه يجب قراءة نموذج موافقة خطية بشكل ضيق للغاية، بحيث ان الموافقة على ضبط "أي ممتلكات" تحت سيطرة المدعى عليه لأجل "الفحص الكامل للعقار و الممتلكات" ضمن عنوان المتهم ، لا تسمح للضبطية القضائية سوى ضبط الحاسوب داخل شقة المتهم، دون أن يمتد نطاق الموافقة إلى تفتيش الحاسوب خارج هذا المكان لأنه بذلك لم يعد موجودا بهذا العنوان".

United States v. Carey, 172 F.3d 1268, 1274 (10th Cir. 1999), Citing *H. Marshall Jarrett, et al*, op cit, p 16.

(3) من التطبيقات القضائية لهذه القاعدة ما تقرّر في قضية *United States v. Turner* حيث أوردت الدائرة الاستئنافية الأولى أنّ القائمين بالتفتيش كانوا يستهدفون البحث عن دليل مادي *physical evidence* بشأن محاولة الإعتداء الجنسي، و حصلوا على موافقة مكتوبة من جار الضحية لأجل تفتيش مسكنه، و قبل قيام هذا الأخير بالتوقيع على الموافقة اكتشفوا سكينا من النوع الكبير و بقع دماء في شقته و شرحوا له أسباب التفتيش بأنهم يبحثون عن المزيد من الأدلة عن هذا الاعتداء الجنسي التي يمكن أن يكون المتهم قد تركها وراءه، و بينما هم يقومون

لذا فإننا نعتقد أنه يلزم لمشروعية الدليل المعلوماتي المستمد من هذا الإطلاع أن يكون الرضا الصادر عن صاحب الشأن صريحا بأن يحدّد على وجه الدقة نطاق هذا الإطلاع (محل المعاينة) و الغاية منه (مستند المعاينة)، فإن قام المحقق أو من يندبه بتجاوز نطاق هذه الإرادة من حيث المحلّ الذي جرى الإطلاع عليه و معاينته أو من حيث ما يسعى إليه المحقق من أدلة و لو كان من نفس النوع (دليلا معلوماتيا) وقع الإجراء باطلا و بالتبعية يبطل معه الدليل المعلوماتي المستمد منه، و يقع على المحكمة في هذه الأحوال استبعاده و عدم بناء حكم الإدانة بناء عليه، لأنّ الشخص لم يتنازل عن الضمانات الجوهرية المقرّرة لمصلحته إلاّ في نطاق ضيق يحدده الرضا، و ما زاد عن حدود الرضا يبقى خاصعا لهذه الضمانات و يصبح حينئذ الإطلاع تفتيشا و ليس معاينة.

ثالثا: بطلان التفتيش لا يتمسك به إلاّ صاحب الشأن

القاعدة العامة هي أنّه "حيث لا مصلحة لا دعوى"، و هذه القاعدة من الأصول العامة التي لا تحتاج في تقريرها إلى نص، فهي لازمة عقلا في كل الأحوال و لا يماري فيها أحد، فالإلتجاء إلى التمسك بالبطلان دون فائدة ترجى من وراء ذلك يعتبر عبثا، إذ أنّ الخصومة الجنائية ليست نشاطا نظريا أو مسرحا للمناظرات و تبادل الآراء و وجهات النظر، بل هي نشاط يهدف إلى تحقيق أغراض عملية، و بالتالي فإنّ كل عمل إجرائي يجب أن تحذوه مصلحة خاصة أي تترتب عليه فائدة عملية⁽¹⁾، بغض النظر عن جسامة العدوان الواقع على الحياة الخاصة⁽²⁾.

بالنّسبة للمادي بادر أحد أعضاء الضبط القضائي بتفتيش الحاسوب الشخصي الخاص بهذا الأخير و إكتشف أنّه يحتوي على صور داعرة للأطفال القصر، أين قرّرت هذه الجهة القضائية أنّ التفتيش يتجاوز نطاق الإرادة بالموافقة و يبطل معه الدليل المعلوماتي المستمد منه.

United States v. Turner, 169 F.3d 84 (1st Cir. 1999), Citing H. Marshall Jarrett, et al, op cit, p 18.

(1) سامي حسن الحسيني، المرجع السابق، ص 435.

(2) في قضاء مستقر لها قضت محكمة النقض المصرية "من المقرّر أنّه لا صفة لغير من وقع في شأنه القبض والتفتيش أن يدفع ببطلانه و لو كان يستفيد منه، لأنّ تحقق المصلحة لاحق لوجود الصفة فيه، كما أنّه من المستقر عليه في قضاء هذه المحكمة أنّه لا يجوز الطعن بالبطلان في الدليل المستمد من القبض أو التفتيش لسبب عدم مراعاة الأوضاع القانونية المقررة لذلك إلاّ ممن شرعت هذه الأوضاع لحمايتهم، وكان الإذن بالتفتيش خاصاً بالمحكوم عليه الآخر فإنّه لا يقبل من الطاعن الدفع ببطلان الإذن الصادر بالتفتيش لأنّه لا صفة له في التحدث

فلا يُقبل الدفع ببطلان التفتيش إلا ممن شرع البطلان لمصلحته، فلا يُقبل من غيره و لو كان يستفيد من تقرير البطلان، إذ أنّ إستفادته من ذلك إنّما تكون على سبيل التبعية، و تطبيقا لذلك فإنّه لا يقبل الإحتجاج ببطلان تفتيش شخص إلا من الشخص الذي جرى تفتيشه، و لا يُقبل الدفع ببطلان تفتيش مسكن إلا من حائز المسكن الذي فُتِش، و بناء على هذه القاعدة كان الدفع ببطلان التفتيش هو في حقيقته تمسك بالحق في حصانة البدن و حرمة المسكن و النّظام المعلوماتي، و لا يقبل ذلك إلا من صاحب هذا الحق⁽¹⁾.

غير أنّ جانب من الفقه يرى أنّه قلّمَا يحتاج الأمر في العمل إلى الكلام عن إنتفاء هذا الشرط من شروط المصلحة لأنّه مفهوم ضمنا، و لأنّه إذا كان التفتيش الباطل لم يسفر عن أي دليل فقد إنتفت بالتالي حاجة المتهم إلى الكلام في مبدأ البطلان، بل تكون مصلحته بالأكثر في التّعاضي عنه، لأنّ إنتفاء الدليل الذي كان يصح أن يفسر الإجراء الباطل عنه قد يكون في بعض الأحيان من قرائن البراءة التي يستفيد منها المتهم⁽²⁾.

و لا يكفي للدفع ببطلان الدليل المعلوماتي المستمد من التفتيش أن يكون هذا الإجراء قد أسفر عن ظهور دليل قبل من يتمسك بالبطلان، بل يجب أن تكون محكمة الموضوع قد عوّلت على الدليل الباطل في إدانته أو تأثرت به في تكوين عقيدتها، أمّا إذا كان التفتيش لم يسفر عن دليل ما أو أسفر عنه و لكن المحكمة أطرحته و إستندت إلى أدلة أخرى لا تتصل بالتفتيش الباطل، فلا تبدو ثمة مصلحة في الدفع ببطلان التفتيش، و إلا لأصبح البطلان نظريا لا فائدة عملية في التمسك به⁽³⁾، و على ذلك فلا مصلحة للمتهم في الدفع ببطلان التفتيش في مرحلتيه - مرحلة التفتيش المادي و مرحلة التفتيش المعلوماتي - طالما أنّ المحكمة قد إستدتت في إدانته إلى إقراره المستقل عن هذا التفتيش أو أيّ دليل آخر.

و يضيف بعض الفقه أنّه لا يقتصر إقتضاء شرط المصلحة على الدفع ببطلان التفتيش المتعلق بمصلحة الخصوم، بل هو متطلب كذلك و لو كان البطلان ممّا يتعلّق بالنّظام

عن ذلك" (الطعن رقم 204 لسنة 17 قضائية، الصادر بجلسة 1966/11/14)، هذه التطبيقات القضائية و أخرى مشار إليها لدى: ايهاب عبد المطلب، المرجع السابق، ص 125.

(1) محمود نجيب حسني، المرجع السابق، ص 532.

(2) رؤوف عبيد، المشكلات العملية الهامة في الإجراءات الجنائية، الطبعة الثالثة، دار الفكر العربي، مصر، 1980، ص 41.

(3) سامي حسني الحسيني، المرجع السابق، ص 435.

العام⁽¹⁾، هذا في الحالة التي لا تستند فيها المحكمة على الدليل المستمد من التفتيش الباطل، أما إذا كان لهذا الدليل أثر في تكوين عقيدتها، فإنه يقع واجبا عليها القضاء بطلانه، لأنه متى تعلّق البطلان بالنظام العام، فإنه لا يُتصوّر إنكار قيام مصلحة المتهم في التمسك به على الوجه السابق بيانه.

يلاحظ أنّ الدفع ببطلان التفتيش هو دفاع عيني لتعلّقه بمشروعية الدليل المستمدّ منه وجودا و عدما لا بأشخاص مرتكبي الجريمة، و يترتّب عليه إستفادة باقي الطاعنين الذين لم يبدوا هذا الدفع بطريق اللّزوم و التّبعية، و ذلك بالنظر إلى وحدة الواقعة و الأثر العينيّ للدفع و كذلك قوّة الأثر القانوني للإرتباط بين المتهمين⁽²⁾، و بالتالي فإنّ القرار بإخراج هذه المحاضر التي نالها البطلان من ملف الدعوى غير قابل للتجزئة بحيث يسري على جميع المتهمين⁽³⁾.

المطلب الثاني: أثر بطلان التفتيش في إستبعاد الأدلة المعلوماتية

متى قرّرت المحكمة بطلان التفتيش عن الدليل المعلوماتي، فهل يجوز لها على الرّغم من تقرير هذا البطلان أن تعتمد في قضائها بالإدانة على آثار هذا التفتيش الباطل؟ (الفرع الأول)، و إذا كان هذا العمل الإجرائي ليس في كافة الحالات مستقلا عن غيره من الإجراءات فهل واقعة تقرير بطلانه تظل قائمة بذاتها، أم لها انعكاسات بحكم الضرورة على غيره من الإجراءات السابقة عليه (الفرع الثاني)، و اللاحقه له (الفرع الثالث).

الفرع الأول: أثر بطلان التفتيش على الأدلة المعلوماتية المستمدة منه

يثور التساؤل هنا حول مدى أحقية المحكمة في الإعتماد على أثر التفتيش المعلوماتي الباطل على الرّغم من تسليم هذه الأخيرة ببطلانه؟ الحقيقة أنّه إذا تقرّر بطلان إجراء معيّن، و جب إستبعاد الدليل المستمدّ منه و إلّا أضحت الضّمّانات التي يقرّها القانون للحفاظ على الحريات الفردية عديمة الجدوى، و الأصل أنّ البطلان لا يرتب آثاره إلّا متى تقرّر بحكم أو بأمر من قاضي التحقيق، و هذه

(1) سامي حسني الحسيني، المرجع السابق، ص 436.

(2) ياسر الامير فاروق، المرجع السابق، ص 621.

(3) Cass Crim, 28 juin 2000, n° 00-80.292, Bull. Crim, 2000, n° 252.

القاعدة مطلقة و لا إستثناء عليها و لو تعلّق البطلان بالنّظام العام، و مصدر هذه القاعدة هو النّظام القانوني الذي تعيش فيه الجماعة في العصر الحديث، حيث لا ينال الفرد حقّه بغير وساطة القضاء⁽¹⁾.

و إسنادا إلى هذه القاعدة فإنّ التّفّيش الباطل يستلزم حتما بطلان الأدلة المعلوماتية المستمّدة منه أيّا كان نوعها أو محلها، فالمتفق عليه أنّ بطلان التّفّيش لمخالفته شرطا من شروطه الموضوعية أو الشّكلية يترتّب عليه بطلان جميع نتائجه "المباشرة"، أي بطلان محضر التّفّيش و الضبط و شهادة الأشخاص الذين أجروا التّفّيش، أو بعبارة أدقّ سقوط هذه الأدلة لأنّها لا تخرج عن كونها أدلة مستمّدة من إجراء باطل⁽²⁾، و لا يتصور ترتيب نتائج قانونية لإجراء غير قانوني.

و على ذلك، فإنّه متى ثبت بطلان التّفّيش تعيّن على القضاء إطراح الدّليل المستمّد منه أو المترتب عليه "مباشرة"، و بالتّالي القول ببراءة المتهم ما لم تكن ثمة أدلة أخرى في ظروف الدعوى تكفي لثبوت التهمة و إدانته⁽³⁾، وهذه القاعدة سبق للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات أن أوصى بها بموجب توصيته رقم (18) و التي جاء فيها "إنّ كلّ الأدلة التي تمّ الحصول عليها عن طريق إنتهاك حق أساسي للمتهم و الأدلة المستمّدة منها تكون باطلة و لا يمكن مراعاتها في أي لحظة خلال الإجراءات"⁽⁴⁾.

و تقضي المادة 336 من قانون الإجراءات الجنائية المصري بأنّه "إذا تقرّر بطلان أي إجراء فإنّه يتناول جميع آثاره التي ترتبت عليه مباشرة و يلزم إعادته متى أمكن ذلك"، و هذه المادة تقرّر إبطال الدّليل المستمّد من الإجراء الباطل و توضح صراحة أنّ البطلان يمتد إلى جميع الآثار التي ترتبت عليه مباشرة لأنّ ما بني على باطل هو باطل بلا شك⁽⁵⁾، و الحقيقة أنّه ليس في القانون حاجة إلى مثل هذا النص لأنّه مفترض منطقي.

(1) توفيق محمد الشاوي، المرجع السابق، ص ص 490 - 491.

(2) احمد فتحي سرور، الوسيط في قانون الاجراءات الجنائية، المرجع السابق، ص 516.

(3) سامي حسني الحسيني، المرجع السابق، ص 465.

(4) XVe Congrès international de droit pénal (Rio de Janeiro, Brésil, du 4 au 10 septembre 1994), op cit , p 38.

(5) و قد إستثنى القانون المصري من القاعدة المتقدمة حالة القضاء بعدم الإختصاص بعد أن سار التحقيق شوطا أمام جهة غير مختصة فقد نصت المادة 163 من قانون الإجراءات الجنائية على أنّه لا يترتب على القضاء بعدم الإختصاص بطلان إجراءات التحقيق و قد لاحظ الشارع في هذا الإستثناء الرغبة في عدم تعطيل سير التحقيق

و هكذا لا يصح للمحكمة أن تستند إلى ما أسفر عنه التفتيش من ضبط أدلة معلوماتية أو حتى شهادة من أجره لأنها تتضمن في واقع الأمر إخباراً منهم عن أمر ارتكبه مخالفاً للقانون، و بالتالي فإنّ الحكم الذي يؤسس على التفتيش الباطل أو على أقوال رجال الضبطية القضائية الذين أجره و لم يكن له سند في الإدانة غير محضر التفتيش يكون باطلاً، و الإعتماد على مثل هذه الشهادة في إصدار الحكم أمر تمقته الآداب، و هو في حد ذاته يشكل جريمة⁽¹⁾، و لما كان ما يثبت في محضر التفتيش من أقوال و إقرارات مقول بحصولها من المتهمين أمام القائم بالتفتيش لا يخرج عن كونه نوعاً من الشهادة، فإنّه لا يصح أيضاً الإعتماد على تلك الأقوال لأنّ ذلك يعني الإستعانة بعمل باطل بطريق غير مباشر⁽²⁾.

واقع الأمر يجب التفرقة بين بطلان التفتيش و بين بطلان محضر التفتيش، فعيوب محضر التفتيش التي يترتب عليها بطلانه لا يترتب عليها بطلان التفتيش، فبطلان المحضر شيء متميز عن بطلان التفتيش ذاته و مختلف عنه في مدى آثاره⁽³⁾، و الأمر كذلك في حالة بطلان الضبط، فقد سبق و أن أشرنا أنّ هذه المسألة مرتبطة بتوهين قيمة الدليل و ليس بطلانه، إذ يظل خاضعاً لتقدير المحكمة و لا تطبق قاعدة الإستبعاد في هذه الحالة.

و في القانون الأنجلوأمريكي، تقضي قاعدة الإستبعاد بضرورة طرح الدليل الجنائي الذي يتم التوصل إليه بطريقة تنطوي على إنتهاك للحقوق الأساسية للفرد حتى و لو كان الدليل

خاصة و أن بعض إجراءاته قد لا يتيسر إعادتها و هذا الإستثناء قاصر على الإختصاص بالتحقيق فلا يمتد إلى نواحي الإختصاص الأخرى كالإختصاص بالإحالة أو الحكم كما أنه لا يرد إلا على الحالات التي يقضى فيها بعدم اختصاص المحقق بإجراء التحقيق برمته و لا يمتد إلى حالات خروج المحقق غير المختص حدود الإختصاص المكاني أو النوعي بمناسبة القيام بإجراء أو أكثر من إجراءات التحقيق. لمزيد من التفصيل راجع: هلالى عبد الله أحمد، المرجع السابق، ص ص 235-236.

(¹) و في ذلك تقول محكمة النقض المصرية " للمنازل حرمة، ودخولها بغير رضاء أصحابها أو بغير إذن من السلطة القضائية المختصة، أو في غير الأحوال المرخص بها قانوناً يجرمه القانون ويعاقب فاعله، فدخول رجال الضبطية القضائية منزل أحد الأفراد وتفتيشه بغير إذنه ورضائه الصريح، أو بغير إذن السلطة القضائية أمر محظور، و التفتيش الذي يجره في تلك الحال باطل قانوناً، و لا يصح للمحاكم الإعتماد عليه بل و لا على شهادة من أجره، لأنّ مثل هذه الشهادة تتضمن إخباراً منهم عن أمر ارتكبه مخالف للقانون، فالإعتماد على مثلها في إصدار الحكم إعتماد على أمر تمقته الآداب، وهو في حد ذاته جريمة ". أنظر: الطعن رقم 1844 لسنة 3 قضائية، الصادر بجلسة 1933/12/27 ماسر إليه لدى إيهاب عبد المطلب، المرجع السابق، ص 134.

(²) سامي حسني الحسيني، المرجع السابق، ص 465.

(³) توفيق محمد الشاوي، المرجع السابق، ص 494.

ملائماً أو موضوعياً، و قد تعرضت هذه القاعدة لمعارضة شديدة من قبل الشراح بسبب طابعها المطلق، إذ سيكون عقبة خطيرة في سبيل إقامة العدالة إذا ما اعتقد بأنّ الدليل الذي قد تحصل عليه بواسطة طرق غير مشروعية لا يمكن إستخدامه ضد المتهم⁽¹⁾.

و قد قرّرت المحكمة العليا الفيدرالية الأمريكية سنة 1914 في قضية **Weeks v. United States** إستبعاد الدليل الناتج عن تفتيش غير صحيح، و ذكرت المحكمة تأسيساً لقضائها أنّ التّعديل الدستوري الرابع يضع قيوداً على ممارسة محاكم الولايات و الموظفين الفيدراليين لسلطاتهم و يحمي المواطنين في أشخاصهم و ممتلكاتهم من التفتيش المخالف للقانون، و تعرضت المحكمة بوجه خاص لمسألة إستخدام الدليل الناتج عن التفتيش الباطل، فأبرزت أنّ استخدام مثل هذا الدليل من شأنه تجريد حماية الدستور للأفراد من كل قمية، بل أن ذلك يعني - في نظر المحكمة - إنكاراً للحقوق الدستورية، و منذ ذلك الوقت تتطلب المحكمة من القائمين على تنفيذ القانون إحتراماً لتلك القاعدة كي تكون درعاً يقي نصوص الدستور من أن تصبح مجرد كلمات شكلية⁽²⁾.

و هو باتت ما تردده فيما بعد بعض محاكم الولايات⁽³⁾، ففي القضايا المتعلقة بالتفتيش، كانت المحكمة الفيدرالية العليا قد درجت على إعتبار استبعاد الدليل نوعاً من جبر

(1) هلاي عبد الله أحمد، المرجع السابق، ص 245.

(2) Weeks v. United States, 232 U.S. 383 (1914).

(3) Cahan, 44 Cal. zd 434, 282 P.zd 905 (1955).

في هذه القضية إنتهت المحكمة العليا في كاليفورنيا بإستعراض مبررات إعتقاد قاعدة إستبعاد الأدلة المستمدة من التفتيش الباطل قائلة " إن المحكمة بإعتقادها على دليل تفتيش باطل تكون قد إشتراك مع القائمين عليه في نشاطهم المخالف للقانون، و أنّه إذا كان الغرض الأصلي للتفتيش الباطل هو الحصول على أدلة إثبات تقدّم إلى المحكمة فإنّ نجاح القائمين بمخالفة القانون في مهمتهم يتوقّف تماماً على قبول الأدلة المقدّمة من قبلهم، و لا يجوز التّحدي بالتمييز بين الحكومة كسلطة إتهام و بين الحكومة كقاض، فإذا كان القانون لا يسمح للضباط و المحققين أن يرتكبوا هذه المخالفات عند مباشرتهم للتفتيش... فلا يجوز تحويل القاضي أن يمكن لهذه المخالفات فرصة النجاح... فإذا أصبحت الحكومة مخالفة للقانون و ترضى عن إنتهاكه بواسطة موظفيها، فإنّها بذلك تدعو كلّ شخص بأن يصبح مخالفاً للقانون و إلى مجتمع لا يحكمه القانون... فإذا أريد للضمانات الدستورية أن تُحمى فلا مفرّ من إهدار الأدلة المستمدة من مخالفتها...".

هذا الحكم المذكور و معلق عليه لدى: أحمد فتحي سرور، أثر التفتيش الباطل (مقارنة بين إتجاهات كل من القضاة الأمريكي والمصري)، المجلة الجنائية القومية، السنة الخامسة، سنة 1962، ص ص 154-159.

الضرر الذي حاق بمن وقعت عليه المخالفة، فضلا عن تحقيق الردع في مواجهة التجاوزات المحتملة⁽¹⁾.

و في إعتقادنا فإنّ أهم سابقة قضائية صادرة عن هذه الهيئة القضائية بخصوص قاعدة إستبعاد الأدلة المتحصلة من التفتيش الباطل، هو القرار الصادر في قضية *Mapp v. Ohio* والذي جاء فيه "إنّ المحكمة بقبولها الدليل المتحصل من التفتيش غير المشروع إنّما تشجع على مخالفة الدستور، و إذا كان تطبيق قاعدة الإستبعاد قد يؤدي إلى زهاب المجرم طليقا لمجرّد أنّ رجل البوليس قد أخطأ، فإن هذا إن حدث في بعض الأحوال إلّا أنّ ثمة إعتبار آخر هو حتمية نزاهة القضاء، فالمجرم قد يذهب طليقا إذا وجب ذلك، لكن القانون هو الذي يطلقه، و ليس هناك ما يمكن أن يحطم الدولة أكثر من فشلها في إحترام قانونها و إهمال ميثاق وجودها، و من ثمّ فلا يمكن السّماح بنقض الدستور بناء على نزوة موظف يحاول بإسم القانون ذاته أن يعطل تطبيقه، و هذا الحكم لا يعطي الفرد أكثر مما يكفله له الدستور، و لا يعطي رجل البوليس أقلّ ممّا يقتضيه شرف تنفيذ القانون، و يبيّن للمحاكم أنّ نزاهة القضاء لا غنى عنها لتحقيق العدالة الحقّة"⁽²⁾.

و هنا نسجل بإعجاب ما تواترت عليه محكمة النقض المصرية في قضائها من "أنّه لا يضير العدالة إفلات مجرم من العقاب بقدر ما يضيرها الإفئات على حقوق الناس و القبض عليهم بغير وجه حقّ".

الفرع الثاني: أثر بطلان التفتيش على الأدلة المستمدة من الإجراءات السابقة عليه

البطلان كجزء إجرائي لا ينال من العمل الإجرائي إلّا نتجية للعيب الذي أثار في صحته، و من ثمّ فلا يمتدّ البطلان إلّا إلى الأعمال التالّية له و المترتبة عليه، أي الذي يعد بطلان العمل السابق عليها بمثابة عيب في صحتها، أمّا الأعمال السابقة التي بوشرت مستقلة عن العمل الباطل فلا تمتدّ إليها آثار البطلان⁽³⁾، و بالتالي تبقى منتجة لجميع آثارها و هذه القاعدة من أولويات المنطق دون حاجة إلى نص في القانون عليها⁽⁴⁾.

(1) أحمد عوض بلال، المرجع السابق، ص 393.

(2) *Mapp v. Ohio*, 367 U.S. 643 (1961).

(3) أحمد فتحي سرور، المرجع السابق، ص 159.

(4) سامي حسني الحسيني، المرجع السابق، ص 469.

و قد إطرده القضاء على تأكيد هذه القاعدة، فقضت محكمة النقض المصرية "إنَّ كلَّ ما يقتضيه بطلان التفتيش هو إستبعاد الأدلة المستمدة منه، لا الوقائع التي حدثت يوم إجرائه، فإذا كانت المحكمة قد أقامت الدليل على وقوع الجريمة من أدلة أخرى لا شأن للتفتيش الباطل بها وكان الإثبات بمقتضاها صحيحاً لا شائبة فيه، فإن منعى الطاعنة في هذا الشأن لا يكون له محل"⁽¹⁾.

غير أن الإجراء الباطل و إن كان ليس له تأثير سلبي على الإجراءات السابقة و المعاصرة له، و بالتالي لا تتأثر به كقاعدة عامة، إلا أن هذه الإجراءات رغم كونها سابقة أو معاصرة قد يمتد إليها البطلان إذا توافر نوع من الإرتباط بينها و بين الإجراء الباطل⁽²⁾، خاصة في مجال التفتيش عن الأدلة المعلوماتية، فإذا تقرّر بطلان التفتيش في مرحلة التفتيش المعلوماتي، فإن التفتيش المادي يعتبر بالتبعية باطلا و يحضر الإستناد إلى آثاره لبناء حكم الإدانة، و الأمر كذلك في حالة الضبط المستند إلى أمر بالتسليم الموالي للأمر بالحفظ الصادر من سلطة التحقيق إلى مزود الخدمات، بحيث يترتب على بطلان التفتيش بطلان الضبط المعلوماتي، و بإختصار فإن بطلان التفتيش (الخطوة الثانية) ينجر عنها بطلان جميع الإجراءات السابقة عليه و التي تعتبر جزء متاصل من هذه العملية لا تستقل عنه.

