مجلة الدراسات القانونية المقارنة
المجلد 06/ العـــدد02 (2020)، ص.ص.1220-1244. ISSN:2478-0022 EISSN:2600-6154

الإشكاليات العملية الهامة للتفتيش الإلكتروني– دراسة مقارنة –

الجزء الأول: إشكالية المفهوم و التّكييف

The Practical Issues that are Important in the Electronic Searche *(*Comparative Study)

Part one: The issue of the concept and the adaptat

رابـح لهـوى

Rabah LAHOUA

طالب دكتوراه،كلية الحقوق و العلوم السياسية جامعة باتنة 1، الجزائر

PhD Student, Faculty of law and Political Science University of Batna1, *Algeria*
Lahoua.rabeh@gmail.com

تاريخ إرسال المقال: 2020/09/27 تاريخ القبول:2020/09/30 تاريخ النشر:/2020/12

ملخص:

لقد استقر في ضمير الهيئة الاجتماعية تمتع أجهزة التّخزين الرّقمية بحرمة تتجاوز المفهوم الرّاسخ لحرمة المساكن وغرف النّوم، بحيث بات مجرّد قيام السلطة الإجرائية بضبط هذه الأجهزة يشكل تهديدا صارخا للحرّيات الفرديّة، و لو لم يتم الاطلاع على أسرار الأفراد، على نحو لم يعد يسعفنا المعيار التّقليدي في تكييف التّفتيش طالما أنّ انتهاك التّوقع المعقول للخصوصيّة يقع في مرحلة إجرائيّة سابقة عن الوّلوج إلى هذا المحلّ، مما يستدعي البّحث عن معيار آخر جديد يتوافق مع هذه الرّؤية الجديدة للحق في الخصوصيّة و ذلك هو مستهدف البّحث.

كلمات مفتاحية:

تفتيش إلكتروني، ضبط رقمي، حريات فردية.تكييف.

Abstract:

It has been fixed in the conscience of the social organization that digital storage devices have a privacy that surpasses the one of houses and even bedrooms. The setting of these devices, that is the job of the procedural authority, has became a real menace to the individual liberties, namely the right of privacy. If this authority had no access to the individual's secrets, as long as the traditional standard failed to help us in the adaptation of the inspection, privacy would be broken even more. Therefore, there should be a new standard that works well with the new vision of privacy right.

Email: lahoua.univ@gmail.com **المؤلف المرسل: رابح لهوى**

Keywords:

Digital Searche, Seizure, Individual Liberties, Adaptation.

مقدمة:

أصبح من الصعب في الوقت الرّاهن تصور جريمة ليس لها بُعد رقمي، نتيجة استغلال المجرمين لتقنية المعلومات في تحقيق مآربهم الجرمية بعيدا عن أعين السطات العامة، و هي حقيقة كانت لها انعكاسات مباشرة على وسائل الإثبات الجنائي من منطلق التّوافق المطلوب تحقيقه دائما بين طبيعة الدّليل و طبيعة الجريمة الّتي يتولد منها، تلك الضرورة الّتي جلبت معها نوعا جديدا من الأدّلة الجنائية يعرف بالأدّلة الإلكترونية، ما فرض على القضاء الاعتراف بحجيتها في بناء حكم الإدانة أو البراءة انطلاقا من مبدأ عتيد في الإجراءات الجزائية يقوم على حرية القاضي الجنائي في قبول الأدلة الجنائية و تقدير قيمتها الاقناعية.

غير أنّ استجابة القضاء المقارن و تفاعله مع الأبعاد الجديدة للظاهرة الإجرامية سرعان ما كشف عن مظهر جديد من مظاهر الصراع بين اعتبارات "الفعالية" من جهة و اعتبارات "الشرعية" من جهة أخرى، بحسبان أنّ إجراءات تحصيل هذا النّوع المستحدث من الأدلة الجنائية قد يُخلف وجها من أوجه التصادم و التعارض بين حق الهيئة الاجتماعية في مواجهة الجريمة في ثوبها التقني و بين حق الفرد في التّمتع بحقوقه الرّقميّة و في مقدمتها الحق في الخصوصيّة المعلوماتيّة، فالصراع المحموم بين هذه الثنائية لا يزال مستمرا و