و في مقابل ذلك قد يؤدي التفتيش المعلوماتي إلى نتائج بعضها صحيح و بعضها باطل، فلا تتأثر النتائج الصحيحة بالنتائج الباطلة، كأن يقع الضبط صحيحا على بيانات دون أخرى، كما لو وقع على رسائل متبادلة بين المتهم و شريك له، و شمل هذا الضبط أيضا رسائل متبادلة بين هذا المتهم و محاميه، ممّا يجعله صحيحا في الحالة الأولى و باطلا في الثانية، و لا شك أن الشق الأول يبقى صحيحا غير معيب رغم بطلان الشق الثاني⁽³⁾، و قد إستقر القضاء الفرنسي على ذلك في العديد من قراراته⁽⁴⁾، أو كأن يقع التفتيش صحيحا على بعض البيانات دون أخرى⁽⁵⁾.

(1) الطعن رقم 1289 لسنة 45 قضائية، الصادر بجلسة 1976/01/05، مشار إليه لدى إيهاب عبد المطلب، المرجع السابق، ص 119.

(2) هلاي عبد الله أحمد، المرجع السابق، ص 236.

(3) سامي حسني الحسيني، المرجع السابق، ص 467.

(4) Cass. Crim, 25 juin 2013, 12-88.021 , Bull. crim 2013, n° 155.

(5) United States v. Carey, 172 F.3d 1268, 1275 n.8 (10th Cir. 1999).

الفرع الثالث: أثر بطلان التفتيش على الأدلة المستمدة من الإجراءات اللاحقة عليه

أشرنا فيما سبق إلى أنه متى ثبت بطلان التفتيش تعين على القضاء إطراح الدليل المعلوماتي المستمد منه أو المترتب عليه مباشرة، و القضاء ببراءة المتهم ما لم تقم أدلة أخرى في الدعوى تكفي لثبوت التهمة، و تطبيق هذه القاعدة يثير فكرة "المعيار" في تحديد ما هو من الآثار المترتبة مباشرة على التفتيش و ما هو مستقل عنه؟ أي ما هو معيار الصلة المباشرة بين التفتيش المعلوماتي الباطل و الإجراءات اللاحقة و التي يترتب عليها بطلان الإجراء اللاحق؟

الواقع أنّ هذا المعيار مشكلة يختلف في شأنها نظر الفقهاء، فالبعض يذهب إلى أنه يكفي أن يكون العيب الذي أصاب الإجراء السابق من شأنه التأثير بأي وجه و لكن جوهرها في السير اللاحق للخصومة أو في بعض الأعمال التي تكونها، و قد أخذ على هذا الرأي أنه يوسع من نطاق البطلان، لأنّ كلّ إجراء في الخصومة يؤثر في الإجراءات اللاحقة عليه و

تتلخص وقائع قضية *United States v. Carey* ، أنّ المتهم Carey كان قيد التحقيق بجريمة حيازة مواد مخدرة تهيئة لعرضها للبيع ، و بعد حصول الضبطية القضائية على إذن بالضبط تم توقيف المتهم بمقر إقامته، و وافق على التفتيش و قدم معلومات حول كيفية العثور على المواد المتعلقة بالمخدرات، أين قامت الضبطية القضائية بضبط جهاز الحاسوب في انتظار الحصول على إذن منفصل للسماح لها بالتفتيش عن أرقام الهاتف وغيرها من الأدلة المتعلقة ببيع وتوزيع المواد المخدرة، و أثناء تنفيذ الإذن واجه مفتش الشرطة صعوبات في عرض بعض الملفات على جهاز الحاسوب الذي كان يستخدمه لإجراء التفتيش المعلوماتي، فقام بنسخ الملفات وفتحها على جهاز حاسوب مغاير ؛ و بعد ذلك، اكتشف ملف من نوع "jpg" ، تبين عند فتحه أنه يحتوي على مواد إباحية للأطفال و قد قام عقبا بتحميل ما يقارب 244 ملفا من ملفات "jpg" ، ولكنه لم يطلع إلا على بعضها لتحديد ما إذا كانت تحتوي على مواد إباحية للأطفال، على إثرها تقدم المتهم بطلب بطلان الأدلة المعلوماتية لبطلان التفتيش و قد قررت الدائرة العاشرة استبعاد هذه الحجّة مؤكدة على أنّ التفتيش كان مقبداً بالمواد المحددة في إذن التفتيش مستبعدة جميع الملفات عدا أول ملف "jpg" ، مضيفة أنّ مفتش الشرطة أثبت أنه لم يكن يبحث عن أدلة على الاتجار بالمخدرات أثناء فتح ملفات الصور، و أنه استأنف فقط التفتيش عن بيانات تتعلق بالمخدرات بعد إكماله لفترة خمس ساعات لتحميل هذه الملفات، و ذكرت أنه بعد أن فتح مفتش الشرطة أول ملف و رأى صورة عن المواد الإباحية المتعلقة بالأطفال، كان المحقق يدرك أنّ أسماء الملفات التي تحمل إحياء جنسيا يُحتمل أن تحتوي على صور مماثلة و قال إنه يتوقع العثور على مواد داعرة للقصر في كلّ الخطوات التي قام بها بعد عرض الملف الأول، و قد قضت المحكمة بصحة الدليل المعلوماتي المستمد من التفتيش و المتمثل في الصورة الرقمية الأولى التي أسفر عنها التفتيش عند فتح الحاسوب إستنادا إلى مبدأ الرؤية الواضحة و بذات الوقت قضت ببطلان باقي الأدلة (الصور) لأن هذا المبدأ لا يسمح بالتوسع في التفتيش بل يجب وقف التفتيش مؤقتا ريثما يتم الحصول إذن آخر للتفتيش عن الصور الداعرة.

لو لمجرد تأثير بسيط، و أن القانون يشترط توافر علاقة تساند بين الإجراء الباطل و الإجراءات التالية له، و ليس مجرد التأثير فيها⁽¹⁾.

و البعض يذهب إلى أن العمل الباطل يجب أن يكون وحده مصدرا للعمل الذي يليه، أي شرطا أو مفترضا " منطقيًا " له، فيكفي أن تكون هناك رابطة بين العاملين مقتضاهما أن يجد العمل اللاحق في العمل السابق أساسه المنطقي، سواء فيما يتصل بصحته أو بما يتصل بحقيقة الوقائع التي يثبتها، و قد قيل أنّ هذا الرأي يعيبه الإعتقاد على عناصر غير منطقية لتقدير صحة أو بطلان العمل اللاحق، و أنّ هذه العناصر غير القانونية لا يمكن أن تكون أساسا سليما للفصل في مسألة قانونية بحتة. و من جهة أخرى، فإنّه يذهب إلى بطلان العمل اللاحق ليس فقط إذا إعتد على العمل السابق في صحته، بل أيضا إذا أعتد عليه فيما يتصل بحقيقة الوقائع التي يثبتها، و لما كانت المشكلة هي البحث في صحة العمل فإنّه من الخطأ النظر إلى حقيقة أو كذب الوقائع التي يثبتها، إذ العمل قد يكون صحيحا رغم كذب هذه الوقائع⁽²⁾.

و المعيار السائد يذهب إلى إعتبار العمل اللاحق مرتبطا بالعمل السابق إذا كان هذا الأخير "مقدمة ضرورية" و "شرعية" و شرطا لصحة العمل اللاحق، و القانون هو الذي يتولّى تحديد إهمية الإجراء بالنسبة للإجراءات اللاحقة عليه، و على ذلك يجب أن ترتبط الإجراءات اللاحقة بالإجراء الباطل برابطة "نشوء" أو "سببية"، و لا تكفي أن تكون مجرد رابطة عرضية، بمعنى أن يكون الإجراء الباطل بالنسبة للإجراء اللاحق بمثابة السبب المنشئ له، بحيث يقال أنّه لولا الإجراء الباطل لما وقع الإجراء اللاحق⁽³⁾.

مثال ذلك الأمر بالندب للتفتيش الذي يعد شرطا جوهريا لصحة الإجراءات التي باشرتها الضبطية القضائية⁽⁴⁾، لذلك قضي بإمتداد البطلان إلى الإجراءات اللاحقة للعمل المعيب إذا

(1) سامي حسني الحسيني، المرجع السابق، ص 476.

(2) المرجع نفسه، ص 477.

(3) عثمان أمال عبد الرحيم، شرح قانون الإجراءات الجنائية، بدون رقم الطبعة، الهيئة المصرية العامة للكتاب، مصر، 1988، ص 390 و أنظر أيضا: ياسر الأمير فاروق، المرجع السابق، ص 736.

(4) أحمد فتحي سرور، المرجع السابق، ص 517.

كان العيب يتصل بها عملاً بمبدأ أنّ ما بنى على باطل فهو باطل⁽¹⁾، كما قُضي ببطلان الإستجواب و الوضع بالحبس المؤقت لبطلان التفتيش المجري خارج الوقت القانوني⁽²⁾.
و إذا عدنا إلى التفتيش المعلوماتي على وجه التحديد لوجدنا أنّ كافة إجراءاته متصلة ببعضها البعض، و يؤدي بطلان أحدها إلى تجريد الإجراءات التالية لها من آثارها القانونية، لأنّه لا يمكن أن ترتب أثراً قانوني لإجراء مخالف للقانون، فبطلان التفتيش المادي أو الضبط المعلوماتي بصورتيه سواء الضبط المترتب عن التفتيش في خطوته الأولى أو المترتب عن الأمر بالإنتاج (التسليم)، يؤدي إلى وصم تفتيش نظم المعلومات بالبطلان، بل في الأحوال التي يكون فيها البطلان قد ترتب نتيجة الحيلة و الخديعة في الوصول إلى الحاوية المادية للدليل معلوماتي أو إستعمال الإكراه و التعذيب لإرغام المتهم على فك التشفير، كلّ ذلك يؤدي إلى إهدار الأدلة المتسمدة عن سلسلة الإجراءات التي تتبعها.

و تقدير الصلة بين الاجراء الباطل و الاجراء اللاحق هي مسألة موضوعية تستقل بتقديرها محكمة الموضوع، على ضوء ظروف كلا الاجرائين، و بالنظر الى شخص القائم بكل منهما و كافة الظروف الواقعية الماثلة في الدعوى⁽³⁾، و يجب على المحكمة أن تلتزم

(1) قرار المحكمة العليا الجزائرية (الغرفة الجنائية الثانية) الصادر بتاريخ 1981/04/21، رقم 24905، مشار اليه لدى: أحمد الشافعي، المرجع السابق، ص 273.

(2) Cass. Crim, 21 juin 2016, 16-80.126, Bull. Crim 2016, n° 188.

(3) تطبيقاً لهذا المبدأ قضت محكمة النقض المصرية "إذا كان الحكم المطعون فيه بعد أن انتهى إلى بطلان القبض على الطاعن وتفتيشه قضي بإدانته قولاً منه أنه يستند في ذلك إلى عناصر الإثبات الأخرى المستقلة عن القبض و التفتيش و المؤدية إلى ذات النتيجة التي أسفر عنها، معتمداً في ذلك على أقوال اثنين من الشهود قررا بأن الطاعن هو صاحب السلة المضبوطة و أنه كان يحملها على ركبته، و أن الضابط أخرج منها و من جيوبه المخدرات المضبوطة، و إلى ما قرره الطاعن في تحقيق النيابة من أنّ المواد المخدرة قد ضبطت بتلك السلة، و إلى ما أسفر عنه تقرير التحليل من أن المادة المضبوطة حشيش و أفيون، و ما تبين منه من وجود فتات من الحشيش بجيوب صدر الطاعن و آثار بالكيس الذي كان بالسلة. لما كان ذلك، و كانت شهادة الشاهدين التي استندت عليها المحكمة في قضائها بالإدانة لا تخرج عن أن تكون تقريراً لما كشف عنه القبض والتفتيش الباطل وتأكيداً له، و لا يمكن أن يتصور لها وجود لولا وقوع التفتيش الباطل الذي أسفر عن وجود المخدر، و كان ما قرره الطاعن من العثور على المخدر في السلة لا يعد اعترافاً منه بحيازته أو إحرازه له و لا يعدو أن يكون تقريراً لما نتج عن التفتيش الباطل، كما أن نتيجة التحليل أثر من آثار ذلك التفتيش الباطل، و إذ انهارت هذه الأدلة فإنه لا يبقى في الدعوى دليل على نسبة إحرار المخدر إلى الطاعن و من ثم فإن الحكم المطعون فيه، إذ قضي بالإدانة استناداً إلى تلك الأدلة رغم قضائه ببطلان القبض و التفتيش، يكون معيباً ويتعين نقضه و القضاء ببراءة الطاعن من التهمة المسندة إليه". أنظر: الطعن رقم 1177 لسنة 32 قضائية، الصادر بجلسة 1962/11/27، مكتب فني سنة 13، قاعدة 191، ص 785.

جانب الحذر و أن تحتاط عند استظهارها للصلة بين التفتيش المعلوماتي الباطل و الإجراءات اللاحقة عليها و أن تدلل بذلك بأسباب سائغة على النتيجة التي خلصت إليها و أن يكون لهذه النتيجة ما يسندها من الأوراق المعروضة عليها⁽¹⁾.

و في حكم حديث لها نجد أن محكمة النقض المصرية قضت بأنه "لما كان الحكم المطعون فيه قد أثبت على الطاعن الثاني أنه اعترف أمام النيابة بالصور و الفيديو المستخرجة من هاتفه، فلا يجديه أن يكون فحص الضابط للهاتف قد وقع باطلاً، لتتحقق القرينة المستخرجة من الهاتف باعترافه، لما هو مقرّر من أن بطلان التفتيش بفرض وقوعه، لا يحول دون أخذ القاضي بجميع عناصر الإثبات الأخرى المستقلة عنه و المؤدية إلى النتيجة التي أسفر عنها التفتيش، و من هذه العناصر الاعتراف اللاحق للطاعن المذكور بالمستخرجات من هاتفه، كما لا يمنع المحكمة من الإعتماد على أقوال رجل الضبط فيما باشره من إجراءات و نما إليه من معلومات فيما لا يتصل بفحص الهاتف المدعى ببطلانه"⁽²⁾.

و هذا القضاء مناقضا لعقيدة هذه المحكمة الثابتة بالأحكام المشار إليها بالهامش، لأن الصلة المباشرة قائمة بين التفتيش الباطل للنظام المعلوماتي للمتهم ممثلاً في الهاتف و الذي قام به الضابط و ما أسفر عنه هذا العمل الإجرائي من صور و فيديوهات تثبت الإدانة و بين إقرار المتهم اللاحق أمام النيابة العامة بهذه الأدلة المعلوماتية، إذ أنه لولا هذا التفتيش الباطل و ما أسفر عنه لما تمت مواجهة المتهم بهذه المستخرجات الرقمية حتى يحصل الإقرار بها، فمعيار "النشوء" أو "السببية" قائم بين الإقرار و ما أسفر عنه تفتيش الهاتف، و على أي حال فإذا ثبت أن الإقرار لم يتأثر بالتفتيش الباطل جاز للمحكمة أن تعتمد عليه كدليل مستقل.

و لعلّ السؤال الذي يثار في الأخير يتعلّق مضمونه ببحث مدى إمكانية إعادة التفتيش الباطل على نظام المعلومات متى تقرّر بطلانه؟

(1) رؤوف عبيد ، المرجع السابق، ص 44.

(2) الطعن رقم 15854 لسنة 84 جلسة 2015/02/23.

لقد أجابت التشريعات بجواز إعادة التفتيش الباطل كقاعدة عامة⁽¹⁾، و في حكم نادر صادر عن القضاء الفرنسي أشارت محكمة النقض أنه لا يوجد مانع يحول دون قيام قاضي التحقيق من جديد بإجراء حزر أدلة كانت قد ضبطت ثم أعيدت لمالكها تنفيذاً لقرار قضائي سابق قضى بإلغاء الإجراءات، طالما أن محضر التفتيش و الحزر لا يستند و لا يعتمد بأيّة صفة من الصفات على الإجراءات الباطلة⁽²⁾.

غير أنه في مجال التفتيش المعلوماتي قد يتعدّر من الناحية العملية إعادة تفتيش نفس المحل الذي سبق و أن خضع للتفتيش، و قد سبق و أن أشرنا عند الحديث عن الحقوق الرقمية للمتهم حال تنفيذ التفتيش أن السلطة الإجرائية مكلفة في حالة تقرير بطلان التفتيش بحذف و إتلاف كافة البيانات التي ضبطتها بمناسبة هذا العمل الإجرائي، ثم إن طول أمد الإجراءات التي تستغرقها التحقيقات و المحكمة و طرق الطعن هي فترة كافية لوقوع الكثير من العبث و التعديل في البيانات الأصلية على نحو لم يعد من فائدة ترجى لتفتيشها، و لا يعقل أن يحتفظ المتهم بالبيانات المجرّمة ضمن محل آخر بعد أن كافح لدرء المسؤولية عنه.

المبحث الثاني

الجزاء التي توقع على مرتكب التفتيش غير المشروع عن الأدلة المعلوماتية

قلنا إن هناك نوعين من الجزاءات، جزاء يصيب التفتيش غير المشروع ذاته فيبطله، و هذا الجزاء قد فرغنا منه، أما الجزاءات الأخرى فهي تصيب من أمر بالتفتيش أو من قام بإجرائه و ذلك بإقامة مسؤوليته الشخصية، و إن كان بحث أنواع هذه المسؤوليات يدخل في دراسة فرع مستقل من فروع القانون - فهي بحسب الأصل تخرج عن نطاق بحثنا- و لكننا إتماماً لدراسة إشكالية البحث نشير بإيجاز إلى القواعد العامة التي تحكم تلك الجزاءات الفردية من مختلف زواياها سواء الجزائية (مطلب أول)، أو المدنية (مطلب ثاني)، أو التأديبية (مطلب ثالث).

(¹) أنظر المادة 336 من قانون الإجراءات الجزائية المصري التي تنص " إذا تقرّر بطلان أيّ إجراء، فإنّه يتناول جميع الآثار التي تترتب عليه مباشرة، و لزم إعادته متى أمكن ذلك " .

(2) Cass. Crim ,23 mars 1977, 75-92.170, Bulletin criminel 1977, n° 109.

المطلب الأول: الجزاء الجنائي

البطلان رغم أهميته إلا أنه يبقى مجرد جزاء سلبي يقتصر على منع التفتيش الذي أتخذ بالمخالفة للقانون من ترتيب آثاره، و من هنا يبدو الجزاء الجنائي المتمثل في إنزال العقوبة الجنائية على كل من تسول له نفسه مخالفة أحكام التفتيش أكثر جدية و فاعلية في إحترام الضمانات الإجرائية المتسوجبة، و إزاء ذلك نكتفي بالإشارة إلى أهم الجرائم التي يمكن نسبتها إلى من يجري التفتيش الباطل دون توسع في درساتها لأنها من موضوعات قانون العقوبات، و هي تختلف بحسب طبيعة المحل و المرحلة الإجرائية و أهمها جريمة إنتهاك حرمة المنزل (فرع أول)، و جريمة الدخول و البقاء غير المشروع في النظام المعلوماتي (فرع ثاني)، و جريمة إفشاء الأسرار التي يسفر عنها التفتيش (فرع ثالث).

الفرع الأول: جريمة انتهاك حرمة المنزل

لقد أعلى المشرع من شأن الحرّيات الفردية فأضفى عليها حماية جنائية دستورية، إذ تنص المادة 41 من الدستور "يعاقب القانون على المخالفات المرتكبة ضدّ الحقوق والحرّيات، وعلى كلّ ما يمسّ سلامة الإنسان البدنية و المعنوية"، و لم يكتف المشرع الدستوري بهذه القاعدة العامة بل خصّ المنازل بنص خاص يضمن حرمتها إزاء إجراء التفتيش بموجب المادة 47 من الدستور التي تقرّر "تضمن الدولة عدم انتهاك حرمة المسكن، فلا تفتيش إلاّ بمقتضى القانون، وفي إطار احترامه، و لا تفتيش إلاّ بأمر مكتوب صادر عن السّلطة القضائية المختصة".

من منطلق هذه القاعدة الدستورية يقرّر المشرع العادي الجزائري - أسوة بالمشرع المصري⁽¹⁾ و المشرع الفرنسي⁽²⁾ - المسؤولية الجنائية للموظف عن مساسه بحرمة مسكن الغير بغير مبرر قانوني بموجب المادة 135 من قانون العقوبات، تحت عنوان إساءة إستعمال السلطة ضد الأفراد على أنّ " كلّ موظف في السلك الإداري أو القضائي و كلّ ضابط شرطة

(1) تقرّر المادة 128 من قانون العقوبات المصري التي تنص " إذا دخل أحد الموظفين أو المستخدمين العموميين أو أي شخص مكلف بخدمة عمومية اعتمادا على وظيفته منزل شخص من آحاد الناس بغير رضائه فيما عدا الأحوال المبينة في القانون أو بدون مراعاة القواعد المقررة فيه يعاقب بالحبس أو بغرامة لاتزيد على مائتي جنيه."

(2) تنص المادة 8/432 من قانون العقوبات الفرنسي " كل موظف عام أو مكلف بخدمة عامة قام خلال ممارسة وظيفته أو مهنته بالدخول أو بالشروع في الدخول في مسكن الغير بدون رضائه في غير الحالات المنصوص عليها في القانون يعاقب بالحبس لمدة سنتين و بغرامة 3000 اورو."

و كلّ قائد أو أحد رجال القوّة العمومية دخل بصفته المذكورة منزل أحد المواطنين بغير رضاه و في غير الحالات المقرّرة في القانون، و بغير الإجراءات المنصوص عليها فيه يعاقب بالحبس من شهرين إلى سنة و بغرامة من 500 إلى 4000 دج دون الإخلال بتطبيق نص المادة 107".

و تنص المادة 107 من نفس القانون على أنّه " يعاقب الموظف بالسجن المؤقت من خمس سنوات إلى عشر سنوات إذا أمر بعمل تحكيمي أو ماس سواء بالحريّة الشّخصية للفرد أو بالحقوق الوطنية لمواطن أو أكثر"⁽¹⁾.

و قد إنتهينا عند تناولنا لضوابط التفتيش أنّه يحضر على سلطة التحقيق أو الضبطية القضائية في إطار النذب أو في أحوال التلبس إنتهاك حرمة المنزل في غير الأحوال التي نصّ عليها القانون، و إذا حدث ذلك فإنّ القانون يقرّر المسؤولية الجنائية للقائم بالتفتيش، غير أنه يلزم لتقرير هذه المسؤولية توافر أركان تلك الجريمة و التي تتمثّل في أن يكون الجاني موظفاً أو مستخدماً عمومياً أو مكلف بخدمة عامة، و هذا ينصرف إلى جميع أعضاء الضبط القضائي و أن يكون الجاني قد أساء إستعمال تلك الوظيفة كما يلزم أن يكون الدخول إلى المسكن قد تم رغم إرادة صاحبه دون أن يكثرث أو يعبأ بهذا الإعتراض⁽²⁾.

و يكون بذلك المشرع قد فرّق بين جريمة إنتهاك حرمة المنزل من أحد الأفراد و بين هذه الجريمة الواقعة من قبل الموظف، و من ثمّ تتحقق الجريمة و لو وقع الولوج إلى المسكن

(¹) و مفهوم الموظف هنا ينطبق على سلطة التحقيق و النيابة العامة أو الضبطية القضائية و ليس قاصراً على أعضاء الضبط القضائي و إن كان الشائع في الواقع ان التفتيش عادة ما يتم من قبلهم، كسلطة استثنائية في حالة التلبس بالجريمة او في إطار تنفيذ الإنابة القضائية، بما يجعل المخالفة القانونية كفعل مادي ترتكب من قبل هؤلاء، و هذا المفهوم مستوحى من ص المادة 2 من القانون 06-01 المؤرخ في 20 سديمبر 2006 المتعلق بالوقاية من الفساد و مكافحته، الجريدة الرسمية عدد 14.

(²) عادل عبد العال خراشي، ضوابط الاستدلال عن الجرائم في الفقه الاسلامي و القانون الوضعي، بدون رقم الطبعة، درا الجامعة الجديدة، 2006، مصر، ص 610.

من غير إستعمال إحدى الوسائل المنصوص عليها بالمادة 295 من قانون العقوبات⁽¹⁾، لأن الحماية مقرّرة في هذا النّص لحرمة المسكن و أسرار شاغليه و ليس للمنزل كملكية⁽²⁾. و قد استعمل المشرع لفظ "المواطن"، و مقتضى ذلك أنّ الجريمة لا تقوم إذا انتهكت حرمة مساكن أجنب لهم إقامة بالتراب الوطني، و هو بذلك يكون قد أنكر عنها هذه الحماية⁽³⁾، غير أنّنا لا نعتقد أنّ نيّة المشرع انصرفت إلى ما ترمي إليه دلالة الألفاظ، لأنّه لا يوجد أي سبب يدعو إلى المغايرة بين مسكن المواطن و مسكن الأجنبي في الحماية، بدليل و أنّ المشرع ذاته إستبعد هذ القيد عند النّص على جريمة إنتهاك حرمة المنازل من قبل الأفراد ممّا يجعل المشرع مطالب بإعادة صياغة النص.

و لا يكفي عدم وجود مسوغ قانوني للتنقيش حتى تقوم المسؤولية الجنائية للقائم به، بل يلزم كذلك توافر القصد الجنائي، و يعدّ هذا القصد قائماً طالما كان القائم بالتنقيش عالماً بأنّه يدخل مسكن شخص رغم إراداته و في غير الأحوال التي يبيح له فيها القانون الدخول، و لذا فإنّه لا يمكن أن يكون الباعث الذي حمّله على الدخول أي إعتبار في إباحة الفعل فلا يهم أن يكون قد دخل المنزل مبالغته منه في الحرص على مصلحة الحكومة و الصالح العام، أو بقصد التّجسس و الإستطلاع أو مدفوعاً برغبة شخصية أو باعث شخصي⁽⁴⁾.

(1) و هذا النص خاص بتجريم فعل انتهاك حرمة المنزل من قبل أحد الأفراد حيث تنص المادة 295 من قانون العقوبات الجزائري "كل من يدخل فجأة أو خدعة أو يقتحم منزل من مواطن يعاقب بالحبس من سنة إلى خمس سنوات و بغرامة من 1.000 دج إلى 10.000 دج و إذا ارتكبت الجناة بالتهديد أو بالعنف تكون العقوبة بالحبس من خمس سنوات على الأقل إلى عشر سنوات على الأكثر و بغرامة من 5.000 إلى 20.000 دج".

(2) و قد عبرت على ذلك محكمة النقض المصرية في أحد أحكامها قائلة " لما كانت حرمة المسكن إنما تستمد من حرمة الحياة الخاصة لصاحبه، فإنّ مدلول المسكن يتحدد في ضوء ارتباط المسكن بحياة صاحبه الخاصة، فهو كل مكان خاص يقيم فيه الشخص بصفة دائمة أو مؤقتة، وعلى ذلك فإن عدم اكتمال بناء المسكن أو عدم تركيب أبواب أو نوافذ له لا يقدح في أنه مكان خاص طالما أنه في حيازة صاحبه يقيم فيه و لو لبعض الوقت ويرتبط به و يجعله مستودعاً لسره و يستطيع أن يمنع الغير من الدخول إليه إلا بإذنه، فلا يعد مكاناً متروكاً يباح للغير دخوله دون إذنه و لا يجوز لرجال السلطة العامة دخوله إلا في الأحوال المبيّنة في القانون". انظر : الطعن رقم 674 لسنة 56 قضائية الصادر بجلسة 4986/06/04، مكتب فني سنة 37 ، قاعدة 121، ص 640.

(3) رحال عبد القادر، الحماية الجزائرية للحق في الخصوصية دراسة مقارنة بين الشريعة الإسلامية و القانون الجزائري الجزائري، أطروحة دكتوراه، كلية العلوم الإنسانية و الاجتماعية، جامعة وهران 1، الجزائر، 2015، ص 284.

(4) عادل عبد العال خراشي، المرجع السابق، ص 612.

و يُلاحظ أنّ المشرع الفرنسي فيما يتعلّق بجريمة إنتهاك حرمة المكسّن التي تقع من آحاد النَّاس (المادة 226 فقرة 4 من قانون العقوبات) جرّم فضلا عن دخول مسكن الغير، فعلا آخر هو فعل البقاء بالمسكن رغم إرادة صاحب الشّان، و يفرق بذلك في شأن الجريمة الواقعة من قبل الموظف، و هي الحالة التي تفترض دخولا مشروعا من قبل ضابط الشرطة القضائية للمسكن في إطار القيام بالتفتيش بحثا عن أجهزة التخزين الرقمية التي يحتمل أن تحتوي على الدليل المعلوماتي المستهدف بالتفتيش، إلاّ أنّه و رغم ضبط كافة الدعامات المادية الموجودة بهذا المحل يصير هذا الأخير على مواصلة البقاء بالمنزل، و لا شك أن النص القانوني بصورته الحالية لا يتناول تفاصيل هذه الحالة، بيد أنّ بعض الفقه يرى إمكانية إستعابه لها⁽¹⁾، و هو ما ذهب إليه القضاء المصري في حكم لا نؤيده، إذ التوسع في تفسير النص أدى الى تجريم سلوك لم يجرمه المشرع و تلك مخالفة واضحة لقاعدة الشرعية الجنائية⁽²⁾.

الفرع الثاني: جرمتي الدخول أو البقاء غير المشروع في النظام المعلوماتي.

خلصنا فيما سبق إلى أنّ المشرع الدستوري قد إستقن من الحرمة التي بات يتمتع بها النظام المعلوماتي في الوقت الراهن، خاصة بعد الإنتشار الرهيب لوسائل الإتصال و شيوع إستعمالها بين الأفراد في مختلف جوانب حياتهم، و على الأخص شؤون الحياة الخاصة التي باتت تحفظ ضمن هذه الأوعية الرقمية، فقرر بموجب 46 من الدستور أنّه "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، و يحميها القانون. سرية المراسلات والاتصالات الخاصة بكلّ أشكالها مضمونة. لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلّل من السلطة القضائية. و يعاقب القانون على انتهاك هذا الحكم. حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون و يعاقب على انتهاكه".

(1) كاظم السيد عطية، الحماية الجنائية لحق المتهم في الخصوصية دراسة مقارنة، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 2007، ص 402.

(2) حيث قضت محكمة النقض المصرية في حكم نادر لها بأن "وجود مأمور الضبط القضائي داخل مسكن الطاعن المأذون بتفتيش مسكنه هو وجود عرضي متى استنفذ الغاية منه تعين على مأمور الضبط القضائي الخروج منه"، طعن رقم 163 لسنة 4 قضائية، الصادر بجلسة 12/31 /1934، مشار إليه لدى كاظم السيد عطية، المرجع السابق، ص 402.

يجري التسؤل في ضوء هذه القاعدة الدستورية عن مدى امكانية مساءلة أعضاء السلطة القضائية جنائيا حال اتخاذ إجراءات التفتيش المعلوماتي في غير الحالات المنصوص عليها قانونا؟

لقد خلا القانون 04/09 من الإشارة إلى إمكانية توقيع جزاءات جنائية على القائم بالتفتيش المعلوماتي إذا ما خالف الضوابط المقررة قانونا لإعمال هذا الإجراء، بيد أنه بالإطلاع على قانون العقوبات يتبين و أنّ المشرع جرّم سلوك الإعتداء على المراسلات في صورتها التقليدية حال صدور هذا الفعل عن الموظف بفهوم عام، بحيث تقرّر المادة 303 من قانون العقوبات أنّ "كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير و ذلك بسوء نية و في غير الحالات المنصوص عليها في المادة 137 يعاقب بالحبس من شهر (1) إلى سنة (1) و بغرامة من 25.0000 دج إلى 100.0000 دج أو بأحدى هاتين العقوبتين فقط"⁽¹⁾.

و المستفاد من هذا النص أنّ المشرع ضيّق من نطاق دائرة التّجريم ليس فقط بقصر الحماية على المراسلات في صورتها التقليدية، بل إنّ الحماية مقرّرة فقط للبيانات المعلوماتية المخزّنة في شكل مراسلة، فليس للنص محل للتطبيق إذا كانت البيانات مخزّنة على ذاكرة الحاسوب أو الهاتف و تم توليدها بمقتضى هذا النّظام المعلوماتي ذاته دون أن تكون مستجلبة من جهاز آخر، و هذه النتيجة تدفعنا إلى طرح تساؤل مؤداه هل تنطبق جريمة الدخول غير المصرح به للنّظام المعلوماتي المنصوص عليها بموجب المادة 394 من قانون العقوبات تطبق على أعضاء السلطة القضائية حال إجراء تفتيش معلوماتي باطل؟

إنّ المنتبّع لمنهج المشرع الجزائري حين تجريمه لمختلف صور الإعتداء على الحياة الخاصة للأفراد يجده قد سلك منهج التّمييز بين وقوع الجريمة من قبل فرد على فرد، و بين وقوعها من قبل سلطة على فرد، إذ رفع العقوبة حين تقع الجريمة على فرد من ممثلي السلطة العامة إعتمادا على وظيفتهم، و هو إتجاه ينم على سياسية جنائية رشيدة، ذلك أنّه لا يجوز أن تكون هناك مساواة في المعاملة العقابية بين ممثلي السلطة و قد أمدهم القانون بسلطة

(1) تنص المادة 137 من قانون العقوبات " كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم بفض أو إختلاس رسائل مسلمة إلى البريد أو يسهل فضها او اختلاسها أو اتلافها يعاقب بالحبس من ثلاثة (3) أشهر إلى خمس (5) سنوات و بغرامة من 30.000 دج إلى 500.000 دج و يعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق و يختلس أو يتلف برقية أو يذيع محتواها و يعاقب الجاني فضلا عن ذلك بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات.

غير محدّدة أو إمكانيات ضخمة تتيح لهم فرصة التصنّت على مختلف المحادلات و المراسلات و إعتراضها، و بين الفرد العادي الذي لا يمكن أن يوقع عدوانا شبيها إلا في ما ندر و في أحوال إستثنائية⁽¹⁾.

إلا أنّ المشرع خالف نهجه السابق سالكا إتجاه المشرع الفرنسي الذي لم يفرّق بين جريمة الدخول غير المشروع للنظام المعلوماتي الواقعة من قبل الأفراد أو من قبل ممثلي السلطة العامة، فتعتبر هذه الجريمة من جرائم "الفاعل المطلق" إذ لم يشترط المشرع وجود صفة معينة في فاعل الجريمة، فقد يكون فردا عاديا و قد يكون موظفا عاما⁽²⁾، حيث تنص المادة 394 من قانون العقوبات "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كلّ أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك...".

و تقوم هذه الجريمة بمجرد الولوج غير المصرّح به إلى النظام المعلوماتي، بمعنى أنّ الدخول يتم دون وجه حقّ و يجري التساؤل في ضوء ذلك حول طبيعة هذه الجريمة، فيما إذا كانت من قبيل الجرائم المادية ذات النتيجة أم أنّها جريمة شكلية فحسب؟ بمعنى آخر هل يجب أن يكون دخول أعضاء السلطة القضائية إلى النظام المعلوماتي دون مسوغ قانوني قد ترتب عنه أثر ما، أي يؤدي إلى تحقيق نتيجة إجرامية محدّدة أم أنّ الجريمة تتحقق بمجرد الدخول غير المشروع إلى النظام المعلوماتي؟

أغلب التشريعات الجنائية- بما فيها التشريع الجزائري- التي تناولت جريمة الدخول غير المشروع إلى النظام المعلوماتي تأخذ بالدخول المجرد، حيث تقوم الجريمة و لو لم يترتب عن هذا الفعل أي فائدة أو ضرر، طالما أنّ ذلك الدخول كان بدون وجه حقّ⁽³⁾، و من الأمثلة على هذه التشريعات المقارنة، القانون الفرنسي الذي إعتبر أنّ مجرد الدخول يشكل الركن المادي لجريمة الدخول غير المشروع للنظام المعلوماتي في صورتها البسيطة (م 1-1323)، و نفس الإتجاه نجده في التشريع القطري (م 371)، و ذات الشيء نجده في قانون الجزاء

(1) ياسر الأمير فاروق، المرجع السابق، ص 748.

(2) رمسيس بهنام، النظرية العامة للقانون الجنائي، الطبعة الثانية، منشأة المعارف، مصر، 1995، ص 525.

(3) حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، مصر، 2007، ص 273.

العماني(م276 مكرر)⁽¹⁾، و في اعتقادنا كان الأحرى بالمشرع أن ينص على صفة الفاعل كظرف من ظروف التّشديد⁽²⁾.

كما قد يتّخذ النشاط الإجرامي الذي يتكوّن منه الركن المادي في الجريمة محل الدراسة صورة البقاء داخل النظام المعلوماتي، و يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحقّ في السيطرة على هذا النظام، و قد يتحقق البقاء المعاقب عليه داخل النظام مستقلاً عن الدّخول إلى النظام و قد يجتمع، و يكون البقاء معاقب عليه إستقلاً حين يكون الدّخول إلى النظام مشروعاً، و من أمثلة ذلك إذا تحقق الدّخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده و ينسحب فوراً، فإذا بقي رغم ذلك فإنّه يعاقب على جريمة أيضاً في الحالة التي يستمر فيها باقياً داخل النظام بعد المدّة المحدّدة له للبقاء داخله⁽³⁾.

الحقيقة أنّ قيام المسؤولية الجنائية لأعضاء السلطة القضائية عن جريمة الدّخول غير المشروع إلى النظام المعلوماتي أو جريمة البقاء غير المشروع داخل هذا النظام قد لا يتيسّر إثباتها إلا في حالة إرتكبها من طرف ممثل السلطة بشكل مستقلّ عن إجراء التفتيش مستغلاً صفته و ليس بمناسبة التفتيش، لأنّه يستحيل إثبات ركن العمد و إتجاه نيّة الفاعل إلى إرتكاب هذه الجريمة حال تنفيذ التفتيش بالولوج إلى نظام معلوماتي أو جزء منه و كان هذا النظام خارج نطاق الإذن القضائي، أي غير مصرّح بالولوج اليه، لأنّ التفتيش بحذ ذاته يتميّز بمنطق إمتدادي أجازة المشرع وفق ضوابط قانونية ليست واضحة المعالم يغلب عليها الطابع

(¹) في حين فإن البعض الآخر من التشريعات يشترط تحقق نتيجة معينة تتمثل في الوصول إلى المعلومات التي يتضمنها النظام المعلوماتي لقيام الجريمة، كما هو الحال في التشريع الفيدرالي الأمريكي لجرائم الحاسب الآلي المنصوص عليها في القسم 1030 § 18 U.S. Code، و قد أورد المشرع سبعة صور لهذه الجريمة.

لمزيد من التفصيل راجع اورين كير، نطاق الجريمة الافتراضية (تفسير الدخول و التصريح به في إطار تشريعات الإساءة الى الحاسوب)، مجلة القانون، جامعة نيويورك، عدد 78، نوفمبر 2003، ترجمة عمر محمد بن يونس، الطبعة الثانية، الأكاديمية الدولية للتجارة الالكترونية، 2008، ص 58 و ما بعدها.

(²) تنص المادة 51 من قانون الفطري رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية "تضاعف العقوبة المقررة للجرائم المعاقب عليها بموجب أحكام هذا القانون، إذا ارتكبها أو سهل ارتكابها، موظف عام مستغلاً صلاحياته وسلطاته في ذلك".

(³) علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونياً، بحث مقدم لمؤتمر مقدم إلى مؤتمر القانون و الكمبيوتر، المنعقد في الفترة بين 1 و 3 ماي 2000 جامعة الإمارات العربية المتحدة، كلية الشريعة و القانون، الطبعة الثالثة، 2004، ص 601.

التَّقني، و من ثمَّ فإنَّ التَّجاهل الصَّارخ لنطاق الإذن القضائي ليس له إرتباط سوى بماديات الجريمة، و لا يقيم المسؤولية، فالمشرع ذاته أهمل ضابط تحديد المحلِّ وفقاً للمفهوم المعلوماتي⁽¹⁾، ممَّا يقع على المحكمة إتخاذ واجب الحذر عند تقديرها لمدى قيام ركن العمدة في هذه الحالة لأنَّ استظهاره أمر غاية في الصعوبة.

و تفرّيعاً على ذلك، فإنَّ القائم بالتفتيش قد يلج النظام المعلوماتي بشكل مشروع وفقاً للقانون، غير أنَّه قد يواصل بقاءه داخل النظام المعلوماتي منتهكاً خصوصية الأفراد على الرِّغم من التَّمكّن من ضبط الدليل المعلوماتي المستهدف بالتفتيش خلال فترة وجيزة، و من النّاحية العملية فإنَّ تصور قيام هذه الجريمة متعذر خاصة إذا كان التفتيش يستهدف الوصول إلى أدلة عن جرائم المحتوى، لأنَّ الفاعل يتدرّج بمواصلة البقاء داخل النظام بداعي الإستمرار في البحث عن أدلة أخرى لا تتفصل عن الدليل المأذون بالتفتيش عنه، كما هو الحال عند التفتيش عن الصور الدّاعرة للأطفال القصر، فضبط الصورة الأولى لا يحول دون مواصلة التفتيش لضبط غيرها، ممَّا قد يطيل فترة البقاء داخل النظام بشكل قد يجد له ما يبرّره، و من جهة أخرى فإنَّ المتهم يجهل أصلاً قيام هذه الجريمة في حقه لأنَّ التفتيش في مرحلته الثّانية (الفحص الإلكتروني) يتم في مختبرات التحليل الحاسوبي الشرعي في غياب المتهم⁽²⁾.

و قد سبق لفت النّظر إلى هذه المسائل عند الحديث عن الضمانات الوقائية لحماية الشّرعية الإجرائية عن طريق تحديد فترة التفتيش في المرحلة الثّانية من هذا العمل الإجرائي، و تحرير محضر - في شكل خبرة تقنية - يثبت سلسلة عمليات التفتيش المعلوماتية بشكل دقيق يبيّن فيه ساعة بداية التفتيش و تاريخ الوصول إلى الدليل المعلوماتي و تاريخ إنتهاء التفتيش و مغادرة النظام المعلوماتي (محل التفتيش)، و تقرير بطلان جميع الأدلة المعلوماتية المكتشفة بشكل عرضي منعا من التّعسف و الشّطط⁽³⁾، ذلك أنّ تقرير المسؤولية الجزائية للقائم بالتفتيش في هذه الفروض جميعاً يعد ضرباً من ضروب الخيال⁽⁴⁾.

(1) راجع ما سبق، إشكالية المنظور المزدوج لمحل التفتيش ص 166 و ما بعدها.

(2) راجع ما سبق، المبررات العملية لتراجع ضمانات حضور المتهم لعملية التفتيش المعلوماتي، ص 222 .

(3) راجع ما سبق، بدائل قاعدة استراتيجية تنفيذ التفتيش ص 248 و ما بعدها.

(4) بقي أن نشير بهذا الصّدّد أنّ حديثنا عن هاتين الجريمتين من جرائم المساس بنظم المعالجة الآلية للمعطيات لا ينفي تصور قيام باقي الجرائم التي نص عليها المشرع بموجب المواد 394 مكرر الى 394 مكرر 7 من قانون العقوبات في حقّ أعضاء السلطة القضائية متى قامت الأركان المتطلبة قانوناً، غير أنّ جريمة الولوج غير المشروع إلى النظام المعلوماتي للمتهم و البقاء داخل النظام دون وجه حقّ، تعتبر من الفروض المحتملة بشكل كبير التي

الفرع الثالث: جريمة إفشاء أسرار التحقيق

سواء كان التفتيش عن الأدلة المعلوماتية صحيحا أو باطلا، فإن القانون يعاقب من أفشى الأسرار الناتجة عنه، بل و يعاقب على إفشاء أسرار التحقيق عامة، و لا يعترض على ذلك بأن التحقيق أصبح حضوريا لأنّ هذه الضمانات حقّ للخصوم أمّا الاحتفاظ بسريّة نتائج التحقيق و التفتيش فواجب على القائمين به، و هذا الواجب لا زال مفروضا عليهم بحكم وظيفتهم، و هم يعتبرون بالنسبة لها من أمناء الأسرار الذين يعاقبهم القانون على إفشاء سر المهنة، و ليس هذا الواجب مقصورا على قاضي التحقيق أو عضو النيابة العامة، بل يلتزم به جميع من حضروا التفتيش بحكم وظيفتهم أو بحكم مهمتهم⁽¹⁾.

و يتحقق هذا الفعل في الجريمة بإفشاء السرّ الذي أوتمن عليه بغض النظر عن وسيلة الإفشاء سواء شفويا أو كتابيا، فالعبرة بحدوث فعل الإفشاء، و يكفي علم الفرد به حيث لا يشترط لإكتمال الإفشاء أن يعرفه عدد محدد من الأفراد، لأنّ السرّ ما هو إلا واقعة معينة ينبغي أن تظلّ في كتمان بعيد عن علم الكافة بحيث ينحصر العلم بها في شخص أو أشخاص ألزمهم المشرع بالكتمان، و فعل الإفشاء مجرد الإفشاء بالسرّ إلى الغير أي اطلاع الغير عليه⁽²⁾.

و بناء على سلف بيانه، فإنّ النتيجة الإجرامية لهذا الفعل تتمثل في أن يصبح سرا معلوما لغير من عهد إليه القانون الاطلاع على السرّ، و سواء بتعمد عضو السلطة القضائية إفشاء السرّ أو ترك الغير يطّلع عليه و كان في مقدوره منعه إلا أنّه يتخلف عن واجبه، فتقوم الجريمة و لو كان المطلع على السرّ شخصا واحدا⁽³⁾، بل إن هذه الجريمة تعتبر قائمة و لو

يمكن وقوعها من قبل ممثلي السلطة العامة بمناسبة التحقيق و التفتيش عن الأدلة المعلوماتية خاصة و أن التفتيش يتمّ في غياب صاحب الشأن مما يفتح باب التعسف من قبل الضبطية القضائية القضائية لأن سلطة التحقيق عادة ما تلجئ إلى النذب في التفتيش المعلوماتي.

(1) توفيق محمد الشاوي، المرجع السابق، ص 517.

(2) عبد القادر محمد القيسي، التحقيق الجنائي السري، الطبعة الأولى، المركز القومي للإصدارات القانونية، مصر، 2016، ص 157.

(3) Cass Crim, 16 mai 2000, 99-85.304, Bulletin criminel 2000 N° 192

تعلق الأمر بمعلومات سيكون مآلها الكشف في جلسة علنية في مرحلة المحاكمة، لأنّ النصّ العقابي حدّد نطاق السّرية بمرحلة التحقيق و ليس المحاكمة⁽¹⁾.

و بطبيعة الحال فإنّ مبدأ سرية التحقيق و ما يسفر عنه من أسرار و معلومات مبرّر بضرورة حماية حقوق الخصوم، بما في ذلك الحقوق التي تستوجبها قرينة البراءة ، و ضمانا لسلطة القضاء و و نزاهته⁽²⁾، لذا تم النصّ على هذه القاعدة في معظم التشريعات المقارنة، حيث قرّر المشرع بموجب المادة 11 من قانون الإجراءات الجزائية " تكون إجراءات التّحري و التحقيق سرية، ما لم ينص القانون على خلاف ذلك و دون إضرار بحقوق الدفاع، و كل شخص يساهم في هذه الإجراءات ملزم بكتمان السّر المهني بالشروط المبيّنة في قانون العقوبات و تحت طائلة العقوبات المنصوص عليها فيه"⁽³⁾.

و قد تضمن قانون الإجراءات الجزائية نصوصا قاطعة في هذه المسألة، فلم يكتف فقط بالنصّ على حضر إفشاء أسرار التحقيق بل عاقب أيضا من يذيع الأسرار التي اطلع عليها أثناء حضوره إجراءات التحقيق أيا كانت الصفة التي حضر بها و ذلك في المادة 85 من هذا القانون - المستوحاة من المادة 58 من قانون الإجراءات الجزائية الفرنسي - التي تقرّر " يعاقب بالحبس من شهرين إلى سنتين و بغرامة من 2000 إلى 20.000 دج كل من أفشى أو أذاع مستندا متحصلا من تفتيش لشخص لا صفة له قانونا في الإطّلاع عليه و كان ذلك بغير إذن من المتهم أو من خلفه أو الموقع بإمضائه على المستند أو الشخص المرسل إليه و كذلك كل من استعمل ما وصل إلى علمه منه ما لم يكن ذلك من ضرورات التحقيق القضائي"⁽⁴⁾.

(1) Cass Crim, 28 septembre 2004, 03-84.003, disponible à l'adresse:

<https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007610535>, (consulté le 20 février 2020).

(2) Cass Crim, 19 juin 2001, 99-85.188, Bull. Crim 2001 n° 149.

(3) تقابلها المادة 75 من قانون الإجراءات الجنائية المصري، و المادة 11 من قانون الإجراءات الجزائية الفرنسي.

(4) و بطبيعة الحال فإنّ هذه الجريمة تختلف من حيث أركانها على جريمة إفشاء أسرار المتهم المتحصل عليها ليس في إطار التحقيق بل نتيجة ارتكاب جريمة من جرائم المساس بنظم المعالجة الآلية للمعطيات حيث تقرّر المادة 394 مكرر 2 " يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات و بغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي...2 - حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم."

و جريمة إفشاء سرية التحقيق أو محتوى مستند رقمي متحصل عليه في إطار التفتيش عن الأدلة المعلوماتية هي جريمة عمدية، و من ثم فإن الإهمال أو عدم الإحتياط من جانب المؤتمن على الأسرار التي أسفر عنها التفتيش و الذي أدى إلى اطلاع الغير عليه لا يشكل جريمة⁽¹⁾.

واقع الأمر أن النص التجريمي لا يفرق في العقوبة الموقعة على الجاني، فالجزاء واحد و إن اختلفت وسيلة الجريمة المستعملة في نشر أسرار التفتيش، أو تباينت صفة الجاني ممن حضر هذا العمل الإجرائي، و هذا النص محل نظر في تقديرنا حال تطبيقه على جريمة إذاعة و نشر أسرار التفتيش المعلوماتي، إذ أن القيام بهذه الفعل إذا ما تم عبر الأنترنت بمختلف التطبيقات التي تتيحها برامج النشر الرقمي يجعل حجم خطورة هذا الفعل تتجاوز ما هو مألوف عادة بمنظور اطلاع فرد معين أو عدد محدود من الأفراد على أسرار ليس لهم حق الإطلاع عليها، أما النشر الرقمي فكبسة زر تتيح للعالم أجمع الإطلاع عليها خاصة إذا ما تعلق الأمر ببيانات المحتوى، و عدم المغايرة بين الأمرين في مقدار العقاب يتجاهل الفارق الواضح بين الفعلين، إذ أن وسيلة المستعملة في الإفشاء محل اعتبار في نظرنا، و جب جعلها ظرف من ظروف التشديد.

و إذا كنا قد تناولنا هذه الطائفة من الجزاءات الموقعة على القائم بالتفتيش الباطل عن الأدلة المعلوماتية، فإن ذلك لا يعني حصر كل تلك الجزاءات التي نص عليها التشريع ضمن نطاق هذه الجرائم المذكورة، لأن السلطة القائمة بهذه العمل الإجرائي قد تقترف أفعال أخرى تدخل في دائرة التجريم و العقاب بمناسبة تنفيذ الأنظمة المعلوماتية كالإقدام على تعذيب المتهم لحملهم على البوح بالأرقام السرية التي تمكنها من الولوج الى النظام المعلوماتي⁽²⁾، أو

(1) Cass Crim, 7 mars 1989, 87-90.500, Bull. Crim 1989 n° 109.

(2) و هذا الفعل مجرم و معاقب عليه بنص المادة 263 مكرر 2 من قانون العقوبات التي تقرّر " يعاقب بالسجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة من 150.000 دج إلى 800.000 دج، كل موظف يمارس أو يحرض أو يأمر بممارسة التعذيب من أجل الحصول على إقرارات أو معلومات أو لأي سبب آخر.

وتكون العقوبة السجن المؤبد، إذا سبق التعذيب أو صاحب أو تلى جنائية غير القتل العمد.

يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات و بغرامة من 100.000 دج إلى 500.000 دج، كل موظف موافق أو يسكت عن الأفعال المذكورة في المادة 263 مكرر من هذا القانون".

قد يتجرأ أحد أعضائها على تفتيش الأنثى بغير الإستعانة بأنثى⁽¹⁾، و غيرها من الأفعال الإجرامية التي يمكن أن تركت من قبل الموظف الذي يستغلّ وظيفته فينحرف عن أداء واجبه إلى المساس بالحريات الفردية دون مسوغ قانوني.

و لعلّ هذه النتيجة تثير لدينا تساؤلا هاما يكمن في البحث عن مدى تحقيق الجزاء الجنائي ردعا للقائم بالتفتيش عن تجاوز و مخالفة ما تفرضه الشرعية الإجرائية للأدلة المعلوماتية من ضمانات؟

أشارت الدراسات الجنائية في الولايات المتحدة الأمريكية إلى أنّه و على الرغم من وجود تشريع فيديريالي يعاقب على تجاوز السلطة نطاق إذن التفتيش أو تنفيذه بقسوة تزيد عما هو ضروري، و مع ذلك لا توجد في السجلات القضائية ما يدل على تطبيق ناجع لهذا الطريق، و لقد تعقبت الدراسات مدى تطبيق هذا التشريع على مدى أربعة و ثلاثين عاما فلم تجد ملاحقة واحدة تحت لوائه، في الوقت الذي كانت فيه المحاكم الفيدرالية الإستئنافية تصدر العديد أحكام إلغاء الإدانة في محاكم أول درجة لثبوت تحصيل الدليل من تفتيش أو ضبط غير قانوني⁽²⁾.

المطلب الثاني: المسؤولية المدنية

تختلف التشريعات في إطار تقرير المسؤولية الشخصية لمن باشر التفتيش المخالف للقانون، طريق المسؤولية المدنية لمن تمثل مخالفته خطأ مدنيا وفقا لقواعد خاصة تختلف من نظام إلى آخر ضيقا و اتساعا، و بحث موضوع المساءلة المدنية للقائم بالتفتيش الباطل يفرض علينا أن نتطرق إلى التشريعات المقارنة بداية بالتشريع الفرنسي بحكم أنّ التشريع

(¹) و هذا الجرم أيضا لم يعين فيه المشرع صفة الفاعل أي ينطبق على كلّ الأفراد و ممثلي السلطة العامة، حيث تنص المادة 335 من قانون العقوبات "يعاقب بالسجن المؤقت من خمس إلى عشر سنوات كل من ارتكاب فعلا مخلا بالحياة ضد إنسان ذكرا كان أو أنثى بغير عنف أو شرع في ذلك. و إذا وقعت الجريمة على قاصر لم يكمل السادسة عشرة يعاقب الجاني بالسجن المؤقت من عشر سنوات إلى عشرين سنة."

(2) F W Miller; R O Dawson; G E Dix; R I Parnas, Criminel Justice Administration Cases and Materials, Fourth Edition, the Université Casebook Series., United States of America, 1996, p 744.

مذكور لدى أحمد عوض بلال، المرجع السابق، ص 547.

الجزائري مستوحى منه (فرع أول) ثم نستعرض موقف المشرع الأمريكي الذي يعتبر أكثر التشريعات تجربة (فرع ثاني)، و نختم ذلك ببيان موقف المشرع الجزائري (فرع ثالث).

الفرع الأول: الوضع في التشريع الفرنسي

لقد كانت القاعدة السائدة في فرنسا حتى سنة 1972 هي إرتباط مسؤولية الدولة عن أعمال السلطة القضائية بإعادة النظر و نتيجة دعوى المخاصمة و الأضرار الناجمة عن الحبس المؤقت و أخطاء رجال الضبطية القضائية⁽¹⁾، غير أنه بمقتضى القانون الصادر في 5 جويلية 1972 المعدّل لقانون المرافعات المدنية الفرنسي قرر المشرع قاعدة جديدة بمقتضاها تسأل الدولة عن أعمال القضاء دون حاجة إلى إعادة النظر أو الى دعوى المخاصمة، و فرق في تنظيمه لهذه المسؤولية بين الخطأ الشخصي لرجال القضاء الذي يترتب عليه المسؤولية الشخصية لهم، و بين الخطأ المرفقي الذي تسأل عليه الدولة⁽²⁾.

و على ضوء ذلك قررت المادة 11 من ذلك القانون على أن تسأل الدولة عن تعويض الأضرار التي تنشأ عن الأخطاء التي يقع فيها مرفق القضاء، في حالة الخطأ الجسيم، و حالة إنكار العدالة، و يسأل القضاة عن أخطائهم الشخصية و في هذه الحالة تضمن الدولة

(1) كانت القاعدة العامة المقررة إلى وقت قريب في مختلف الأنظمة القانونية، هي عدم مسؤولية الدولة عن أخطاء القضاء بصفة عامة، إلا بصفة إستثنائية في الحالات التي قد ينص فيها المشرع على ذلك، و لكن نزولا على اعتبارات شتى فقد تغيرت تلك القاعدة كثيرا، و حلت محلها قاعدة مسؤولية الدولة عن تلك الأخطاء، و القول بتقرير المسؤولية المدنية للدولة الناجمة عن إهدار الشرعية الاجرائية للأدلة المعلوماتية المستمدة من التفتيش، تتنازعه ثلاثة اعتبارات رئيسية يتعين ضرورة العمل على التوفيق بينها، دون افتئات أو تقصير أو تغليب يؤدي إلى التضحية بأحدها لحساب الآخر، و تتمثل أول هذه الاعتبارات في ضرورة حماية الحرية الشخصية للأفراد و عدم المساس بها أو النيل منها إلا في حدود ما يرخص به القانون و في إطاره، أما ثاني الاعتبارات السلفة الذكر، فيكمن في ضرورة حماية موظف السلطة القضائية، أيا ما كانت وظيفته، حتى لا يكون مبدأ تقرير المسؤولية بمثابة سيف مسلط عليه، مما يحول دون أدائه لوظيفته، بسبب ترده و خوفه من الترددي في الخطأ الذي قد يؤدي إلى إمكان مساءلته، و الاعتبار الثالث و الأخير، يتمثل في ضرورة حماية نظام الدولة و عدم التفریط في أي عمل يؤدي إلى المساس به، أو يعرض سلامته و أمنه لأي خطر.

راجع تفصيلا: عادل عبد البديع ادم حسين، جزاء الإخلال بقاعدة مشروعية الدليل الجنائي، الطبعة الأولى، دار النهضة العربية، مصر، 2015، ص ص 247-248.

(2) أحمد ضياء الدين محمد خليل، المرجع السابق، ص 263.

حصول المضرور على تعويض عن الأضرار التي أصابته من هذه الأخطاء الشخصية على أن ترجع على من سبب الضرر ليتحمل العبء النهائي للتعويض⁽¹⁾.

ثم أقرّ قانون المرافعات الفرنسي رقم 75-1123 الصادر في 5 ديسمبر 1978 هذا الإتجاه و أورد نفس الحكم في المادة 505 منه، و أساس مسؤولية الدولة وفق ما قرره ذلك النص يكمن في نظرية الخطأ، حيث يتطلب المشرع فيه ضرورة توافر الخطأ المرفقي و حصره في الخطأ الجسيم و إنكار العدالة، و بالتالي لا تسأل الدولة عن الأضرار التي تترتب على تلك الأفعال القضائية ما لم يكن هناك خطأ من جانب المرفق، و الملاحظ أن القضاء الفرنسي قد ذهب في بعض أحكامه إلى تقرير مسؤولية الدولة عن أعمال الضبط القضائي ليس فقط على أساس الخطأ الجسيم بل أيضا على أساس الخطأ اليسير⁽²⁾.

أما بالنسبة للمسؤولية الشخصية للقضاة، فإنه بعد ذلك التعديل لم يعد المشرع يتطلب بشأنها اتباع قواعد المخاصمة التي كان ينص عليها قانون 7 فيفري 1933، إلا إن المادتين 11 و 505 المشار إليهما قد قررتا تأجيل تطبيق قواعد المسؤولية عن الخطأ الشخصي للقضاة إلى غاية صدور قانون تنظيم القضاء في 18 جانفي 1979، مضيفا في مادته الأولى إلى القانون الأساسي المتعلق بتنظيم القضاء الصادر في 22 سبتمبر 1958 المادة 1/11 و تنص على أن " قضاة المحاكم العادية لا يسألون إلا عن أخطائهم الشخصية و أنّ مسؤولية القضاة التي تترتب على الخطأ الشخصي المتصل بمرفق القضاء لا تقرّر إلا بدعوى ترفع ضد الدولة و هذه الدعوى تباشر أمام الدائرة المدنية بمحكمة النقض"⁽³⁾.

و نلاحظ أنّ نص المادة 11 السالف الذكر، و إن كان قد قرّر أنّ القضاة مسؤولون عن أخطائهم الشخصية إلا أنّه لم يحدّد هذه الأخطاء و ترك بذلك تحديدها إلى المعايير المختلفة بشأن تحديد الأخطاء الشخصية لأعمال الإدارة، و إذا رجعنا على معايير التفرقة بين الخطأ الشخصي و الخطأ المرفقي في نشاط رجال الإدارة نجد أنّ القضاء الفرنسي قد فرّق

(1) و بالرغم من ان نص المادة 11 من قانون 5 جويلية 1972 المعدل لقانون المرافعات المدنية الفرنسي قد استعمل اصطلاح القضاة إلا أنّ غالبية القضاء و الفقه الفرنسي قد اتجه إلى ضرورة تفسيره تفسيراً واسعاً بحيث يشمل أيضا رجال الضبطية القضائية، لمزيد من التفصيل راجع: أحمد ضياء الدين محمد خليل، المرجع السابق، ص 263.

(2) حسين فريجة، مسؤولية الدولة عن أعمال السلطة القضائية، رسالة دكتوراه، معهد الحقوق و العلوم الإدارية، جامعة الجزائر، الجزائر، 1990، ص ص 276-283.

(3) عادل عبد البديع اد م حسين، المرجع السابق، ص 279.

بين نوعين من التصرفات، تصرفات تتخذ خارج نطاق الوظيفة و أخرى تتم داخلها، و اعتبر الخطأ الشخصي متوافرا في كل مرة يقع خطأ الموظف خارج نطاق الوظيفة و يتطلب لكي ترتب الأخطاء التي يرتكبها الموظف داخل وظيفته مسؤوليته الشخصية ان تتسم بطابع من الجسامة تغدو معه و كأنها منفصلة عن المرفق و يكون ذلك إما لأن خطأ الموظف عمدي و إما لأنه قد بلغ حدا كبيرا من الجسامة⁽¹⁾.

و تطلب توافر الخطأ الجسيم من المشرع الفرنسي لقيام مسؤولية الدولة عن أعمال القضاء يتفق مع قضاء مجلس الدولة الفرنسي في تقدير جسامة الخطأ المؤدي إلى مسؤولية الإدارة، فمجلس الدولة الفرنسي يكتفي بالخطأ اليسير إذا كانت الخدمة التي يقوم عليها المرفق سهلة الأداء لا صعوبة فيها، بينما يتطلب الخطأ الجسيم إذا كانت الخدمة تكتنفها صعوبات تعرض المرفق لإرتكاب أخطاء⁽²⁾، و يترتب على الحكم الصادر بتقرير المسؤولية الشخصية للقاضي أن تقوم الدولة بدفع التعويض للمضرور و لها أن ترجع على القاضي المخطئ لمطالبته بردّ المبلغ الذي دفعته بسبب خطئه الشخصي، فمسؤولية الدولة عن الخطأ الشخصي للقاضي ليست سوى مسؤولية مؤقتة تعمل في مواجهة المضرور فقط دون القاضي المخطئ الذي تبقى مسؤوليه قائمة تجاه الدولة.

الفرع الثاني: الوضع في التشريع الأمريكي

سبق أن أوضحنا أن التعديل الدستوري الأمريكي الرابع ينص على ضرورة حماية حقوق الافراد سواء في أشخاصهم أو في مساكنهم أو في مستنداتهم و أوراقهم و في كافة ممتلكاتهم، و من ثم ضرورة أن يكونوا في مأمن من أي تفتيش أو قبض غير معقول، و بالتالي عدم قبول المحاكم الفيدرالية لأي دليل ناجم أو مكتشف بالمخالفة للحقوق، و ما نصّ عليه التعديل الرابع عشر على حظر قبول تلك الأدلة أمام محاكم الولايات⁽³⁾.

رغم أن تلك التعديلات لم تنص على المسؤولية المدنية الناجمة عن إهدار الشرعية الإجرائية لهذه الأدلة الجنائية، إلا أن ذلك لم يكن مانعا يحول دون قبول القضاء لطلبات

(1) المرجع نفسه، نفس الموضوع.

(2) حسين فريجة، المرجع السابق، ص 289.

(3) أحمد ضياء الدين محمد خليل، المرجع السابق، ص 950.

الأفراد الرامية إلى تعويضهم عن الأضرار اللاحقة بهم جزاء تعريضهم لتفتيش غير قانوني، و لكن من التادر قبول تلك الدعاوى التي ترفع ضد الهيئات الحكومية.

واقع الأمر أنه حتى في الوضع الأمريكي فإن ثمة اتجاه قوي يبرز عدم فعالية التعويض المدني في ردع تجاوزات القائم بالتفتيش، و تأتي المحكمة الفيدرالية العليا و المحكمة العليا في ولاية كاليفورنيا على رأس هذا الإتجاه، و يدعم أنصاره موقفهم بكون أن التجربة تثبت صعوبة تنفيذ هذا الحل و عدم جدواه، لأن دفع الضابط بحسن نيته في مباشرة الإجراء يقبل في مثل تلك الدعاوى حتى و لو كان نشاطا منطويا على مخالفة دستورية، و من ناحية ثانية يتردد الأفراد العاديون في رفع الدعاوى المدنية ضد الضابط المخالف الذي قلما يكون مليئا بالقدر الكافي لدفع التعويض، فضلا عن طول أمد تلك الدعوى و إرتفاع تكلفتها و صعوبة اثبات الخطأ، و هكذا لن يلعب الجزاء المدني أي دور يذكر في ردع الضابط على إرتكاب المخالفات⁽¹⁾.

الفرع الثالث: الوضع في التشريع الجزائري

كانت المسؤولية الشخصية للقضاة تقوم في الجزائر طبقا لقواعد دعوى المخاصمة⁽²⁾، و في ما يتعلّق بسير إجراءات هذه الدعوى فقد كانت معقدة و صعبة و تنحصر أسبابها حسب

(1) و قد لوحظ في القضايا المدنية أن الجوانب الأخلاقية للقضايا ليست في صالح المدعين حتى أن فرصة النجاح في الدعوى لا تتاح الا للمدعين ذوي السمعة ناصعة البياض و الذين يتمتعون بوضع اجتماعي مرموق أما السمعة غير الطيبة للمدعين لا سيما عند أصحاب السوابق منهم فسيب يقلل من فرص نجاح طلباتهم لأنها تمثل عاملا يؤخذ في الاعتبار لتخفيض مبلغ التعويض أو لإطعاف الثقة، كما لوحظ أن معظم تجاوزات الشرطة تقع ضد الطبقات الدنيا في المجتمع و أن الشرطة تدرك ان هؤلاء يعيشون في مناطق يرتفع فيها معدل الجريمة و يفقدون للسعة الطيبة و بالتالي تدرك أن ما قد يرفعونه من دعاوى تعويض ضدهم مصيرها الفشل حتى إن المحامين أنفسهم قلما يقبلون تمثيل موكلهم في مثل هذا النوع من الدعاوى. لمزيد من التفصيل حول موضوع عدم فاعلية الجزاء المدني في الحفاظ على الشرعية الإجرائية للأدلة الجنائية في التشريع الأمريكي راجع : أحمد عوض بلال، المرجع السابق، ص 524.

(2) تنص المادة 2014 من الأمر رقم 66-154 المؤرخ في 8 جوان 1966 والمتضمن قانون الإجراءات المدنية (الجريدة الرسمية عدد 48 الصادرة بتاريخ 9 جوان 1966) تجوز مخاصمة القضاة من غير أعضاء المحكمة العليا في الأحوال الآتية :

(1) - إذا وقع من أحدهم تدليس أو غش أو غدر أثناء سير الدعوى أو عند صدور الحكم .

(2) - إذا كانت المخاصمة منصوبا عليها صراحة في نص تشريعي .

ما ورد في المادة 214 من قانون الإجراءات المدنية القديم في الغش و التدليس و الغدر، و كانت المخاصمة منصوص عليها بنص صريح⁽¹⁾، غير أن المشرع الجزائري لم يقرّر مسؤولية الدولة عن هذه الأخطاء، إذ يقدم طلب المخاصمة إلى أمانة ضبط الغرفة المدنية بالمحكمة العليا، و فسرت النصوص التي تحكم هذه الدعوى تفسيراً ضيقاً، فالمسؤولية المدنية التي كانت سائدة بهذه الطريقة كانت في الواقع تؤدّي إلى شبه عدم مسؤولية القضاة أثناء مباشرتهم لمهامهم⁽²⁾.

و لهذه الأسباب نجد أنّ القضاء الجزائري لم يصدر أي حكم يتعلق بقبول دعوى مخاصمة القضاة عن أخطائهم الشخصية إلى غاية إلغاء هذه القاعدة بموجب قانون رقم 08-09 المؤرخ في 25 فيفيري سنة 2008، يتضمن قانون الإجراءات المدنية والإدارية⁽³⁾، على الرغم من أنّ مسؤولية الدولة عن الأخطاء القضائية مقرّرة بقاعدة دستورية نصت عليها جميع الدساتير⁽⁴⁾، و ذلك تماشياً مع المادة 31 من القانون الأساسي للقضاة التي نصت " لا يكون

(3) - في الأحوال التي يقضي فيها القانون بمسؤولية القاضي والحكم عليه بالتعويضات .

(4) - إذا امتنع القاضي عن الحكم .

(1) هذا الوضع التشريعي كان مستوحى من قواعد مخاصمة القضاة التي تبناها المشرع الفرنسي قبل تعديله سنة 1933، و من بين التشريعات التي لا تزال الى غاية اليوم تعتمد هذا النهج التشريع المصري، حيث تقرّر المادة 494 من قانون رقم 13 لسنة 1968 الصادر بتاريخ 9 ماي 1968 بشأن إصدار قانون المرافعات المدنية والتجارية: " تجوز مخاصمة القضاة وأعضاء النيابة في الأحوال الآتية (1): إذا وقع من القاضي أو عضو النيابة في عملهما غش أو تدليس أو غدر أو خطأ مهني جسيم (2). إذا امتنع القاضي من الإجابة على عريضة قدمت له أو من الفصل في قضية صالحة للحكم وذلك بعد إعداره مرتين على يد محضر يتخللها ميعاد أربع وعشرين ساعة بالنسبة إلى الأوامر على العرائض وثلاثة أيام بالنسبة إلى الأحكام في الدعاوى الجزئية والمستعجلة والتجارية وثمانية أيام في الدعاوى الأخرى. ولا يجوز رفع دعوى المخاصمة في هذه الحالة قبل مضي ثمانية أيام على آخر إعدار (3). في الأحوال الأخرى التي يقضي فيها القانون بمسؤولية القاضي والحكم عليه بالتعويضات."

(2) حسين فريجة، المرجع السابق، ص 297.

(3) صحبي محمد أمين، مسؤولية الدولة عن الأخطاء القضائية و التعويض عنها في التشريع الجزائري، مجلة آفاق فكرية، كلية العلوم الإنسانية و الاجتماعية، جامعة سيدي بلعباس، الجزائر، العدد 6، 2017، ص 308.

(4) تنص المادة 61 من الدستور الحالي "يترتب على الخطأ القضائي تعويض من الدولة. و يحدّد القانون شروط التعويض وكيفية". و هي نفس القاعدة التي تضمنها دستور 1976 و دستور 1989 بموجب المادة 46 منهما بحيث لم يطرأ أي تعديل على حكم المادة أو صياغتها.

القاضي مسؤولاً إلا عن خطئه الشخصي و لا يتحمل القاضي مسؤولية خطئه الشخصي المرتبط بالمهنة إلا عن طريق دعوى الرجوع التي تمارس ضد الدولة⁽¹⁾.

حقيقة الأمر أنّ المشرع الجزائري لم يصدر أي قانون يحدّد كيفية التعويض باستثناء القانون رقم 08-01 المؤرخ 26 يونيو سنة 2001 المعدل و المتمم، و ذلك بموجب المادة 531 مكرّر من قانون الإجراءات الجزائية التي تمنح المحكوم عليه المصرّح ببرائته تعويضا عن الضرر المادي و المعنوي الذي تسبّب فيه حكم الإدانة، أو التعويض عن الحبس المؤقت التعسفي طبقا المادة 137 مكرر من قانون الإجراءات الجزائية، و التي تقرر " يمكن أن يمنح تعويض للشخص الذي كان محل حبس مؤقت غير مبرّر خلال متابعة جزائية إنتهت في حقّه بصدور قرار نهائي قضى بأن لا وجه للمتابعة أو بالبراءة إذا ألحق به هذا الحبس ضررا ثابتا و متميزا، و يكون التعويض الممنوح طبقا للفقرة السابقة على عاتق الدولة مع احتفاظ هذه الأخيرة بحق الرجوع على الشخص المبلغ سيء النية أو شاهد الزور الذي تسبّب في الحبس المؤقت".

و المتأمل في هذه النصوص القانونية يجد أنّ المشرع أرسى قاعدة عامة و هي عدم مسؤولية الدولة عن أخطاء السلطة القضائية إلا ما ينقرّر منها إستثناء بنص تشريعي، و هو ما لا نجد له سوى تطبيقا واحدا يتمثّل في الحبس التعسفي، فلم ينص على مسؤولية الدولة مدنيا عما ثبت من مخالفة أو إهدار لقاعدة الشرعية الإجرائية للأدلة الجنائية، و من ثمّ فإنّ مخالفة القواعد الشكلية أو الموضوعية للتفتيش عن الأدلة المعلوماتية لا يقيم مسؤولية الدولة في التعويض عن الخطأ القضائي.

و هو موقف يطرح تساؤلا حول النطاق الحقيقي لمضمون نص الدستور، فيما إذا كان الخطأ القضائي الموجب للتعويض يقتصر فقط على الحبس التعسفي أم أنّ مسؤولية الدولة تمتد لتشمل كلّ ضرر يلحق الأفراد نتيجة إهدار الشرعية الإجرائية بموجب أي إجراء صادر عن السلطة القضائية؟

إنّ النطاق الموضوعي لمسؤولية الدولة يجب أن يمتد ليشمل كافّة ما يتسبّب فيه أعضاء السلطة القضائية من أضرار تنجم عن مخالفة قاعدة الشرعية الإجرائية، غاية ما هناك أنّه يتعيّن ضرورة التمييز بين تلك الأعمال التي تدخل في نطاق الخطأ المرفقي و تلك

(1) القانون العضوي رقم 11/04 المؤرخ في 06/09/2004 و المتضمن القانون الاساسي للقضاء، المنشور بالجريدة الرسمية عدد 57 و المؤرخة في 08 سبتمبر 2004.

التي تعدّ من قبيل الخطأ الشّخصي، و من ثمّ ترتيب مسؤوليّة الدولة بصفة أصلية عن النّوع الأوّل منه دون إمكان ذلك بالنّسبة للنّوع الثّاني، و بعبارة أخرى تقرير مسؤوليتها عمّا يدخل في نطاق النّوع الأوّل دون رجوع منها على العضو القضائي الذي يحتمل تسببه في إحداث تلك الأضرار بينما يعترف لها بحقّها في الرجوع عليه إذا ما ارتفع قدر المخالفة إلى مستوى الخطأ الشّخصي⁽¹⁾، الذي لا علاقة له بالمرفق بل يرتبط بجانب مادي أو نفسي خاص بمرتكب الخطأ، أمّا بالنّسبة للأخطاء المرتكبة من قبل الضبطية القضائية فتخضع للقواعد العامة (124 من القانون المدني) و لا تقيدها أحكام خاصّة.

و نختم هذه الجزئية بمسألة غاية في الأهمية مفادها أنّ انتهاك حق الخصوصية المعلوماتية عن طريق إهدار الشّرعية الإجرائية يتسبب عادة في ضرر معنوي يتعدّر معه عملية تحديد مقدار التعويض المتوجب للمتهم (المدعي)، خاصّة في الأحوال التي يتجاوز فيها أثر الضّرر شخص صاحب الشّأن إلى أفراد أسرته، ممّا يجعل أي تعويض قد يقرره القضاء غير كاف لجبر ما أسفر عنه التفتيش المخالف للقانون، يتعيّن معه البّحث عن جزاء آخر يكون أكثر ردعا منعا من الإقدام على هذه التّجاوزات في المستقبل.

المطلب الثالث: الجزاء التأديبي

قد تكون المخالفة الإجرائية التي تمّ تحصيل الدليل على إثرها خطأ تأديبيا يؤاخذ عليه الموظف العام الذي باشر الإجراء بالمخالفة للقواعد التي تتحدّد إطار عمله، و حينئذ لا تعارض بين تقرير هذا النّوع من المسؤولية التأديبية للموظف العام من ناحية، و تقرير أنواع أخرى من المسؤولية، كالمسؤولية المدنية و المسؤولية الجزائية أو تقرير استبعاد الدليل⁽²⁾. إنّ الموظف العمومي الذي يجري تفتشا لأنظمة المعلوماتية بشكل تعسفي أو غير صحيح يكون مسؤولا عن عمله مسؤولية إدارية أمام رؤسائه الذين لهم الحق في فرض جزاءات إدارية عليه طبقا لما تخوله لهم القوانين و اللوائح من اشراف و توجيه لمرؤوسيه، و

(1) أحمد ضياء الدين محمد خليل، المرجع السابق، ص 972.

(2) أحمد عوض بلال، المرجع السابق، ص 526.

تتدرج هذه الجزاءات الإدارية من مجرد "اللوم" أو "لفت النّظ" أو "الإنذار" إلى العزل الذي يتضمن الحرمان من الوظيفة و مزاياها⁽¹⁾.

و يلاحظ أنّ الجزاءات الإدارية لها أهمية كبرى فيما يتعلّق بمأموري الضبط القضائي أما فيما يخص القضاة فإنهم يتمتّعون في عملهم باستقلال كبير يجعل سلطة الرؤساء عليهم لأقل تأثيراً من الرقابة الرئاسية على الضبطية القضائية⁽²⁾.

و رغم المزايا التي تبدو جليّة في طريق المساءلة التأديبية للقائم بالتفتيش غير المشروع عن الأدلة المعلوماتية، إلا أنّ التجربة المقارنة تثبت كذلك عدة مثالب مقابلة مرتبطة به، إذ تشير التجربة في الولايات المتحدة الأمريكية إلى إنعدام فعالية المساءلة التأديبية للضابط المخالف، فذلك المساءلة لا تطبق إلا فيما ندر، و قلّمَا يسمع عن ضابط أوقف عن العمل أو خفضت درجته الوظيفية أو عوقب بأي طريقة تأديبية أخرى لأنّه أقدم على تفتيش دون مسوغ قانوني، و هو السبب المحتمل في وقوع الجريمة و تورط المشتبه به في ارتكابها⁽³⁾.

صفوة القول، أنّه لا يوجد أي بديل آخر يحل محل قاعدة إستبعاد الأدلة المعلوماتية المتحصلة عن طريق تفتيش غير مشروع (البطلان)، غير أنّ الجزاءات الأخرى الموقعة على مرتكب الإجراء المخالف للقانون قد تتفاوت أهميتها من جزاء إلى آخر إلا أنّها تظل تحقق نوعاً من الردع من ارتكاب هذه التجاوزات مستقبلاً، فالطابع الشخصي لهذه الجزاءات الفردية تدفع القائم بالإجراء إلى الإلتزام بالمشروعية الإجرائية في أبعاد مدى لها حال التفتيش عن الأدلة المعلوماتية.

(1) تم تحديد مفهوم الخطأ التأديبي للقضاة و صوره و أنواع الجزاءات الموقعة على مرتكبه بموجب المواد 60-61 من القانون الأساسي للقضاة، و في مواجهة الضبطة القضائية يلاحظ أنّ قانون الإجراءات الجزائية (المادة 206 و ما بعدها) استحدث رقابة فعالة تمارسها غرفة الإتهام على تصرفات عضو الضبطية القضائية لاسيما في تحصيلهم للأدلة الجنائية بطرق غير مشروعة.

(2) توفيق محمد الشاوي، المرجع السابق، ص 511.

(3) في بعض المدن الكبرى الأمريكية قد تصدر مباحث الآداب العامة خمسة آلاف أمر بالتفتيش في السنة و يتبين بعد ذلك عدم إستنادها إلى سبب محتمل و من ثم تطرح جانبا دون أن يسأل أي أفرادها تأديبياً، كما أنّه من غير المرجح أن تعمل المسؤولية التأديبية كرادع إلا في أضيق نطاق ممكن، نظراً لأنّ الشرطة تقع تحت ضغط هائل للتوصل الى نتائج سريعة و ملموسة بينما تقع غالبية التجاوزات أثناء ممارسة الشرطة نشاطها المعتاد.

لمزيد من التفصيل حول مبررات عدم فعالية الجزاءات التأديبية في ردع تجاوزات الضبطية القضائية إزاء التفتيش غير المشروع راجع: أحمد عوض بلال، المرجع السابق، ص ص 531-532.

خلاصة الباب الثاني

بطبيعة الحال فمرحلة التفتيش عن الأدلة المعلوماتية ليست سوى أحد طرفي المعادلة، ففي مرحلة عرض الدليل على المحكمة لتقول كلمتها فيه، تثار تساؤلات أخرى، و ما من شك أنّ أول سؤال يتبادر إلى ذهن المحكمة يتعلّق بأصالة هذا الدليل، و قيمته الإقناعية سيما و أنّ المشرع أعتمد منطق اصالة الدليل المعلوماتي رغم أنّ الدليل المطروح على القضاء ليس سوى نسخة مستمدة من البيئة الرقمية عن طريق النسخ.

من هذا المنطلق عالجنا من خلال الفصل الأول حرية القاضي الجنائي في الإثبات بالدليل المعلوماتي المستمد من التفتيش و حدودها من خلال التطرق إلى قيد المشروعية و النزاهة، في ضوء التعقيد التقني الذي تتميز به هذه الادلة، كل ذلك من خلال المبحث الأول و أيضا عالجنا حدود سلطة الاقضي الجنائي في تقدير قيمة هذا الدليل بتناول مبدأ حرية القاضي في الاقتناع و اثر القيمة العلمية لهذا الدليل على اقتناعه الشخصي من خلال المبحث الثاني.

و لأنّ قاعدة مشروعية الدليل المعلوماتي المستمد من التفتيش تفقد قيمتها إذا لم تكن هناك رقابة فعالة على السلطة التي تباشر التفتيش، و لا معنى لهذه الرقابة إذا لم يكن هناك جزاء يتقرّر جزاء مخالفة كلّ ما تفرضه قواعد القانون من ضوابط و شروط، فقد تطرقنا من خلال الفصل الثاني إلى أثر التفتيش المعلوماتي غير المشروع، بتحديد الجزاء الإجرائي المترتب حال اتخاذ اجراءات التفتيش بالمخالفة للقانون من خلال المبحث الأول، و أيضا بتحديد باقي الجزاءات سواء الجزاءات التأديبية أو المدنية أو حتى المتابعة الجزائية التي يمكن أن توقع على من أمر بالتفتيش أو بتنفيذه، و بيان مدى قيام مسؤولية الدولة بهذا الشأن، كل ذلك من خلال المبحث الثاني.

خاتمة

بعد أن فرغنا من العرض التفصيلي لجميع المسائل التي تعرضت لها الدراسة، و التي تمت من خلالها الإجابة على الإشكالية الرئيسية و التي مبنها إلى أي مدى تشكل ضوابط الشرعية الإجرائية قيذا على مبدأ حرية الإثبات الجنائي في قبول الأدلة المعلوماتية المستمدة من التفتيش في بناء حكم الإدانة أو تعزيز قرينة البراءة؟ و الإجابة أيضا على جميع التساؤلات الفرعية و الي توصلنا من خلالها إلى أنه لا يوجد تفاعل بين إجراءات التفتيش التقليدية مع البيئة الرقمية.

و انطلاقا من طبيعة هذا الدليل التي جعلته يتميز بذاتية فريدة عن غيره من الأدلة التقليدية، فقد حاولنا لقاء الضوء على هذه الذاتية من مختلف جوانبها مع بيان اثرها على طبيعة إجراءات استخلاصه، التي اقتضت فعاليتها تقييد بعض الحقوق و الحريات في اطار استرجاع البيانات كقيمة اثباتية، مع الأخذ بعين بعين الإعتبار قيمة بعض الضوابط التي من شأنها أن تحقق التوازن النسبي بين حق المجتمع في مواجهة الجريمة و حق الفرد في التمتع بحقوقه.

غير أنه لا يمكن اعتماد مبدأ الشرعية في شكل جامد حال التفتيش عن الأدلة المعلوماتية، بل ينبغي التقليل من جموده نظرا لما تتطلبه عناصر الفعالية، لذا نجد تساهلا في هذا المنحى من طرف التشريعات، فالقدرات التخزينية في البيئة الرقمية و هي تستوعب هذا العدد الهائل من البيانات لم تتفاعل كليا مع القواعد الإجرائية حيث لم يتم التوصل إلى إمكانية قيام عملية فرز ذاتية داخلية للملفات و استرداد البيانات المجرمة دون استعراض البيانات التي لا علاقة لها بالواقعة الجرمية نتيجة استغلال المجرمين لهذه السعة التخزينية بجعل الأدلة مخفية أو مضغوطة أو مفخخة أو تحمل عناوين مضللة أو مشفرة أو مدفونة ضمن مساحة التخزين الفارغة بطرق تجعل من المستحيل اكتشافها دون استعراض عدد كبير من الملفات، فالوصول إلى البيانات المستهدفة وسط هذا الكم من البيانات يفرض حتما توسيع نطاق التفتيش بامتداده عبر كافة البيانات، و هو ما يتجاوز الغاية من التفتيش كأهم ضمان تقوم عليه نظرية التفتيش الجنائي في حماية الحريات الفردية لذا تقتضى الامر البحث عن ضمانات رقمية جديدة و من بينها الحق في الحذف.

و من الطبيعي أن تلقي تلك الطبيعة التقنية المعقدة لهذا النوع المستحدث من الأدلة بظلالها ليس فقط على مرحلة التفتيش عنه، بل أيضا على مرحلة عرضه على المحكمة لتقول كلمتها فيه من حيث سلطة القاضي في قبول هذا الدليل، من حيث مدى مشروعيته و نزاهته، و أيضا من حيث اعمال سلطته في تقدير حجية هذا الدليل و قيمته الاقناعية، كل ذلك ضوء ظروف و ملابسات الدعوى.

نختتم هذه الدراسة بخاتمة تشمل فقط أهم النتائج التي خلصنا إليها من خلال بحثنا، فضلا عن النتائج التي جاءت في مواضعها المختلفة ضمن هذا البحث:

1. الأدلة المعلوماتية المستمدة من التفتيش نوع متميز عن الأدلة المعروفة في فكر الإثبات التقليدي، فهي ليست من قبيل الأدلة المادية لإنعدام الأثر الفيزيائي لها و ليست من الأدلة القولية التي يكون مصدرها الأشخاص، بل هي مكون رقمي ثنائي في شكل نبضات مغناطيسية غير مرئية تتواجد في بيئة رقمية تتعدم فيها الأبعاد المادية ما يؤهلها بحكم ذاتيتها لتشكل إضافة جديدة لنظرية الإثبات الجنائي.

2. رغم أن أمن الفرد في نظامه المعلوماتي يعد أقوى مظاهر الحماية الاجتماعية التي يجب أن تكفل له بإعتباره المستودع الطبيعي الذي يغلب أن يحفظ الإنسان فيه أسرارها، إلا أن المشرع العادي لا يزال يقيم أشكال التمييز بين حرمة المسكن و حرمة النظام المعلوماتي، مع خضوع الحرمة الأولى لضمانات أقوى، بيد أن حرمة المسكن في الحقيقة ليست سوى وجها من أوجه حماية حرمة الأشخاص، و حماية المعلومات ليست سوى مظهرا عاما لحماية هذا الحق في صورته الرقمية، و قد حاول المشرع الدستوري إستدراك هذا القصور عن طريق فرض الإشراف القضائي على التفتيش المعلوماتي، إلا أن الرقابة القضائية على التفتيش دون تقييده بضوابط تراعي حقوق الأفراد في البيئة الرقمية يفقده الأهمية المتوخاة منه.

3. يعتبر الضبط العرضي الشامل لبيانات المتهم في مرحلة التفتيش المادي ضرورة حتمية بحكم العدد الهائل من البيانات المخزنة ضمن وسائط التخزين الرقمية التي تظم عالما من المعلومات تختلط فيه البيانات المتسهدفة مع البيانات الخارجة عن نطق الإذن القضائي التي تعد موضوعا للدليل الجنائي، لذا يستحيل وقت الضبط

الأولي تحديّد البيانات المستهدفة بالتفتيش و فصلها عن غيرها من البيانات لأتّها عملية تستغرق وقتاً طويلاً و البديل العملي الوحيد هو ضبط معظم أو حتّى جميع دعامات التخزين الرّقميّة و تفتيشها لاحقاً خارج الموقع، فالضبط العرضي الشّامل يعتبر جزء متأصل من عملية التفتيش عن الأدلّة المعلوماتيّة.

4. في سياق التفتيش عن الدليل المعلوماتي يتكامل السؤال "المتعلق بكيفية التفتيش" مع "ما سيجري التفتيش عنه"، لأنّ المفهوم المادّي للحدود يصبح مجازياً، و من ثمّ فإنّ استراتيجية التفتيش هي الوسيلة الوحيدة لوصف موقع البيانات و الملفات الرّقميّة التي سيتم تفتيشها، ذلك أنّ الوصول إلى الأدلّة المعلوماتيّة يتمّ من خلال الأوامر الموجهة لأجهزة الحاسوب، فعند محاولة وصف البيانات التي يجب ضبطها، لن تكون هناك طريقة لتحديد مساحات معيّنة عن طريق وصف الإحداثيات المادّيّة الخاصّة بها و لكن عن طريق وصف كيفية تحديد موقعها نتيجة لذلك، فإنّ الطريقة الوحيدة لتحديد منطقة معيّنة من مساحة التخزين الرّقمية هي تحديد كيفية التفتيش.

5. حاول المشرّع الجزائري تنظيم أحكام التفتيش عن الدليل المعلوماتي بمقتضى القانون 04/09 المتعلّق بالوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها بالمحافظة على مبدأ عتيد يقوم على خطوة واحدة يعرف بـ "آلية التفتيش ثم الإستراداد"، على خلاف الواقع الذي فرضته ظاهرة اختلاط البيانات و تعذر فرزها في موقع التفتيش المادّي و التي توجب اعتماد آلية "الاسترجاع ثم التفتيش"، فعدم وجود أيّ قيود على مرحلة التفتيش المادّي من شأنه تجريد حماية الدستور للخصوصية المعلوماتية من أي قيمة.

6. أبانت لنا الدراسة في مواضع كثيرة قدرنا متيقنا من الخلل و التّعقيدات التي تهدر تماماً ما يحرص عليه النّظام القانوني من محافظة على الحرّيات الفردية نتيجة إهمال المشرّع لكثير من الضمانات التي يجب أن تقيد عملية التفتيش عن الأدلّة المعلوماتية منها ما هو موضوعي كإعتماد المنظور المادي لمحل التفتيش بدل قصره على بعض الملفات فقط، و ترك تقدير أسلوب تنفيذه للقائم به بدل فرض استراتيجية تحول استعراض البيانات الخارجة عن نطاق الإذن القضائي، و منها ما

هو شكلي كعدم تحديد مدة سريان الإذن بالتفتيش خلال مرحلة التفتيش المادي و ترك المتهم مهددا بالتفتيش إلى أجل غير مسمى، و إجازة امتداد التفتيش إلى أي نظام معلوماتي مرتبط به دون إشراف قضائي، ما جعل النصوص الدستورية مجرد كلمات شكلية.

7. إن التسامح الملحوظ من طرف المشرع الجزائري بخصوص الإستثناءات التي أوردها على قاعدة حظر التفتيش المعلوماتي لاكتشاف الجرائم و منع وقوعها، يعد مساسا خطيرا بضمانات دستورية و يتنافى بشكل صارخ مع مبدأ افتراض البراءة، لأن الغاية من التفتيش قضائية، فصيانة الأمن بمنع وقوع الجريمة غاية جلية، لكنها ليست غرضا قضائيا لذلك مهما يكن من نبل هذا الهدف، فإنه لا يجوز اجراء التفتيش لتحقيقه خاصة و أنه فشل في تعداد الحالات التي يجوز فيها اتخاذ هذا الإجراء، و من هنا أضحي التوسع في هذا الاجراء الاستثنائي هو القاعدة و انقلبت العلاقة بين الحرية الفردية كحق و التفتيش كقيّد.

8. تحقيقا لفعالية التفتيش في الوصول إلى الدليل المعلوماتي قبل حذفه من قبل الجناة، سنّ المشرع قاعدة الاحتفاظ الشامل بالبيانات كإلتزام ملقى على عاتق مزودي الخدمات لمدة سنة كاملة تسري من تاريخ تسجيلها، و هو ما يناقض حق الفرد في الدّخول في طبي النسيان و يخالف مبدأ التناسب و الضرورة لكونه لا يستهدف فئة معينة من الأفراد قامت حولهم الشبهات في ارتكاب أفعال إجرامية بل لا يستثني حتى فئة البيانات التي تتمتع بالسريّة المهنية، و هو نهج محل نقد كبير من طرف منظمات حقوق الإنسان.

9. جاء حظر التفتيش المعلوماتي العابر للحدود بنص عام ، إذا لم يتم الحصول على إذن من الدولة التي يوجد النظام المعلوماتي المستهدف بالتفتيش على أراضيها، على الرغم من أنّ اتفاقية بودابست و حتى الإتفاقية العربية لمكافحة جرائم تقنية المعلومات - التي صادقت عليه الجزائر - قد نصتا على استثنائيين، بحيث يمكن الوصول إلى أية بيانات مخزّنة في نظام معلوماتي، و ضبطها، أيّا كان مكان وجودها داخل أو خارج الدولة، إذا كانت موضوعة تحت تصرف الجمهور أو في

حال موافقة الشّخص المخوّل قانوناً بإفشاء هذه البيانات.

10. يعد مبدأ حرية الإثبات الجنائي ركيزة أساسية تقوم عليها نظرية الإثبات بمقتضاه يتقرّر للقاضي سلطة قبول الدليل المعلوماتي المستمد من التفتيش لبناء هيكله الإدانة، غير أنّ هذه السلطة مقيدة بمبدأ الشرعية في معناه الواسع ، فقيمة هذا المبدأ ليست كما يدركها العقل بقدر ما تتعلق بصون الحريات الفردية كما يدركها الضمير، فالقضاء الذي يبيح الإستناد إلى أدلة غير مشروعة لبناء الإدانة و يرضى عن مخالفة الشرعية الاجرائية بذريعة حماية المجتمع من مخالفتي القانون هو في الحقيقة يشجع لأن يصبح الكلّ مخالفاً للقانون.

11. السلطة التقديرية للقاضي الجنائي لا تتناول القيمة العلمية للدليل المعلوماتي المستمد من التفتيش، لأنها قائمة على أسس و أصول علمية تتميز بالثبات و الثقة في مصادرها، بخلاف الظروف و الملابسات التي وجد فيها هذا الدليل فإنّها تدخل بطبيعتها في نطاق تقديره الذاتي، فله أن يطرحها على الرغم من قطعيتها إذا تبين له أنّها لا تتفق من ظروف الواقعة و ملابساتها.

12. الأصل أنّ التحقق من أصالة الدليل المعلوماتي المستمد من التفتيش يعادل عبء تقديم الدليل، إلا أنّ تطبيق هذه القاعدة بشكل جامد يؤدي الى التخلي عن هذا الدليل بحكم ما تستنفذه الخبرات التقنية من جهد و وقت و مال يثقل كاهل الهيئة الاجتماعية بمعزل عن تلك التي استنفذها في مرحلة التفتيش، لذا سلك القضاء المقارن مسلك افتراض الموثوقية في الدليل المعلوماتي و يقع على من يدعي خلاف ذلك إثبات العكس، و في حالة الشك المعقول يعتبر الدليل المعلوماتي مجرد قرينة تحتاج إلى دليل يعزز مصادقيتها للإعتماد عليها في بناء حكم الإدانة، بالإستناد على شهادة الشهود، أو تصريحات الضحية إذا لم ينكرها المتهم، أو شواهد أخرى تؤكد قيام العلاقة بين الدليل المطعون في صحته و بين الوقائع المراد إثباتها دون إشتراط إجراء خبرة تقنية.

13. تبقى الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش مجرد فلسفة سائدة ليس إلا، ما لم تكن هناك رقابة قضائية على السلطة التي تباشر التفتيش، و لا

قيمة لهذه الرقابة ما لم يكن هناك جزء إجرائي يترتب جزء مخالفة ما تفرضه هذه القاعدة من ضوابط، بتقرير بطلان هذا الإجراء و إهدار الدليل المعلوماتي المستمد منه، و لا يمكن للجزاءات الفردية الموقعة على مرتكب التفتيش غير المشروع أن تحل محل هذه القاعدة في تحقيق الردع و حماية الحريات الفردية، لأن التجربة كشفت أنّ هذه الجزاءات لم تفلح في الحيلولة دون ارتكاب التفتيش الباطل.

14. على الرغم من أنّ الدستور قرّر مسؤولية الدولة عن الأخطاء القضائية بنص عام، إلا أنّ المشرع العادي قصر نطاق هذه المسؤولية عن أخطاء القضاء في حالة واحدة تتعلق بالضرر الذي مني به الفرد جزاء الحبس التعسفي، و أنكر مسؤوليتها عن كافة الأخطاء الأخرى الناجمة عن إهدار الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش، في وقت يكشف فيه الواقع العملي أنّ حجم الضرر الذي قد يلحق الأفراد جزاء مخالفة هذه القاعدة لا يقلّ عن الضرر يلحقهم جزاء الحبس التعسفي.

في ضوء ما توصلت إليه الدراسة من نتائج تم التوصل إلى الإقتراحات الآتية:

1. ضرورة تدخل المشرع لتحديد ماهية الجرائم ذات الجسامة الخاصة و التي ينطبق عليها الاستثناء المتعلق بجواز التفتيش المعلوماتي في سياق التحوط من الجرائم المستقبلية و منع وقوعها، مع تجنب استعمال عبارات فضفاضة تمنح للسلطات الإجرائية سلطة تقديرية واسعة في تفسيرها للقانون.

2. نهييب بالمشرع أن يبادر إلى خفض آجال الإحتفاظ الشامل بالبيانات المخزنة إلى مدة أقصاها 180 يوم متصلة من تاريخ تسجيلها، مع تغليظ العقوبة حال الإحتفاظ بالبيانات المخزنة بعد إنقضاء هذا الأجل، بإستثناء الأحوال التي يصدر فيها الأمر بالحفظ العاجل للبيانات.

3. النص على حظر اللجوء إلى التفتيش عن الأدلة المعلوماتية بدون إذن قضائي مسبق، حتى في أحوال التلبس و القبض، فالظروف الطارئة لا تسمح سوى بالتفتيش المادي و الضبط الرقمي الأولي لمنع تدمير الدليل أما التفتيش المعلوماتي فيبقى خاضعا للإشراف القضائي في جميع الأحوال بدون أي إستثناء.
4. تحديد المدّة التي يبقى خلالها الإذن بالتفتيش عن الأدلة المعلوماتية ساريا لتنفيذ مرحلة التفتيش المادي، حتى لا يبقى المتهم مهددا بالإجراء فترة طويلة، و المدّة الملائمة في هذا الشأن هي مدة 14 يوما تسري من تاريخ صدور الأمر بالتفتيش، مع ترك تحديد مدّة تنفيذ مرحلة التفتيش المعلوماتي لتقدير سلطة التحقيق على أن تلتزم هذه الأخيرة بتحديد هذه المدّة ضمن الإذن القضائي مع جواز تمديدها بمدد أخرى بموجب طلبات إضافية تبرر دواعي ذلك.
5. يجب أن يتضمّن الإذن بالتفتيش عن الأدلة المعلوماتية وصفا لوسائط التخزين الرقمية المراد ضبطها في مرحلة التفتيش المادي و تحديدا للأدلة المعلوماتية التي تستهدفها مرحلة التفتيش المعلوماتي كلّ ذلك في ضوء ما تكشف عنه ظروف الواقعة الجرمية، و أن يتضمّن استراتيجية تفتيش محدّدة قابلة للمراجعة عند فشها في التوصل للدليل المستهدف.
6. يجب أن يحزّر محضر التفتيش عن الأدلة المعلوماتية في شكل خبرة تقنية تتضمّن بالتفصيل كافّة البيانات الشكلية المستوجبة حسب سلسلة الإجراءات المتبعة، في مرحلة التفتيش المادي و مرحلة الضبط الرقمي و مرحلة التفتيش المعلوماتي، منعا من التفتيش الشامل غير المبرر.
7. دعوة المشرع إلى اعتماد آلية الأمر بالحفظ العاجل للبيانات مع تقييد الجرح التي تجيز إصدار الأمر بحفظ بيانات المحتوى، بأن تكون مما يعاقب عليها بعقوبة لا تقلّ عن ثلاثة سنوات حتى يمتنع اللجوء إلى هذا الإجراء في الجرح البسيطة بالنظر إلى تفاقتها مقارنة بخطورة هذا الإجراء، على أن لا تزيد مدّة الأمر بالحفظ 14 يوما لإتخاذ إجراءات تقديم الأمر بالتسليم حتى يتحقّق التنسيق بين مرحلة التفتيش المادي و حالة الأمر بالحفظ للبيانات لوحدة الغاية من الإجراءات

و هي الضبط الأولي.

8. يحسن إضافة نص يقضي بأنه يمكن النفاذ إلى أية بيانات مخزنة وضبطها، أيا كان مكان وجودها داخل أو خارج الإقليم الوطني، إذا كانت موضوعة بتصرف الجمهور أو في حالة الحصول على الموافقة القانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات من خلال نظام معلوماتي موجود على الأراضي الجزائرية.
9. ضرورة النص على مصير البيانات التي تم ضبطتها في سبيل جمع الأدلة سواء تلك التي تقرر عدم مشروعيتها أم تلك التي تمت بطريقة مشروعة، بحيث يتعين النص على حذفها كلياً في حالة عدم المشروعية أو انتهاء التفتيش بعدم الجدوى، و يكون الحذف جزئياً بخصوص البيانات الخارجة عن نطاق الإذن بالتفتيش.
10. ضرورة تجريم فعل محو الدليل المعلوماتي أو العبث بمسرح الجريمة في البيئة الرقمية من خلال تعديل نص المادة 43 من قانون الاجراءات الجزائية.
11. حظر استغلال أي دليل جنائي معلوماتي مكتشف بشكل عرضي في مرحلة التفتيش المعلوماتي بإستثناء الأدلة المحددة في الإذن القضائي.
12. تقرير مسؤولية الدولة عن كافة أخطاء السلطة القضائية سواء من أمر بالتفتيش أو قام به متى ترتب عن فعله إهدار و تجاوز للضمانات التي تستوجبها الشرعية الإجرائية للتفتيش عن الأدلة المعلوماتية.

قائمة المصادر والمراجع

أولا/ قائمة المصادر و المراجع باللغة العربية:

أ- قائمة المصادر:

الدساتير:

1. دستور الجمهورية الجزائرية الديمقراطية الشعبية السنة 1996، المصادق عليه بإستفتاء 1996/11/28، الصادر بموجب المرسوم رئاسي رقم 96-438 مؤرخ في 7 ديسمبر 1996 الصادر بالجريدة الرسمية عدد 76، بتاريخ 8 ديسمبر 1996.
2. التعديل الدستوري لسنة 2008، الصادر بموجب القانون رقم 19/08 المؤرخ في 15 نوفمبر 2008 الجريدة الرسمية المؤرخة عدد 63، بتاريخ 2008/11/16.
3. التعديل الدستوري لسنة 2016، الصادر بموجب القانون رقم 16-01 مؤرخ في 6 مارس 2016، الجريدة الرسمية عدد 14، بتاريخ 7 مارس 2016.
4. التعديل الدستوري لسنة 2020 المصادق عليه بإستفتاء 2020/11/01، الصادر بموجب المرسوم رئاسي رقم 20-442 مؤرخ في 30 ديسمبر 2020 الصادر بالجريدة الرسمية عدد 82، بتاريخ 30 ديسمبر 2020.

الاتفاقيات الدولية:

1. الإعلان العالمي لحقوق الإنسان لسنة 1948 اعتمد بموجب قرار الجمعية العامة للأمم المتحدة 217 (أ-د) المؤرخ في 10 ديسمبر 1948.
2. إتفاقية حماية حقوق الإنسان في نطاق مجلس أوروبا المعتمدة سنة 1950 الموقعة بروما في 4 نوفمبر 1950.
3. إتفاقية فينا للعلاقات الدبلوماسية و التي إنضمت إليها الجزائر بموجب المرسوم الرئاسي رقم 74/64 المؤرخ في 4 مارس 1964 المتضمن المصادقة على هذه الإتفاقية المؤرخة في 18 أبريل 1961 .
4. إتفاقية مناهضة التعذيب و غيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة لسنة 184، اعتمدت و عرضت للتوقيع و التصديق و الانضمام بموجب قرار الجمعية العامة للأمم المتحدة 46/39 المؤرخ في 10 ديسمبر 1984.
5. الإتفاقية الأوروبية لمكافحة الجرائم المعلوماتية و المسماة "بإتفاقية بودابست" التي تم إعتماها و تقريرها التفسيري من لدن لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد

المائة (8 نوفمبر 2001) و فتح باب التوقيع على الإتفاقية في بودابست المجرية في 23 نوفمبر 2001 بمناسبة المؤتمر الدولي حول الجريمة الإلكترونية.

6. إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني و حماية البيانات ذات الطابع الشّخصي، التي تمّ اعتمادها في الدورة العادية الثالثة و العشرون لقمة رؤساء و حكومات الإتحاد الإفريقي المنعقدة في ملابو، غينيا الإستوائية، بتاريخ 27 يونيو 2014.

7. الإتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تم اعتمادها من قبل مجلس وزراء العرب و الداخلية بتاريخ 21-12-2010 و تمّ المصادقة عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 252/14 المؤرخ في 08 سبتمبر 2014، الصادر بالجريدة الرسمية عدد 57، بتاريخ 28 سبتمبر 2014.

8. مشروع اتفاقية الأمم المتحدة للتعاون في مكافحة الجريمة الإلكترونية الذي تقدمته به روسيا و عمم بصفة وثيقة رسمية صادرة عن الجمعية العامة للأمم المتحدة، تحت رقم A/C.3/72/12* مؤرخة في 16 أكتوبر 2017.

القوانين:

القوانين الجزائرية:

1. الامر رقم 66-155 المؤرخ في 08 جوان 1966 المتمضن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 48 بتاريخ 10 جوان 1966.
2. الامر رقم 66-156 المؤرخ في 8 جوان 1966 المتمضن قانون العقوبات، الجريدة الرسمية عدد 49 ، بتاريخ 11 جوان 1966.
3. القانون العضوي رقم 11/04 المؤرخ في 06/09/2004 و المتمضن القانون الأساسي للقضاء، الجريدة الرسمية عدد 57 ، بتاريخ 08 سبتمبر 2004.
4. القانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يعدل و يتم الامر رقم 66-155 و المؤرخ في 8 يونيو 1966 و المتمضن قانون الاجراءات الجزائية، الجريدة الرسمية عدد 74، بتاريخ 10 نوفمبر 2004.
5. القانون رقم 06-22 مؤرخ في 20 ديسمبر 2006 ، يعدل و يتم الامر رقم 66-155 المؤرخ في 8 يونيو 1966 و المتمضن قانون الاجراءات الجزائية، الجريدة الرسمية عدد 84 بتاريخ 24 ديسمبر 2006.

6. القانون رقم 04-09 المؤرخ في 5 أوت 2009 المتضمّن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها الجريدة الرّسمية عدد 47، بتاريخ 16 أوت 2009.
7. القانون رقم 07/13 المؤرخ في 29 أكتوبر 2013 المتضمّن تنظيم مهنة المحاماة، الجريدة الرّسمية عدد 55، بتاريخ 30 أكتوبر 2013.
8. القانون رقم 07-17 مؤرخ في 27 مارس 2017 يعدل و يتم الامر رقم 66-155 المؤرخ في 8 يونيو 1966 المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية عدد 20 بتاريخ 29 مارس 2017
9. القانون رقم 07-18 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرّسمية عدد 34، بتاريخ 10 جوان 2018.

النصوص التنظيمية:

- المرسوم الرئاسي رقم 19-172 مؤرخ في 06 جوان 2019 يحدّد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها و تنظيمها و كفاءات سيرها، الجريدة الرسمية عدد 37 ، بتاريخ 9 يونيو 2019.

القوانين العربية:

1. المرسوم التشريعي السوري رقم 17 لسنة 2012 المتعلّق بتطبيق أحكام قانون التّواصل على الشّبكة و مكافحة الجريمة المعلوماتية الصّادر بالجريدة الرّسمية بتاريخ 15 فيفيري 2012.
2. قرار وزارة الاتصال السوريّة رقم 2012/290 المتضمّن التّعليمات التّوضيحية و التّنفيذية لقانون تنظيم التّواصل على الشّبكة و مكافحة الجريمة المعلوماتية الصّادر بالجريدة الرسمية بتاريخ 07 ماي 2012.
3. قانون دولة البحرين رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات الصّادر بالجريدة الرّسمية رقم 3178 بتاريخ 09 أكتوبر 2014.
4. قانون دولة قطر رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية الصّادر بالجريدة الرّسمية عدد 15 بتاريخ 20 اكتوبر 2014.
5. قنون دولة المملكة الأردنية رقم 27 لسنة 2015 و المتعلّق بالجرائم الإلكترونية، الصّادر بالجريدة الرّسمية عدد 5343 ، بتاريخ 04 ماي 2015.

6. القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات الصادر بالجريدة الرسمية عدد 32 مكرر (ج) بتاريخ 14 أوت 2018.
7. القانون اللبناني رقم 81 لسنة 2018 و المتعلق بالمعاملات الإلكترونية و البيانات ذات الطابع الشخصي، الصادر بالجريدة الرسمية عدد 45 بتاريخ 18 أكتوبر 2018.

الأحكام والاجتهادات القضائية :

- قرار صادر عن المحكمة العليا غرفة الجناح المخالفات بتاريخ 29 جانفي 1991 رقم 1991، المجلة القضائية للمحكمة العليا، قسم الوثائق و الدراسات القانونية و القضائية، العدد 4، 1992 .
- قرار صادر عن المحكمة العليا غرفة الجناح المخالفات بتاريخ 24 جوان 2009 رقم 443709، المجلة القضائية للمحكمة العليا، قسم الوثائق و الدراسات القانونية و القضائية، العدد 2، 2009.
- قرار صادر عن المحكمة العليا غرفة الجناح المخالفات بتاريخ 2010/07/22 رقم 676593، المجلة القضائية ، قسم المستندات و النشر بالمحكمة العليا، الجزائر، العدد 2، 2011 .
- قرار صادر عن المحكمة العليا غرفة الجناح المخالفات بتاريخ 29 مارس 2016 رقم 1010894، المجلة القضائية للمحكمة العليا، قسم الوثائق و الدراسات القانونية و القضائية، العدد 01، 2016.
- قرار صادر المحكمة العليا صادر في 2005/12/21 عن الغرفة الجنائية طعن رقم 391134 المجلة القضائية قسم المستندات و النشر بالمحكمة العليا، العدد 02، سنة 2006.

الوثائق الدولية:

- الأمم المتحدة، تدابير لمكافحة الجريمة المتصلة بالحواسيب، مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة و العدالة الجنائية المنعقد ببناكوك، في الفترة 18-25 أبريل 20015، و وثيقة رقم A/conf.203/14.
- تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان الحق في الخصوصية في العصر الرقمي، وثيقة رقم A/hrc/2737 .

- الجمعية العامة للأمم المتحدة مجلس حقوق الإنسان، تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان الحق في الخصوصية في العصر الرقمي، وثيقة رقم A/hrc/2737 .
- الفريق العامل المعني بالتعاون الدولي "جمع و تبادل الأدلة الإثباتية الإلكترونية"، مؤتمر الأطراف في إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المنعقد بفيينا، في الفترة: 27 و 28 أكتوبر 2015، وثيقة رقم CTOC/COP/WG.3/2015/2.
- لائحة الجمعية العامة للأمم المتحدة رقم (63-65) المؤرخة في 22 جانفي 2001 المتعلقة بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، وثيقة رقم: A/RES/56/121
- مجلس حقوق الإنسان، الدورة الثامنة والعشرون التقرير السنوي لمفوض الأمم المتحدة السامي لحقوق الإنسان و تقارير المفوضية السامية و الأمين العام، موجز حلقة نقاش مجلس حقوق الإنسان المتعلقة بالحق في الخصوصية في العصر الرقمي بتاريخ 19 ديسمبر 2014، وثيقة رقم A/HRC/28/39 .
- مكتب الأمم المتحدة المعني بالمخدرات و الجريمة، دراسة شاملة عن مشكلة الجريمة السيبرانية و التدابير التي تتخذها الدول الأعضاء و المجتمع الدولي و القطاع الخاص للتصدي لها،" تقرير فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية و التدابير التي تتخذها الدول الأعضاء و المجتمع الدولي و القطاع الخاص للتصدي لها"، مكتب الأمم المتحدة المعني بالمخدرات و الجريمة، منظمة الأمم المتحدة، فيينا، بتاريخ 25-28 فيفيري 2013 ، وثيقة رقم . UNODC/CCPCJ/EG.4/2013/2 .
- موجز حلقة نقاش مجلس حقوق الإنسان المتعلقة بالحق في الخصوصية في العصر الرقمي، تقرير مفوضية الأمم المتحدة لحقوق الإنسان، بتاريخ 19 ديسمبر 2014، وثيقة رقم A/HRC/28/39

ب- قائمة المراجع:

الكتب:

الكتب المتخصصة:

1. توبي مندل، أندرو بوديفات، وبن واجندر، ديسكي هوتن، نتاليا توريس: دراسة استقصائية عالمية حول خصوصية الأنترنت و حرية التعبير، منظمة الأمم المتحدة للتربية و العلم و الثقافة (اليونسكو)، فرنسا، 2012.

2. **توفيق محمد الشاوي:** حرمة الحياة الخاصة و نظرية التفتيش، الطبعة الأولى، منشأة المعارف، مصر، 2006.
3. **حسام الدين محمد أحمد:** الإذن بالضبط و التفتيش، بدون رقم الطبعة، دار النهضة العربية، مصر، 2003.
4. **خالد حازم إبراهيم:** دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية (الأنترنت) دراسة مقارنة، دار النهضة العربية، مصر، 2014.
5. _____: البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الأنترنت، بدون رقم الطبعة، دار الكتب القانونية، مصر، 2006.
6. **سامي جلال فقي حسين:** الأدلة المتحصلة من الحاسوب و حجيتها في الإثبات الجنائي، بدون رقم الطبعة، دار الكتب القانونية، مصر، 2011.
7. **سامي حسني الحسيني:** النظرية العامة للتفتيش في القانون المصري و المقارن، الطبعة الأولى، دار النهضة العربية، مصر، 1972.
8. **طارق إبراهيم الدسوقي:** الأمن القانوني النظام القانوني لحماية البيانات، بدون رقم الطبعة، دار الجامعة الجديدة، مصر، 2015.
9. **عادل عبد البديع آدم حسين:** وسائل الرقابة القضائية على مشروعية الدليل الجنائي دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، مصر، 2015.
10. **عائشة بن قارة مصطفى:** حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن، دار الجامعة الجديدة، 2010.
11. **عبد الحميد الشواربي:** إذن التفتيش في ضوء الفقه و القضاء، بدون رقم الطبعة، منشأة المعارف، مصر، 1988.
12. **علي حسن محمد الطالبة:** التفتيش الجنائي على نظم الحاسوب و الأنترنت دراسة مقارنة، الطبعة الأولى، عالم الكتاب الحديث أريد، الأردن، 2004.
13. _____: أشهر المبادئ المتعلقة بالأنترنت في القضاء الأمريكي، الطبعة الأولى، دار النهضة العربية، مصر، 2004.
14. **عمر محمد بن يونس:** الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي

المرشد الفديريالي الأمريكي لتفتيش و ضبط الحواسيب توصلنا إلى الدليل الإلكتروني في التحقيقات الجنائية - ترجمة و دراسة و تحقيق - الطبعة الثانية، دار النهضة العربية، مصر، 2006

15. **ماركو جيري**: فهم الجريمة السيبرانية: الظواهر و التحديات و الاستجابة القانونية، منشورات الإتحاد الدولي للاتصالات، سوسيرا، 2014.

16. **مجدى محب حافظ**: إذن التفتيش دراسة تحليلية تطبيقية في التشريع المصري و التشريعات العربية و التشريع المقارن في ضوء الفقه و أحكام القضاء في مائة عام، بدون رقم الطبعة، دار النهضة العربية، 2001.

17. **محمد الأمين البشري**: التحقيق في الجرائم المستحدثة، الطبعة الأولى، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

18. **محمود عبد الحميد عبد المطلب**: البحث و التحقيق الجنائي الرقمي في جرائم الحاسب الآلي و الأنترنت، دار الكتب الجامعية، مصر، 2006.

19. **محمود محمد محمود جابر**: الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقال، بدون رقم الطبعة، المكتب الجامعي الحديث، مصر، 2018.

20. **مصطفى محمد موسى**: التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، 2009.

21. **منى جاسم الكواري**: التفتيش شروطه و حالات بطلانه، الطبعة الأولى، منشورات الحلبي، الحقوقية، لبنان، 2008.

22. **هشام محمد فريد رستم**: الجوانب الإجرائية للجرائم المعلوماتية دراسة مقارنة، مكتبة الآلات الحديثة، مصر، 1994.

23. **هلالى عبد الله أحمد**: التزام الشاهد بالإعلام في الجرائم المعلوماتية، الطبعة الثانية، دار النهضة العربية، القاهرة، 2008.

24. _____: المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري و البحريني على ضوء إتفاقية بودابست، الطبعة الثانية، دار النهضة العربية، مصر، 2014.

25. _____: تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999.

26. _____: حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، مصر، 2008.
27. ياسر الأمير فاروق: مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دراسة مقارنة، الطبعة الأولى، دار المطبوعات الجامعية، مصر، 2009.

الكتب العامة:

1. إبراهيم التّجاني أحمد: نظرية البطلان و أثرها على الحقوق الشرعية في القوانين الإجرائية و الجنائية السودانية، الطبعة الأولى، مركز الدراسات و البحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2001.
2. أحمد أبو القاسم: الدليل المادي و دوره في الإثبات في الفقه الجنائي الإسلامي، دار النشر بالمركز العربي للدراسات الأمنية و التدريب، الرياض، 1994.
3. أحمد الشّافعي: البطلان في قانون الإجراءات الجزائية، دراسة مقارنة، الطبعة الثانية، دار هومة، الجزائر، 2015.
4. أحمد علي عبود الخفاجي: الحصانة البرلمانية: دراسة تطبيقية في ظل دستور العراق لسنة 2005 م"، الطبعة الأولى، المركز العربي للنشر و التوزيع، مصر، 2018.
5. أحمد عوض بلال: قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، الطبعة الثالثة، دار النهضة العربية، 2014.
6. أحمد فتحي سرور: الوسيط في قانون الإجراءات الجنائية، الطبعة الثامنة، دار النهضة العربية، القاهرة، 2012.
7. _____: الشرعية الدستورية و حقوق الإنسان في الإجراءات الجنائية، بدون رقم الطبعة، دار النهضة العربية، القاهرة، 1995.
8. _____: القانون الجنائي الدستوري الطبعة الثانية، دار الشروق، مصر، 2002.
9. إيهاب عبد المطلب: الإثبات في جرائم المخدرات، الطبعة الأولى، المركز القومي للإصدارات القانونية، مصر، 2015.
10. _____: النظرية العامة للإثبات الجنائي دراسة مقارنة بين النظم

الإجرائية اللاتينية و الإنجلوساكسونية و الشريعة الإسلامية، بدون رقم الطبعة، دار النهضة العربية، مصر، 2011.

11. حسن صادق المرصفاوي: المرصفاوي في أصول الإجراءات الجنائية : الدّعى الجنائية-الدّعى المدنية- التّحقيق الإبتدائي-المحاكمة-طرق الطّعن في الأحكام، الطبعة الأخيرة، منشأة المعارف للطباعة و التّشر و التّوزيع، مصر، 1981.

12. رمزي رياض عوض: سلطة القاضي الجنائي في تقدير الأدلة، بدون رقم الطبعة، دار النهضة العربية، مصر، 2010.

13. رمسيس بهنام: الإجراءات الجنائية تأصيلا و تحليلا، الجزء الأول، منشأة المعارف، مصر، 1977.

14. _____: النظرية العامة للقانون الجنائي، الطبعة الثانية، منشأة المعارف، مصر، 1995.

15. رؤوف عبيد: المشكلات العملية الهامة في الاجراءات الجنائية، الطبعة الثالثة، دار الفكر العربي، مصر، 1980.

16. الطّبيبائي عادل: الحدود الدّستورية بين السّلتتين التّشريعية و القضائية "دراسة مقارنة"، الطبعة الأولى، مجلس النّشر العلمي، جامعة الكويت، الكويت، 2000.

17. عادل عبد العال خراشي: ضوابط التحري و الاستدلال عن الجرائم في الفقه الإسلامي و القانون الوضعي (دراسة مقارنة)، بدون رقم الطبعة، دار الجامعة الجديدة، الإسكندرية، 2006.

18. عبد القادر محمد القيسي: التحقيق الجنائي السري، الطبعة الاولى، المركز القومي للإصدارات القانونية، مصر، 2016

19. عبد الله اوهايبية: شرح قانون الإجراءات الجزائية الجزائري التّحري و التّحقيق، الطبعة التّانية، دار هومة، الجزائر، 2011.

20. عثمان أمال عبد الرحيم: شرح قانون الاجراءات الجنائية، بدون رقم الطبعة، الهيئة

- المصرية العامة للكتاب، مصر، 1988.
21. عصمت عبد المجيد بكر: مشكلات التشريع دراسة نظرية و تطبيقية مقارنة، دار الكتب العلمية، بيروت، لبنان، 2013.
22. فوزية عبد الستار: شرح قانون الإجراءات الجنائية ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، 2011.
23. مأمون سلامة: الإجراءات الجنائية في التشريع المصري، الجزء الثاني، بدون رقم الطبعة، دار النهضة العربية، مصر، 1992.
24. محمد زكي أبو عامر: الإثبات في المواد الجنائية، بدون رقم الطبعة، الفنية للطباعة و النشر، مصر، بدون سنة الطبع.
25. _____: الإجراءات الجنائية ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، لبنان، 2010.
26. _____: شائبة الخطأ في الحكم الجنائي، محاولة فقهية و نظرية لإرساء نظرية عامة، بدون رقم الطبعة، دار الجامعة الجديدة، مصر، 2011.
27. محمود نجيب حسني: شرح قانون الإجراءات الجنائية، بدون رقم الطبعة، دار النهضة العربية، القاهرة، 2013.
28. نبيل شديد الفاضل رعد: الدفوع الشككية في قانون أصول المحاكمات الجزائية، الطبعة الأولى، المؤسسة الحديثة للكتاب، 2005.
29. هلالى عبد الله أحمد: المركز القانوني للمتهم في مرحلة التحقيق الابتدائي - دراسة مقارنة بالفكر الجنائي الإسلامي"، الطبعة الثانية، دار النهضة العربية، مصر، 1988.
30. سامي صادق الملا: إقرار المتهم، الطبعة الثانية، دار النهضة العربية، مصر، 1975.
31. فاضل زيدان محمد: سلطة القاضي في تقدير الأدلة، دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر و التوزيع، الأردن، 2006.

الأطروحات الجامعية:

1. أحمد ضياء الدين محمد خليل: مشروعية الدليل في المواد الجنائية، أطروحة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 1984.
2. مفيدة سعيد سويدان: نظرية الإقتناع الذاتي للقاضي الجزائي دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 1985.
3. حسين فريجة: مسؤولية الدولة عن اعمال السلطة القضائية، أطروحة دكتوراه، معهد الحقوق و العلوم الادارية، جامعة الجزائر، الجزائر، 1990.
4. فرج إبراهيم العدوي عبده: سلطة القاضي الجنائي في تقدير الأدلة، أطروحة دكتوراه، كلية الحقوق جامعة القاهرة، 1995.
5. إيمان محمد علي الجابري: يقين القاضي الجنائي، أطروحة دكتوراه، كلية الحقوق جامعة الإسكندرية، مصر، 2002.
6. محمد حسن شريف: النظرية العامة للإثبات الجنائي، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 2002.
7. عمر محمد بن يونس: الجرائم الناشئة عن استخدام الأنترنت، أطروحة دكتوراه، كلية الحقوق جامعة عين شمس، مصر، 2004.
8. جلـول شيتـور: ضمانات تقييد الحرّية الفردية، أطروحة دكتوراه، كلية الحقوق، جامعة بسكرة، 2006.
9. طه أحمد طه متولي: الدليل العلمي و أثره في الإثبات الجنائي، أطروحة دكتوراه، كلية الحقوق جامعة طنطا، مصر، 2007.
10. كاظم السيد عطية: الحماية الجنائية لحق المتهم في الخصوصية دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 2007.
11. حسين بن سعيد الغافري: السياسة الجنائية في مواجهة جرائم الانترنت، أطروحة دكتوراه، كلية الحقوق جامعة عين شمس، مصر، 2007.
12. أحمد بن عبد الله الرّشودي: حجية الوسائل الإلكترونية في الإثبات الجنائي دراسة تأصيلية مقارنة، أطروحة دكتوراه، كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية، المملكة العربية السّعودية، 2008.

13. محمد سيد حسن محمد: ضوابط سلطة القاضي في تقدير الأدلة، دراسة مقارنة بالشريعة الإسلامية، أطروحة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 2008.
14. مستاري عادل: المنطق القضائي و دوره في سلامة الحكم الجزائي، رسالة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر بسكرة، 2011.
15. تركي بن عبد الرحمن المشير: بناء نموذج أمني لمكافحة الجرائم المعلوماتية و قياس فاعليته، أطروحة دكتوراه، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2012.
16. أميرة محمود بدوي الفقي: الإثبات الجنائي للجرائم المرتكبة عبر الأنترنت، أطروحة دكتوراه، كلية الحقوق جامعة عين شمس، مصر، 2014.
17. بدر الدين يونس: سلطة القاضي الجنائي في تقدير الدليل الجنائي، أطروحة دكتوراه، كلية الحقوق جامعة قسنطينة، 2014.
18. عادل عبد البديع آدم حسين: قاعدة مشروعية الدليل الجنائي، أطروحة دكتوراه، جامعة القاهرة، مصر، 2014.
19. محمد بركات فارس الطراونة: حجية الدليل العلمي في الإثبات الجنائي، أطروحة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 2015.
20. بن فريدة محمد: الإثبات الجنائي للجرائم المعلوماتية، أطروحة دكتوراه كلية الحقوق و العلوم السياسية، جامعة الجزائر 1، 2015.
21. رجال عبد القادر: الحماية الجزائية للحق في الخصوصية دراسة مقارنة بين الشريعة الإسلامية و القانون الجزائري، أطروحة دكتوراه، كلية العلوم الإنسانية و الاجتماعية، جامعة وهران 1، الجزائر، 2015.
22. حازم محمد حنفي عثمان: الدليل الإلكتروني و دوره في المجال الجنائي، أطروحة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 2016.
23. حسن عواد السريحي: دور البحث الجنائي في الكشف عن الجرائم المعلوماتية، أطروحة دكتوراه، كلية العدالة الجنائية جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2016.
24. محمود عبد الغني فريد جاد المولى: دور الدليل الإلكتروني و دوره في المجال الجنائي،

- أطروحة دكتوراه، كلية الحقوق جامعة بنها، مصر، 2016.
25. **ربيـعي حسيـن**: آليات البحث و التّحقيق في الجرائم المعلوماتية، أطروحة دكتوراه كلية الحقوق و العلوم السّياسية، جامعة باتنة1، 2016.
26. **سليمان غازي بخيت المقيطي العتيبي**: دور البحث الجنائي في الكشف على الجرائم المعلوماتية، أطروحة دكتوراه، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السّعودية، 2016.
27. **فيصل بدري**: مكافحة الجريمة المعلوماتية في القانون الدّولي و الدّخلي، أطروحة دكتوراه، كلية الحقوق جامعة الجزائر1 بن يوسف بن خدة، الجزائر، 2017.
28. **يوسف مناصرة**: الإثبات الإلكتروني في القانون الجنائي المقارن، أطروحة دكتوراه، كلية الحقوق جامعة الجزائر1 سعيد حمدين، 2017.
29. **بن الصّادق أحمد**: سلطة القاضي الجنائي في تقدير أدلة الإثبات، أطروحة دكتوراه، كلية الحقوق جامعة الجزائر1، الجزائر، 2017.
30. **رشيدة بوكور**: الحماية الجزائية للتعاملات الإلكترونية، أطروحة دكتوراه، كلية الحقوق و العلوم السّياسية، جامعة الجيلاني الياصب سيدي بلعباس، 2017.
31. **شرف الدّين وردة**: الإثبات الجنائي بالأدلة الإلكترونية دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق و العلوم السّياسية جامعة بسكرة، 2017.
32. **خليفة محمد صالح جاد المولي**: الدّليل الرّقمي وحجّيته في إثبات جرائم المعلومات، أطروحة دكتوراه، كلية الحقوق جامعة طنطا، مصر، 2018.
33. **بن طـالب لينـدا**: الدّليل الإلكتروني و دوره في الإثبات الجنائي دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق و العلوم السّياسية، جامعة تيزي وزو، 2019.

المقالات:

1. **أحمد ضياء الدّين محمد خليل**: الخديعة و أثرها على الدّليل الجنائي، المجلة العربية للدراسات و التّدريب، المجلد 2، العدد 2، الرّياض، أكتوبر 1985.
2. **أحمد فتحي سرور**: أثر التفتيش الباطل (مقارنة بين اتجاهات كل من القضاءين الأمريكي والمصري)، المجلة الجنائية القومية السنة الخامسة، مصر، 1962.
3. **أسامة بن غانم العبيدي**: التفتيش عن الدّليل في الجرائم المعلوماتية، مجلة البحوث

- الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، المجلد 29 العدد 58، نوفمبر 2013.
4. **أشرف محمد عبد القادر سمحان**: القواعد النّاطمة لسّطة تقدير الدّلائل الكافية (الجزء الأول)، مجلة كلية القانونيّة الكويتيّة العالميّة، الكويت، السّنة 4 العدد 1، مارس 2019.
5. **ترتيل تركي الدّرويش**: القواعد الإجرائيّة الخاصّة بالدّليل المعلوماتي في لبنان، مجلة الحقوق و العلوم السّياسيّة، الجامعة اللّبنانيّة، لبنان، المجلد 03، العدد 23، 2019.
6. **رؤوف عبيد**: نوع بطلان التّفّتيش في القانون المصري، المجلة الجنائيّة القوميّة، العدد الأول ، مصر، مارس 1960.
7. **سالم محمد الأولجي**: مقبوليّة الدّليل الرّقمي في المحاكم الجنائيّة، مجلة دراسات قانونيّة، كلية الحقوق، جامعة بنغازي، ليبيا، العدد 19، جانفي 2016.
8. **سامي حمدان الزّواشدة**: الأدلّة المتحصّلة من مواقع التّواصل الإجتماعي و دورها في الإثبات الجنائي دراسة في القانون الإنجليزي و الأمريكي، المجلة الدّولية للقانون، كلية الحقوق جامعة قطر، قطر، المجلد 3، 2017.
9. **صحبى محمد أمين**: مسؤوليّة الدولة عن الاخطاء القضائيّة و التعويض عنها في التشريع الجزائري، مجلة افاق فكريّة، كلية العلوم الانسانيّة و الاجتماعيّة، جامعة سيدي بلعباس، الجزائر، العدد 6، 2017.
10. **طارق محمد الجملي**: الدّليل الرّقمي في مجال الإثبات الجنائي، مجلة الحقوق، جامعة التّهرين، العراق، المجلد 12، العدد 1، 2010.
11. **مسعود بن حميد المعمري**: الدّليل الإلكتروني لإثبات الجريمة الإلكترونيّة، مجلة الحقوق، كلية الحقوق العلميّة، قطر، ملحق خاص، العدد 3، الجزء الثّاني، 2018.
12. **مصطفى إبراهيم العربي**: دور الدّليل الرّقمي في الإثبات الجنائي، مجلة البحوث القانونيّة، كلية القانون جامعة مصراتة ، ليبيا، مجلد 4، عدد 4، 2016.
13. **معاذ سليمان الملا**: فكرة الحق في الدّخول في طي النّسيان الرّقمي في التّشريعات الجزائريّة الإلكترونيّة الحديثة دراسة مقارنة بين التّشريع العقابي الفرنسي و التّشريع الجزائري الكويتي مجلة كلية الحقوق الكويتيّة العالميّة، الكويت، العدد 3، الجزء الأول، 2018.
14. **معتصم خميس مشعشع**: إثبات الجريمة بالأدلّة العلميّة، مجلة الشّريعة و القانون،

- جامعة الشارقة، الإمارات العربية المتحدة، السنة الرابعة و العشرون، العدد 56، 2013.
15. **ممدوح خليل البحر**: نطاق حرية القاضي الجنائي في تكوين قناعته الوجدانية، مجلة الشريعة و القانون جامعة الشارقة، الإمارات العربية المتحدة، عدد 21، 2004.
16. **ميسون خلف حمد الحمداني**: مشروعية الأدلة الإلكترونية في الإثبات الجنائي، مجلة كلية الحقوق جامعة النهدين، العراق، المجلد 18، العدد 2، 2016.
17. **ناصر بن محمد البقمي**: أهمية الأدلة الرقمية في الإثبات الجنائي، دراسة وفقا للأنظمة السعودية، مجلة الفكر الشرطي، مركز بحوث الشرطة القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مجلد 21، عدد 80، 2012.
18. **نضال ياسين الحاج حمو**: دور الدليل الإلكتروني في الإثبات الجنائي، مجلة جامعة تكريت للعلوم القانونية و السياسية، مجلد 1 السنة 5 العدد 2013، 19.

المدخلات في المنتقيات و الندوات:

1. **ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم، عبد الله عبد العزيز**: مداخلة بعنوان نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، ورقة بحثية مقدمة لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة و القانون، المنعقد في الفترة بين 10 و 12 ماي 2003، كلية الشريعة و القانون، جامعة الإمارات العربية المتحدة، المجلد الخامس، 2003.
2. **علي عبد القادر القهوجي**: مداخلة بعنوان الحماية الجنائية للبيانات المعالجة الكترونياً، ورقة بحثية مقدمة لمؤتمر مقدم إلى مؤتمر القانون و الكمبيوتر، المنعقد في الفترة بين 1 و 3 ماي 2000 جامعة الإمارات العربية المتحدة، كلية الشريعة و القانون، الطبعة الثالثة، 2004.
3. **محمد الأمين البشري**: مداخلة بعنوان (التحقيق في جرائم الحاسب الآلي، ورقة بحثية مقدمة إلى مؤتمر القانون و الكمبيوتر)، المنعقد في الفترة بين 1 و 3 ماي 2000 جامعة الإمارات العربية المتحدة، كلية الشريعة و القانون، الطبعة الثالثة، 2004.
4. **هشام محمد فريد رستم**: مداخلة بعنوان "الجرائم المعلوماتية و أصول التحقيق الجنائي الفني و اقتراح إنشاء آلية عربية موحدة للتدريب التخصصي، ورقة بحثية مقدمة لمؤتمر القانون و الكمبيوتر"، المنعقد في الفترة بين 1 و 3 ماي 2000، كلية الشريعة

و القانون، جامعة الإمارات العربية المتحدة، الطبعة الثالثة، 2004.

5. هـلالي عبد الله أحمد: بحث بعنوان (حجية المخرجات الكمبيوترية في المواد الجنائية دراسة مقارنة) ورقة بحثية مقدمة لمؤتمر القانون و الكمبيوتر، المنعقد في الفترة بين 1 و 3 ماي 2000 جامعة الإمارات العربية المتحدة، كلية الشريعة و القانون، الطبعة الثالثة، 2004.

6. عبد الناصر محمد محمود فرغلي، عبيد سيف سعيد المسماري: مداخلة بعنوان "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية دراسة تطبيقية مقارنة" ورقة بحثية مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي، جامعة نايف العربية للعلوم الأمنية، المنعقد بالرياض، في الفترة 2-4/11/2007.

A. Les dictionnaires

Serge Guinchard : Lexique des termes juridiques 2017-2018 - 25e éd, Dalloz, France, 2018.
Thierry Debard

B. Les Codes et les Lois

Liste des lois française:

- : Code pénal.
- : code de procédure pénale .
- : la Loi française n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, JORF n°129 du 5 juin 2003.
- : Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques, JORF n°73 du 26 mars 2006.
- : la LOI n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, JORF n°0129 du 4 juin 2016.
- : La Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, JO n° 0263 du 14 novembre 2014
- : la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale JORF n°0129 du 4 juin 2016.
- : Code des postes et des communications électroniques Modifié par Ordonnance n°2000-916 du 19 September 2000 JORF 22 September 2000 .

Liste des lois belges

- : Loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales, JORF du 14 janvier 2017.
- : Loi du 5 MAI 2019 portant des dispositions diverses en matière pénale et en matière de cultes, et modifiant la loi du

28 mai 2002 relative à l'euthanasie et le Code pénal social, JORF du 24 mai 2019.

Liste des Directives Européennes:

- : directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. (JO U.E n° L 201 du 31/07/2002).
- : Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, (JO U.E L 105/54 du 13.4.2006).
- : Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO U.E L 335 du 17.12.2011).
- : Directive 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, (J.O.U.E., L 65 du 11 mars 2016).
- : Directive 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017).
- : la Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale COM/2018/225 final - 2018/0108 (COD)
- : proposition de règlement (la Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale COM/2018/225 final - 2018/0108 (COD) .
- : Proposition de règlement du parlement européen et du conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, 2018/0108(COD), Strasbourg, 17 avril 2018.

C. Ouvrages:

Bouzat Pierre : La loyauté dans la recherche des preuves, in Problèmes

- contemporains de procédure pénale Recueil d'études en hommage à Louis Hugueney, Paris, Sirey, 1964.
- M. BENILLOUCHE** : Les transformations de l'administration de la preuve pénale, Société de législation comparée, France, 2006.
- Marie-Cristine Piatti** : Les libertés individuelles à l'épreuve des nouvelles technologies de l'information, Presses universitaires de Lyon, France 2001.

D. Theses :

- FRIEDRICH, Cyrielle** : Les nouvelles technologies dans la procédure pénale: aspects techniques et juridiques de ces moyens de preuve. Thèse de doctorat : Université. Genève, 2013.
- Marie Marty** : La légalité de la preuve dans l'espace pénal européen, thèse de doctorat ,Université de Strasbourg, 2016.
- Mathias Murbach-Vibert** : Les pouvoirs d'investigation en droit français, Essai d'une théorie générale, thèse de doctorat, Faculté de droit, Université Jean Moulin - Lyon 3,2010 .
- Monika Zwolinska** : Sécurité et libertés fondamentales des communications électroniques en droit français, européen et international, thèse doctorat, Université Nice Sophia Antipolis, France, 2015.

E. Articles:

- Alexandre Rousselet-Magri** : « Les perquisitions « informatiques » à l'épreuve du principe de souveraineté, dans un contexte de mondialisation du stockage de données. Étude comparée en droit français et états-unien », Revue de science criminelle et de droit pénal comparé, vol. 4, no. 4, 2017.
- Catherine Forget** : La collecte de preuves informatiques en matière pénale, Pas de droit sans technologie, Larcier, Bruxelles, 2015.
- Derrida Fernand** : Perquisitions et saisies chez les avocats, avoués et notaires, Revue de science criminelle et de droit pénal comparé, n° 2, Dalloz, France , 1953.
- Giudicelli-Delage** : Les transformations de l'administration de la preuve pénale Perspectives comparées : Allemagne, Belgique, Canada, Espagne, Etats-Unis, France, Italie, Portugal, Royaume-Uni, Archives de politique criminelle, n° 26, 2004.
- Gorphe (François).** : La méthode générale d'examen critique des preuves, Revue de science criminelle et de droit pénal comparé, n° 1, Dalloz, France ,1947.
- H. LECLERC** : Les limites de la liberté de la preuve; Aspects actuels en France, Revue de science criminelle et de droit pénal comparé, Dalloz, France, 1992.
- Halard, Guillaume.** : Réflexions sur la provocation policière, Revue de science

- criminelle et de droit pénal comparer, vol. 1, no 1, Dalloz, France, 2018.
- John SPENCER** : La preuve en procédure pénale, droit anglais, Revue internationale de droit pénale, v 63, 1er et 2eme trim, Editions ERES, Paris, 1992.
- Larguier (Jean)** : La protection des droits de l'homme dans le procès pénal dans le sens de la protection des droits des personnes suspectes ou poursuivies depuis l'enquête jusqu'à la fin du procès, Revue internationale de droit pénal, Editions ERES, Paris, 1966.
- Larguier (Anne-Marie)**
- Leroux Olivier** : En marge de l'affaire Gaia : de la recevabilité de la preuve pénale et du respect de la vie privée, Revue générale de droit civil belge (Mechelen), 2003.
- Poullet Yves**
- Olivier Decima** : les investigations numériques en procédure pénale français: du piratage informatique aux réquisitions et saisie numériques ? Revue la faculté de droit, université de galatasaray, n° 1, 2017.
- Philippe Belloir** : Les réquisitions judiciaires en matière de délinquance numérique. Revue Lamy droit de l'immatériel ex Lamy droit de l'informatique, n° 92, 2013.
- Renucci, Jean-François** : Droits de l'homme, Revue de science criminelle et de droit pénal comparé, vol 4, n° 4, Dalloz, France ,2014.
- Rousselet Marcel** : Les ruses et les artifices dans l'instruction criminelle, Revue de science criminelle et de droit pénal comparé, n° 1, Dalloz, France, 1946.
- Sophie Sontag Koenig** : Les perquisitions 2.0 : quand l'informatique se saisit de l'immatériel, AJ pénal, Dalloz, France, 2016.

F. Documents Internationaux:

- Conseil de l'Europe** : la criminalité informatique, (Recommandation no R (89) 9 sur la criminalité en relation avec l'ordinateur et rapport final du comité européen pour les problèmes criminels, Editions du Conseil de l'Europe, Strasbourg, 1990.
- Conseil de l'Europe** : Rapport final du Groupe de travail du T-CY sur les preuves dans le clou, TCY(2016)5F Accès de la justice pénale aux preuves électroniques dans le cloud : Recommandations pour examen par le T-CY , Direction générale des droits de l'homme et de l'Etat de droit Conseil de l'Europe, Strasbourg, France, 2016.
- Conseil de l'Europe** : Recommandation n° R(95)13 du Comité des Ministres aux Etats membres relative aux problèmes de procédure pénale liés à la technologie de l'information. (Adoptée par le Comité des Ministres le 11 septembre 1995, lors de la 543e réunion des Délégués des Ministres).

G. Actes des Congrès

- Association internationale de droit penal** : XVIème Congrès International de Droit Pénal, (Rio de Janeiro, Brésil/Brazil, 4-10 Septembre 1994), Revue International de Droit Penal, 1-2 éme trimestres Editions ERES, Paris 1995.
- Erman Sahir** : les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Turquie, Revue internationale de droit pénale, Editions ERES, Paris, 1993.
- JAEGER (Marc)** : les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France Revue internationale de droit pénale, Editions ERES, Paris, 1993.
- Lorena Bachmaier Winter** : Procédure pénale. Société de l'information et droit pénal. Rapport Général, Revue internationale de droit pénal 2014/1 (Vol. 85)
- Marsh, Norman S** : Le principe de la légalité dans une société libre : rapport sur les travaux du Congrès international de juristes tenu à New Delhi (Janvier 1959).

H. La Jurisprudence

la jurisprudence de la cour de cassation française

- Cass crim, 24 nov 1970, no 70-90.161, Bull. Crim, 1970, n° 312.
- Cass. Crim ,23 mars 1977, n° 75-92.170, Bull. Crim, 1977, n° 109.
- Cass Crim, 18 mai 1983, n°1983, 82-93.410 Bull. Crim, 1983, n° 148.
- Cass Crim, 20 nov 1984, n° 84-91.332, Bull. Crim, 1984, n° 361
- Cass Crim, 7 mars 1989, 87-90.500, Bull. Crim, 1989, n° 109.
- Cass Crim, 19 juin 1991, n° 90-86.630, Bull. Crim. 1991, n° 267
- Cass Crim., 12 mars 1992, n° 91-86.843, Bull. Crim, 1992, n° 112.
- Cass crim, 20 mai 1992, n° 91-84.297, Bull. Crim, 1992, n° 201.
- Cass. Crim, 15 juin 1993, n° 92-82.509, Bull. Crim, 1993, n° 210.
- Cass crim.29 mars 1994, n°39-85.995, Bull. Crim, 1994, n° 118,
- Cass Crim, 4 janv. 1996, n° 95-84.330, Bull. Crim 1996, n° 5.
- Cass. Com, 9 mars 1999, n° 96-16.559, Bull. Crim 1999, n°54
- Cass Crim, 27 avril 2000, n° 00-80.420, Bull. Crim 2000, n°170.
- Cass Crim, 16 mai 2000, 99-85.304, Bull. Crim, 2000, n° 192
- Cass Crim, 28 juin 2000, n° 00-80.292, Bull. Crim, 2000, n° 252
- Cass Crim, 25 octobre 2000, n°00-80.829, Bull Crim2000, n° 317.
- Cass Crim, 30 janv. 2001, n° 00-87.155, Bull. Crim 2001, n° 26.
- Cass Crim, 19 juin 2001, n°99-85.188, Bull. Crim, 2001, n° 149.

- Cass Crim 27 juin 2001, n° 01-81.865, Bull. Crim, 2001, n° 163.
- Cass Crim, 11 juin 2002, n° 01-85.559, Bull. Crim. 2002, n° 131.
- Cass Crim, 12 janv. 2005, n° 04-81.982, Bull. Crim, 2005, n° 17
- Cass Crim ,8 juin 2005, n°05-82.012, Bull. Crim 2005, n°173.
- Cass Crim, 8 juin 2005, n°05-82.012, Bull. Crim.2005 n°173.
- Cass Crim, 11 mai 2006, n° 05-84.837, Bull. Crim. 2006, n° 132.
- Cass Crim., 9 août 2006, n° 06-83.219, Bull. Crim, 2006, n°202.
- Cass Crim, 3 déc 2006 n°06-82196, Bull. Crim 2006, n° 313
- Cass Crim 4 juin 2008, n° 08-81.045, Bull. Crim n°141.
- Cass crim.27 janvier 2010, n°09-83.395, Bull. Crim 2010, n° 16.
- Cass. Crim, 30 novembre 2011, n° 10-81749 ,Bull. Crim, 2011, n° 243.
- Cass. crim, 24 avril 2013, n 12-80331, Bull. Crim, 2013, n° 102.
- Cass. crim 25 juin 2013, n°12-88.021, Bull. Crim, 2013, n° 155.
- Cass crim 25 juin 2013, n° 12-88.021, Bull. Crim, 2013, n° 155
- Cass Crim, 25 juin 2013, n° 12-88.021, Bull. Crim. 2013, n° 155.
- Cass. Crim, 6 nov. 2013, n° 12-87.13, Bull. Crim 2013, n° 217.
- Cass. Crim, 27 novembre 2013, n°12-85.830, Bull. Crim, 2013, n° 242
- Cass crim, 26 févr. 2014, n o 13-87.065, Bull. Crim, 2014, n° 61
- Cass crim 30 avr. 2014, n o 13-88.162, Bull. crim, 2014, n° 119.
- Cass Crim, 30 avril 2014, n°13-88.162, Bull. Crim 2005, n°119.
- Cass crim8 juillet 2015, n° 14-88457, Bull. Crim, 2015, n° 176
- Cass. crim 9 février 2016, 15-85.063, Bull. Crim, 2016, n° 34
- Cass Crim, 21 juin 2016, n°16-80.126, Bull. Crim,2016 , n° 188.
- Cass Crim, 16 mai 2018, n° 17-84909. Bull. Crim 2018 ,n° 05.
- Cass Crim, 14 mai 2019, n° 19-81.408, Bull. Crim. 2019, n° 92.

la Jurisprudence du Conseil Constitutionnel français

- Décision n° 2016-536, QPC du 19 février 2016.

la jurisprudence de la Cour Constitutionnelle belge

- l'arrêt n° 174/2018 du 6 décembre 2018 Numéro du rôle : 6711

la jurisprudence de la cour européenne des droits de l'homme

- CEDH, Arrêt VINCI CONSTRUCTION ET GTM GÉNIE CIVIL ET SERVICES c. FRANCE, 2 avril 2015, n° 63629/10 et 60567/10.
- CEDH, Arrêt Funke c. La France du 25 février 1993, Série A, n° 256-A.
- CEDH, Arrêt John Murray c. Royaume-Uni, 8 février 1996, n° 18731/91.
- CEDH, Arrêt SAUNDERS v. UNITED KINGDOM du 17 Décembre 1996, Série A, n°

19187/91.

- CEDH, Arrêt Saunders c. Royaume-Uni, du 17 décembre 1996, n° 19187/91.
- CEDH., Société colas Est et autres / France, 16 avril 2002, n° 37971/97.
- CEDH, Van Rossem colas / Belgique, 09 décembre 2004, n° 41872/98
- CEDH, arrêt RAMANAUSKAS c. LITUANIE, du 5 févr. 2008, n° 74420/01.
- CEDH, arrêt S. et Marper c. Royaume Uni, 4 décembre 2008 nos 30562/04 et 30566/04.
- CEDH, Da Silveira c/ France, 21 janv. 2010, n° 43757/05.
- CEDH, AFFAIRE MESSIER c. FRANCE, 30 juin 2011, 25041/07.

La jurisprudence de la cour de justice de l'union européenne

- Cour européenne de justice, arrêt de la Cour dans les affaires jointes C-293/12 et C-594/12, Digital Rights Irelan et Seitlinger et autres, arrêt du 8 avril 2014.

I. Sources électroniques :

Conseil de l'Europe : Guide sur l'article 6 de la Convention européenne des droits de l'homme - Droit à un procès équitable (volet pénal), 2014, p. 37, disponible sur www.echr.coe.int (consulté le 12/11/2019).

Cour européenne des droits de l'homme

Serge Migayron : Critères d'appréciation technique, vraies et fausses preuves numérique, Colloque du 13/04/2010. La preuve numérique à l'épreuve du litige. Les acteurs du litige à la preuve numérique (l'information numérique fait la preuve).
Disponible à l'adresse

www.cnejita.org/.../CNEJITA-ACTESCOLLOQUE13042010-A5-V5.1.pdf, Consulté le 15 janvier 2018.

Union internationale des télécommunications : Preuve électronique, Modèles de lignes directrices politiques et de textes législatifs Harmonisation des politiques, législations et procédures réglementaires en matière de TIC dans les Caraïbes, Disponible à l'adresse

hipcar.gov.kn/sites/hipcar.gov.kn/files/HIPCAR_1-2_B_Model_Policy_Guidelines_and_Legislative_Texts_Electronic_Evidence.pdf, Consulté le 08 décembre 2018.

A. International conventions.

: Project « EVIDENCE » (European Informatics Data Exchange Framework for Courts and Evidence).

B. Books :

Sveva Avveduto, Sara Conti, Daniela Luzi, and Lucio Pisacane : The Conceptual Representation of the “Electronic Evidence” Domain, Handling and Exchanging Electronic Evidence Across Europe, Springer International Publishing, 2018.

United States Department of Justice : Forensic Examination of Digital Evidence: A Guide for Law Enforcement, National Institute of Justice , Washington, 2004, - Richard boddington, practical digital forensics, first edition, packt publishing, London, 2016.

Eoghan Casey : Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet, Academic Press, London, 2000.

Eoghan Casey, Susan W. Brenner : Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet, 3rd Edition, Academic Press, London, 2011.

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.

Mattia Epifani, Pasquale Stirparo : Learning IOS Forensics, First published, Packt Publishing, England, 2015.

Spoenle, Jan : cloud computing and cybercrime investigations: territoriality vs the power of disposal, Conseil de l’Europe, Strasbourg. Economic Crime Division Directorate General of Human Rights and Legal Affairs Council of Europe Strasbourg, 2010.

Stephen Mason, Daniel Seng : Electronic Evidence, Fourth edition published by the Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017.

C. Thesis:

Carrier Brian : A hypothesis-based approach to digital forensic Investigations, philosophy doctoral thesis, Purdue

- University, United States of America, 2006.
- Shahzad Saleem** : Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics, philosophy doctoral thesis, Stockholm University, Sweden, 2015.
- Khaled Ali Aljneibi** : The Regulation of Electronic Evidence in the United Arab Emirates: Current Limitations and Proposals for Reform, philosophy doctoral thesis, Bangor University, Royaume-Uni, 2014.
- D. Articles:***
- Adam M. Gershowitz** : The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches, Vanderbilt law review, Vol 69, 2016.
- Bartholomew Paige** : Seize First, Search Later: The Hunt for Digital Evidence, Touro Law Review, Vol. 30: No. 4, 2014
- Berman Emily** : Digital Searches, the Fourth Amendment, and the Magistrates' Revolt, Emory Law Journal, Emory University School of Law, Vol 68, Issue 1, 2018.
- Chan, Gerald.** : "Life after Vu: Manner of Computer Searches and Search Protocols." The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference 67. 2014.
- 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.
- Christine Sgarlata Chung and David J. Byer** : The Electronic Paper Trail: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence, Journal of Science & Technology Law, V 179, boston university, 1998.
- 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.
- Frank Adelstein** : Live forensics: diagnosing your system without killing it first, Communications of the ACM, V.49 N.2, 2006.
- Howard A. Denemark** : Search for Scientific Knowledge in Federal Courts in the Post-Frye Era: Refuting the Assertion that Law Seeks Justice While Science Seeks Truth, High Technology Law Journal, Vol. 8, No. 2 ,1993.
- Manfred Mohrenschrager** : Computer Crime and Other Crime Against Information Technology in Germany, Revue internationale de droit

- pénale, Editions ERES, Paris, 1993.
- James T. Stinsman** : Computer seizures and searches rethinking the application of the plain view doctrine, Temple Law Review, Vol. 83, 2011.
- Josh Goldfoot** : The Physical Computer and the Fourth Amendment, Berkeley J. Crim. L. Vol 16, Issue 1, 2011.
- Lily R. Robinton** : Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence, YALE J.L. & TECH V 12, 2010.
- Mark Krotoski** : Effectively Using Electronic Evidence Before and At Trial, United States Attorneys Bulletin, Vol. 59, N 6, 2011.
- Mark Taticchi** : Note, Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures, George Washington Law Review, Vol 78, 2010.
- 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.
- : Digital Evidence and the New Criminal Procedure, Columbia Law Review, Vol 105, Issue 1, 2005.
- : Note: «Digital Duplications and the Fourth Amendment», HARV. L. REV. Vol. 129, 2016.
- : Ex Ante Regulation of Computer Search and Seizure, Virginia Law Review, Vol 96, Issue 6, 2010.
- : Executing Warrants for Digital Evidence: The Case for Use Restrictions on Non responsive Data, Texas Tech Law Review, Vol 48, Issue 1, 2015.
- : Fourth Amendment Seizures of Computer Data, Yale Law Journal, Vol. 119, Issue 4, 2010.
- : Search Warrants in an Era of Digital Evidence, Mississippi Law Journal, Vol 75, Issue 1, 2005.
- : Searches and Seizures in a Digital World, Harvard Law Review, Vol 119, Issue 2, 2005.
- Paul Ohm** : Massive Hard Drives, General Warrants, and the Power of Magistrate Judges, Virginia Law Review, Vol 97, 2011.
- Paul Ohm** : The Fourth Amendment Right to Delete, Harvard Journal of Law. Vol 119, 2005.
- 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, No. 4, 2012.

- Susan W. Brenner & Barbara Frederiksen** : Computer Searches and Seizures: Some Unresolved Issues, Michigan Telecommunications and Technology Law Review, Vol. 8, Issue 39, 2002.
- Thomas K. Clancy** : The Fourth Amendment Aspects of Computer Searches and Seizures, Miss. L.J, Vol 75 ,2005.

E. Web sites :

- Orin S. Kerr** : When Does a Carpenter Search Start and When Does It Stop? [Available online].Retrieved November 26,2019,from ://www.lawfareblog.com/when-does-carpenter-search-start-and-when-does-it-stop.
- Usama Salama, Vijay Varadharajan, and Michael Hitchens,** : “Metadata Based Forensic, nalysis of Digital Information in the Web”, Annual Symposium on Information Assurance & Secure Knowledge Management, 2012, Available online].Retrieved January 20.2018
from <https://pdfs.semanticscholar.org/eaf2/42704b6915e6b359218c1c6725c3245e65f0.pdf>.

F. Reports :

- : Report on Digital Evidence - Prepared by: Mark M. Pollitt, BS, Unit Chief Computer Analysis Response Team - FBI Laboratory, Washington, DC, USA, 13th INTERPOL Forensic Science Symposium, Lyon, France, October 16-19, 2001.

G. Jurisprudences :

- Andresen v. Maryland, 427 U.S. 463 (1976)
- Bolger v. United States, 189 F. Supp. 237 (S.D.N.Y. 1960)
- Commonwealth v. Fulton, 179 A.3d 475 (Pa. 2018).
- Commonwealth v. Johnson, L., Pet, 434 WAL 2018 (Pa. 2019)
- Commonwealth v. Keown, 478 Mass. 232, 240-41 (2017),
- Commonwealth v. McDermott, 448 Mass. 750, 776 (2007).
- Dalia v. United States, 441 U.S. 238 (1979)
- Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001)
- In re 3817 W. West End, First Floor Chicago, Illinois. 60621.2004 WL 138002272(ND III May 27,2004)
- In re F.P., 878 A.2d 91, 95–96 (Pa.Super.2005).
- In re Search of 3817 W. West End, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004)
- In Re Search of 3817 W. West End, First Floor Chicago, Ill. 60621, 321 F. Supp. 2d 953 (N.D. Ill. 2004)
- In re Search Warrant, 71 A.3d 1158, 1169 n.11 (Vt. 2012)
- In re Search Warrant, 71 A.3d 1158, 1169 n.11 (Vt. 2012).

- Klayman v. Obama, 13-cv-851 (D.D.C. Feb. 10, 2014.)
- People v Covlin 2018 NY Slip Op 28011 Decided on January 22, 2018 Supreme Court, New York Country.
- Riley v. California, 134 S. Ct. 2473, 2493–94 (2014)
- Smith v. Maryland, 442 U.S. 735, 739–40 (1979)
- State v. Eleck, 130 Conn. App. 632, 23 A.3d 818 (2011),
- State v. Mansor, 421 P.3d 323 (Ore. 2018).
- United States v Carpenter, No. 16-402, 585 U.S. (2018)
- United States v Giberson, 527 F.3d 882, 886 (9th Cir. 2008)
- United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007)
- United States v. Apple iPhone, IMEI 013888003738427, Criminal No. 2014-0278 (D.D.C. 2014),
- United States v. Burgess, 576 F.3d 1078, 1093 (10th Cir. 2009)
- United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000)
- United States v. Carey, 172 F.3d 1268, 1275 n.8 (10th Cir. 1999).
- United States v. Galpin, 720 F.3d 436, 446 (2d Cir. 2013)
- United States v. Ganas, 755 F. 3d 125, 134 (2d Cir. 2014).
- United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008)
- United States v. Gorshkov, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001)
- United States v. Gourde, 440 F.3d 1065, 1077 (9th Cir 2006)
- United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999)
- United States v. Greathouse, 297 F. Supp. 2d 1264, 1275 (D. Or. 2003).
- United States v. Hill, 459 F.3d 966, 977 (9th Cir. 2006)
- United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998)
- United States v. in the Matter of the Search Associated With Rwgann, Criminal No. 2014-0228 (D.D.C. 2014)
- United States v. Mann, 592 F.3d 779 (7th Cir. 2010),
- United States v. Metter, 860 F. Supp. 2d 205, 212 (E.D.N.Y. 2012).
- United States v. Micah J. Gourde, 440 F.3d 1065 (9th Cir. 2006)
- United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018) United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000).
- United States v. Payton, F.3d, 2009 WL 2151348 (9th Cir. July 21, 2009)
- United States v. Reyes 798 F.2d 380, 383 (10th Cir. 1986)
- United States v. Richards, 659 F.3d 527 (6th Cir. 2011)
- United States v. Russian, No. 17-3157 (10th Cir. 2018)
- United States v. Schesso, 730 F.3d 1040 (9th Cir. 2013)
- United States v. Turner, 169 F.3d 84 (1st Cir. 1999),

قائمة المصادر والمراجع

- United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999)
- United States v. Comp. Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010).

الفهرس

مقدمة

2	أولاً: التعريف بالموضوع
3	ثانياً: الأشكالية الرئيسية
4	ثالثاً: تساؤلات البحث
4	رابعاً: منهج البحث
5	خامساً: أسباب اختيار الموضوع
5	سادساً: أهمية البحث
7	سابعاً: أهداف البحث
7	ثامناً: الدراسات السابقة
8	تاسعاً: صعوبات البحث
8	عاشراً: خطة البحث

الفصل التمهيدي

ماهية الأدلة المعلوماتية المستمدة من التفتيش

11	تمهيد و تقسيم:
12	المبحث الأول: مدلول الأدلة المعلوماتية المستمدة من التفتيش
12	المطلب الأول: مفهوم الدليل المعلوماتي المستمد من التفتيش
12	الفرع الأول: تعريف الدليل المعلوماتي المستمد من التفتيش
12	أولاً: تعريف الإتفاقيات للدليل المعلوماتي المستمد من التفتيش
15	ثانياً: التعريف التشريعي للدليل المعلوماتي المستمد من التفتيش
18	ثالثاً: التعريف الفقهي للدليل المعلوماتي المستمد من التفتيش
18	أ) : ربط تعريف الدليل المعلوماتي بمنطق تكوينه
23	ب) : ربط تعريف الدليل المعلوماتي بفكرة المعلومة
26	الفرع الثاني: تحديد المصطلح الدقيق للدلالة على الدليل المعلوماتي المستمد من التفتيش
26	أولاً: موقف الفقه المقارن

27موقف الفقه العربي	ثانياً :
32خصائص الدليل الجنائي المعلوماتي المستمد من التفتيش	المطلب الثاني :
34الدليل المعلوماتي دليل علمي	الفرع الأول :
35الدليل المعلوماتي من طبيعة تقنية متطورة	الفرع الثاني :
36الدليل المعلوماتي مفهوم يحتوي التنوع و التطور	الفرع الثالث :
37ذاتية الدليل المعلوماتي المستمد من التفتيش	المطلب الثالث :
37الجوانب السلبية للدليل المعلوماتي المستمد من التفتيش	الفرع الأول :
37الطابع غير المستقر للدليل المعلوماتي المستمد من التفتيش	أولاً :
38صعوبة الوصول إلى الدليل المعلوماتي	ثانياً :
40صعوبة نسبة الدليل المعلوماتي إلى متهم معين	ثالثاً :
42مزايا الدليل الإلكتروني الدليل المعلوماتي	الفرع الثاني :
42الدليل المعلوماتي دليل قابل للنسخ	أولاً :
44الدليل المعلوماتي يصعب التخلص منه	ثانياً :
47الدليل المعلوماتي يحتوي على معلومات أكثر تفصيلاً عن الوقائع	ثالثاً :
49تقسيمات الأدلة المعلوماتية المستمدة من التفتيش و تصنيفها	المبحث الثاني :
49تقسيمات الأدلة المعلوماتية المستمدة من التفتيش	المطلب الأول :
50تقسيم الأدلة المعلوماتية على أساس درجة تعارضها مع الحق في الخصوصية	الفرع الأول :
50الأدلة المعلوماتية المستمدة من البيانات المتعلقة بالمرور	أولاً :
51الأدلة المعلوماتية المستمدة من البيانات المتعلقة بالمحتوى	ثانياً :
52الأدلة المعلوماتية المستمدة من البيانات المتعلقة بالمشاركين	ثالثاً :
54تقسيمات الأدلة المعلوماتية على أساس قيمتها الإثباتية	الفرع الثاني :
54أدلة معلوماتية أعدت لتكون وسيلة إثبات	أولاً :
55أدلة معلوماتية لم تعد لتكون وسيلة إثبات	ثانياً :
56تقسيمات الأدلة المعلوماتية على أساس المحتوى	الفرع الثالث :
57الأدلة المعلوماتية المستمدة من سجلات الحاسوب المتولدة	أولاً :
57الأدلة المعلوماتية المستمدة من سجلات الحاسوب المخزنة	ثانياً :

58	الأدلة المعلوماتية المستمدة من سجلات الحاسوب المتولدة و المخزنة	ثالثا:
59	تصنيف الأدلة المعلوماتية المستمد من التفتيش	المطلب الثاني:
59	تصنيف الدليل المعلوماتي من حيث علاقته بالواقعة الإجرامية	الفرع الأول:
64	تصنيف الدليل المعلوماتي من حيث مصدره	الفرع الثاني:

الباب الأول

الأحكام الإجرائية للأدلة المعلوماتية المستمدة من التفتيش

73	وضع المشكلة:
----	-------	--------------

الفصل الأول

تأصيل التفتيش عن الأدلة المعلوماتية

74	تمهيد و تقسيم:
75	مدلول فكرة التفتيش عن الأدلة المعلوماتية	المبحث الأول:
75	مفهوم التفتيش عن الأدلة المعلوماتية	المطلب الأول:
75	تعريف التفتيش عن الأدلة المعلوماتية	الفرع الأول:
75	تعريف التفتيش المادي	أولا:
78	تعريف التفتيش المعلوماتي	ثانيا:
80	خصائص التفتيش المعلوماتي	الفرع الثاني:
80	الجبر و الإكراه	أولا:
82	المساس بحق الخصوصية المعلوماتية	ثانيا:
86	الطبيعة القانونية للتفتيش المعلوماتي	الفرع الثالث:
90	التمييز بين التفتيش المعلوماتي و الضبط الرقمي	المطلب الثاني:
90	مدلول الضبط الرقمي	الفرع الأول:
90	تعريف الضبط الرقمي	أولا:
93	الأساس القانوني لاعتبار النسخ الرقمي بمثابة ضبط	ثانيا:
94	الاتجاه الأول الضبط الرقمي يتعارض مع الحق في الحذف	(أ):
94	الاتجاه الثاني الضبط الرقمي يتعارض مع الحق في الحياة الحصرية للمعلومات	(ب):

96	الاتجاه الثالث الضبط الرقمي تجميد للأدلة المعلوماتية.....	: (ج)
97	معيان التمييز بين التفتيش المعلوماتي و الضبط الرقمي.....	الفرع الثاني:
106	مراحل التفتيش المعلوماتي و الضبط الرقمي.....	الفرع الثالث:
109	مقدمات التفتيش عن الأدلة المعلوماتية.....	المبحث الثاني:
110	الضبط العرضي الشامل للبيانات الموجودة بحوزة المتهم.....	المطلب الأول:
110	أساس مشروعية الضبط العرضي الشامل للبيانات الموجودة بحوزة المتهم.....	الفرع الأول:
115	الموقف التشريعي من مشروعية الضبط العرضي الشامل للبيانات الموجودة بحوزة المتهم.....	الفرع الثاني:
119	ضبط بيانات المتهم الموجودة بحوزة مزود الخدمة.....	المطلب الثاني:
119	الحفظ العاجل للبيانات المعلوماتية المخزنة و تسليمها.....	الفرع الأول:
123	التنظيم التشريعي للأمر بالحفظ العاجل للبيانات المخزنة.....	الفرع الثاني:
129	قيود الأمر بالحفظ العاجل للبيانات المعلوماتية المخزنة.....	الفرع الثالث:
129	القيود الموضوعية للأمر بالحفظ العاجل للبيانات المخزنة.....	أولاً:
134	القيود الزمنية للأمر بالحفظ العاجل للبيانات المخزنة.....	ثانياً:
137	الإشراف القضائي على إجراء الأمر بالحفظ العاجل للبيانات و تسليمها.....	ثالثاً:

الفصل الثاني

ضوابط التفتيش عن الأدلة المعلوماتية

143	تهديد وتقسيم:
144	الضوابط الموضوعية للتفتيش عن الأدلة المعلوماتية.....	المبحث الأول:
144	سبب التفتيش المعلوماتي.....	المطلب الأول:
144	التحقق الفعلي لجريمة من نوع جنائية أو جنحة.....	الفرع الأول:
144	الوقوع الفعلي للجريمة.....	أولاً:
145	حظر التفتيش المعلوماتي في سياق التحوط لجريمة مستقبلية.....	: (أ)
146	الاستثناء الوارد على قاعدة حظر التفتيش المعلوماتي لمنع وقوع الجريمة.....	: (ب)
152	نوع الجريمة.....	ثانياً:

156	إتهام شخص بارتكاب جريمة أو الاشتراك فيها	الفرع الثاني:
157	توافر الدلائل الكافية	الفرع الثالث:
162	المحل	المطلب الثاني:
163	المقصود بمحل التفتيش المعلوماتي	الفرع الأول:
164	مفهوم محل التفتيش	أولاً:
163		
165	إشكالية تحديد محل التفتيش المعلوماتي	ثانياً:
165	إشكالية المنظور المزدوج لمحل التفتيش المعلوماتي	أ) :
171	إشكالية ارتباط محل التفتيش المعلوماتي بمستهدف التفتيش المادي	ب) :
175	متطلبات التّحديد الكافي لمحل التفتيش المعلوماتي	الفرع الثاني:
175	المعالجة القضائية لمتطلبات التّحديد الكافي لمحل التفتيش	أولاً:
177	مدى كفاية متطلبات التّحديد الكافي لمحل التفتيش في تضييق نطاقه	ثانياً:
180	مشروعية محل التفتيش المعلوماتي	الفرع الثالث:
180	حضر تفتيش المحل المعلوماتي المتمتع بالحصانة	أولاً:
180	الحصانة الدبلوماسية	أ) :
182	الحصانة البرلمانية	ب) :
185	حق الدفاع	ج) :
189	استراتيجية مراجعة ملفات الحاسوبية في المحل المتمتع بالحصانة	ثانياً:
190	الصّوابط الشّكلية للتفتيش عن الأدلة المعلوماتية	المبحث الثاني:
193	الإذن بالتفتيش المعلوماتي	المطلب الأول:
193	لزوم استصدار إذن مسبب بالتفتيش المعلوماتي	الفرع الأول:
193	التّظيم التّشريعي و القضائي لشرط الإذن بالتفتيش المعلوماتي	أولاً:
193	ضرورة استصدار إذن بالتفتيش يستهدف النّظام المعلوماتي على وجه التّخصيص	أ) :
198	حالات التفتيش المعلوماتي بدون إذن قضائي	ب) :
198	التفتيش المعلوماتي بدون إذن قضائي لظروف طارئة	- 1
201	التفتيش المعلوماتي بناء على القبض على الأشخاص	- 2
205	المقومات الشّكلية للإذن القضائي بالتفتيش المعلوماتي	ثانياً:

205	بيانات الإذن القضائي بالتفتيش المعلوماتي	: (أ)
206	تسبب الإذن القضائي بالتفتيش المعلوماتي	: (ب)
207	الإختصاص بتنفيذ الإذن بالتفتيش المعلوماتي	الفرع الثاني:
208	امتداد الاختصاص بالتفتيش داخل إقليم الدولة	أولاً:
208	ارتباط فعالية التفتيش المعلوماتي بسرعة امتداد نطاقه	: (أ)
212	ضمانات امتداد التفتيش المعلوماتي داخل الإقليم	: (ب)
212	ارتباط محل التفتيش الأولي بنظام معلوماتي آخر	- 1
217	تجديد الإذن القضائي بامتداد التفتيش المعلوماتي	- 2
218	امتداد الاختصاص بالتفتيش خارج إقليم الدولة	ثانياً:
223	الاتجاه المؤيد لامتداد التفتيش المعلوماتي العابر للحدود	: (أ)
228	الاتجاه المناهض للتفتيش المعلوماتي العابر للحدود	: (ب)
228	الميعات الزماني لتنفيذ إذن التفتيش المعلوماتي	الفرع الثالث:
228	ميعاد تنفيذ إذن التفتيش المعلوماتي	أولاً:
231	ميعاد تنفيذ مرحلة التفتيش المادي	: (أ)
233	ميعاد تنفيذ مرحلة التفتيش المعلوماتي	: (ب)
237	مدة سريان الإذن في مرحلة التفتيش المعلوماتي	ثانياً:
237	تحديد أسلوب تنفيذ التفتيش المعلوماتي	المطلب الثاني:
243	مدلول قاعدة لزوم تحديد أسلوب تنفيذ التفتيش المعلوماتي	الفرع الأول:
244	المعاملة القضائية و الفقهية لقاعدة لزوم تحديد أسلوب تنفيذ التفتيش المعلوماتي	الفرع الثاني:
244	الاتجاه المؤيد للقاعدة	أولاً:
245	حماية الحريات الفردية	: (أ)
246	الإشراف القضائي المباشر على التنفيذ	: (ب)
246	اعتبارات عملية	: (ج)
246	الاتجاه المناهض للقاعدة	ثانياً:
256	الاعتبارات الدستورية	: (أ)
250	اعتبارات الفعالية	: (ب)

256 نقص خبرة القضاة في فرض استراتيجية التفتيش	: (ج)
259 بدائل قاعدة لزوم تحديد أسلوب تنفيذ التفتيش المعلوماتي	: الفرع الثالث:
264 خلاصة الباب الأول	
 الباب الثاني	
 حجية الأدلة المعلوماتية المستمدة من التفتيش	
266	: وضع المشكلة:
 الفصل الأول	
 القيمة الإثباتية للأدلة المعلوماتية المستمدة من تفتيش مشروع	
267	: تمهيد وتقسيم:
268 حرية القاضي الجنائي في قبول الدليل المعلوماتي المستمد من التفتيش المشروع.....	: المبحث الأول:
268 ماهية حرية القاضي الجنائي في قبول الدليل المعلوماتي المستمد من التفتيش.....	: المطلب الأول:
268 مدلول حرية القاضي في قبول الدليل المعلوماتي المستمد من التفتيش	: الفرع الأول:
268 التّحديد القانوني لمبدأ حرية القاضي الجنائي في قبول الدليل.....	: أولاً:
270 التّعريف الفقهي لمبدأ حرية القاضي الجنائي في قبول الدليل.....	: ثانياً:
270 التّعريف القضائي لمبدأ حرية القاضي الجنائي في قبول الدليل.....	: ثالثاً:
271 مبررات مبدأ حرية القاضي الجنائي في قبول الدليل.....	: الفرع الثاني:
271 السند المنطقي لسلطة القاضي الجنائي في قبول الدليل المعلوماتي المستمد من التفتيش.....	: أولاً:
273 السند التشريعي لسلطة القاضي الجنائي في قبول الدليل المعلوماتي المستمد من التفتيش.....	: ثانياً:
276 السند القضائي لسلطة القاضي الجنائي في قبول الدليل المعلوماتي المستمد من التفتيش.....	: ثالثاً:
277 نطاق حرية القاضي الجنائي في قبول الدليل المعلوماتي المستمد من التفتيش.....	: الفرع الثاني:
277 قيد تحديد الأدلة في جريمة الرّنا.....	: أولاً:

279	قيد إثبات المسائل غير الجزائية.....	ثانياً:
281	القيود الواردة على حرّية القاضي في قبول الدليل المعلوماتي المستمد من التفتيش.....	المطلب الثاني:
281	مبدأ مشروعية الدليل المعلوماتي المستمد من التفتيش.....	الفرع الأول:
281	أولاً: مدلول قاعدة مشروعية الدليل المعلوماتي المستمد من التفتيش.....	أولاً:
281	المفهوم العام لقاعدة مشروعية الدليل الجنائي.....	أ):
284	تعريف المشروعية في مجال الأدلة المعلوماتية المستمدة من التفتيش....	ب):
286	نطاق قاعدة مشروعية الدليل المعلوماتي المستمد من التفتيش في حالة البراءة.....	ثانياً:
290	مبدأ نزاهة الدليل المعلوماتي المستمدة من التفتيش.....	الفرع الثاني:
290	مفهوم مبدأ نزاهة الدليل المعلوماتي المستمد من التفتيش.....	أولاً:
293	متطلبات نزاهة الأدلة المعلوماتية المستمدة من التفتيش.....	ثانياً:
293	حظر الخديعة و التحريض على الجريمة حال التفتيش عن الدليل المعلوماتي.....	أ):
298	حظر إجبار المتهم على البوح بالأرقام السرية لإجراء التفتيش المعلوماتي.....	ب):
304	حظر تفتيش النظام المعلوماتي للأثنى بغير الاستعانة بأثنى.....	ج):
307	حرّية القاضي الجنائي في تقدير الدليل المعلوماتي المستمد من التفتيش المشروع.....	المبحث الثاني:
308	مبدأ حرّية القاضي الجنائي في الاقتناع.....	المطلب الأول:
308	مضمون حرّية القاضي الجنائي في الاقتناع.....	الفرع الأول:
308	التحديد الفقهي لمبدأ الاقتناع الذاتي للقاضي الجنائي.....	أولاً:
310	المفهوم القانوني لمبدأ الاقتناع الذاتي للقاضي الجنائي.....	ثانياً:
314	التحديد القضائي لمبدأ الاقتناع الذاتي للقاضي الجنائي.....	ثالثاً:
316	أثر القيمة العلمية للدليل المعلوماتي على اقتناع القضاة الجنائي.....	الفرع الثاني:
321	القيود الواردة على حرّية القاضي الجنائي في الاقتناع بالدليل المعلوماتي المستمد من التفتيش.....	المطلب الثاني:
321	مبدأ يقينية الدليل المعلوماتي المستمد من التفتيش.....	الفرع الأول:

321 مفهوم اليقين القضائي.	أولاً:
324 حدود التزام القاضي بقاعدة يقينية الدليل المعلوماتي.	ثانياً:
324 اشتراط يقينية الدليل المعلوماتي المستمد من التفتيش للقضاء بالإدانة...	أ) :
328 استثناء حالة البراءة من شرط يقينية الدليل المعلوماتي المستمد من التفتيش.....	ب) :
330 مبدأ وضعية الدليل المعلوماتي المستمد من التفتيش.....	الفرع الثاني:
330 مفهوم مبدأ وضعية الدليل المعلوماتي المستمد من التفتيش.....	أولاً:
335 النتائج المترتبة على مبدأ وضعية الدليل المعلوماتي المستمد من التفتيش.....	ثانياً:
338 مبدأ موثوقية الدليل المعلوماتي المستمد من التفتيش.....	الفرع الثالث:
338 إشكالية ارتباط موثوقية الدليل المعلوماتي بأصلته.....	أولاً:
341 المعالجة الفقهية و القضائية لإشكالية موثوقية الدليل المعلوماتي.....	ثانياً:
344 معيار تقييم موثوقية الدليل المعلوماتي المستمد من التفتيش.....	ثالثاً:
الفصل الثاني		
القيمة القانونية للأدلة المعلوماتية المستمدة من تفتيش غير مشروع		
351	تمهيد وتقسيم:
352 جزاء التفتيش غير المشروع عن الأدلة المعلوماتية	المبحث الأول:
352 تحديد الجزاء الإجرائي للتفتيش غير المشروع عن الأدلة المعلوماتية.....	المطلب الأول:
352 قواعد البطلان بشكل عام.....	الفرع الأول:
352 تعريف البطلان.....	أولاً:
354 مذاهب البطلان.....	ثانياً:
354 مذهب البطلان القانوني.....	أ) :
356 مذهب البطلان الذاتي.....	ب) :
357 الموقف التشريعي من مذاهب البطلان.....	ثالثاً:
360 تقسيمات البطلان.....	رابعاً:
361 أنواع البطلان.....	أ) :

363 معيار التمييز بين البطلان المطلق و البطلان النسبي	: (ب)
365 أهمية التمييز بين البطلان المطلق و البطلان النسبي	: (ج)
367 طبيعة بطلان التفتيش عن الأدلة المعلوماتية	الفرع الثاني:
367 موقف التشريع	أولاً:
370 موقف الفقه	ثانياً:
370 الرأي القائل بالبطلان النسبي	: (أ)
371 رأي يعدد حالات البطلان المطلق	: (ب)
372 الرأي الذي يفرق بين القواعد الموضوعية و القواعد الشكلية	: (ج)
374 موقف القضاء	ثالثاً:
376 أحكام الدفع ببطلان التفتيش عن الأدلة المعلوماتية	الفرع الثالث
377 الدفع ببطلان التفتيش من الدفع الموضوعية	أولاً:
378 لا محل للبطلان في حالة الرضا	ثانياً:
382 بطلان التفتيش لا يتمسك به إلا صاحب الشأن	ثالثاً:
384 أثر بطلان التفتيش في استبعاد الأدلة المعلوماتية	المطلب الثاني:
384 اثر بطلان التفتيش على الأدلة المعلوماتية المستمدة منه	الفرع الأول:
388 أثر بطلان التفتيش على الأدلة المستمدة من الإجراءات السابقة عليه	الفرع الثاني:
388 أثر بطلان التفتيش على الأدلة المستمدة من الإجراءات اللاحقة عليه	الفرع الثالث:
394 الجزاءات التي توقع على مرتكب التفتيش غير المشروع عن الأدلة المعلوماتية	المبحث الثاني:
395 الجزاء الجنائي	المطلب الأول:
395 جريمة انتهاك حرمة المنزل	الفرع الأول:
398 جرمي الدخول أو البقاء غير المشروع في النظام المعلوماتي	الفرع الثاني:
403 جريمة إنشاء أسرار التحقيق	الفرع الثالث:
406 المسؤولية المدنية	المطلب الثاني:
407 الوضع في التشريع الفرنسي	الفرع الأول:

409الوضع في التّشريع الأمريكي	الفرع الثاني:
410الوضع في التّشريع الجزائري	الفرع الثالث:
413الجزاء التأديبي	المطلب الثالث:
415	خلاصة الباب الثاني	
417النتائج و الإقتراحات	خاتمة:
419	قائمة المراجع
449	فهرس المواضيع

ملخص:

لما كانت الفلسفة الكلية التي يستقيم عليها قانون الإجراءات الجزائية هي الموازنة بين أهدافه الثلاثة "الفعالية" و "الشرعية" و "الحقيقة"، كان لدراسة الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش - على ضوء هذه الفلسفة الكلية - هدف وحيد لا تتعقب سواه هو البحث عن ضوابط المحافظة على التوازن بين هذه الثلاثة بإرساء قيود جديدة يتفاعل من خلالها التفتيش عن الأدلة الجنائية مع البيئة الرقمية التزاما بالشرعية و تقرير البطلان جزاء مخالفتها التزاما بالمشروعية، و لا يحول دون ذلك أن يكون هذا الدليل صارخا في مظهره على نسبة الجريمة إلى المتهم متى انطوى على مساس بمقتضيات الشرعية، فمهما بلغت صعوبة الإثبات و جب أن يظل مبدأ الشرعية قيذا على حرية الإثبات الجنائي، و إلا أصبحت الضمانات الدستورية مجرد كلمات شكلية، و الضمان القضائي مجرد وهم زائف لحماية الحريات الفردية، طالما أن الضوابط الإجرائية ليست سوى عزاء تافه لضحايا القانون.

كلمات مفتاحية: دليل معلوماتي، تفتيش، شرعية، فعالية، حقيقة، حريات فردية.

Résumé :

Étant donné que la philosophie générale sur laquelle repose le Code de procédure pénale est un équilibre entre ses trois objectifs, "efficacité", " La légalité " et "vérité", l'étude de La légalité procédurale des preuves informatiques tirées de la perquisition - à la lumière de cette philosophie - n'a qu'un seul objectif : chercher les commandes de contrôle de l'équilibre entre cette trilogie en établissant de nouvelles restrictions grâce auxquelles la recherche de preuves légales interagit avec l'environnement numérique conformément à la légalité constitutionnelle et le rapport de nullité pour violation d'un engagement de légalité. Et cela n'empêche pas que cette preuve soit flagrante dans son apparence sur la condamnation de l'accusé, tant qu'elle est entachée de violation des lois. Même s'il est difficile à prouver, le principe de légalité doit rester une restriction à la liberté de la preuve. Sinon, les garanties constitutionnelles ne sont que des mots formels et la sécurité judiciaire n'est qu'une fausse illusion pour protéger les libertés individuelles, tant que les contrôles procéduraux ne sont qu'une consolation triviale pour les victimes de la loi.

Mots-clés: Preuve informatique, perquisition, légalité ,l'efficacité, Vérité , libertés individuelles.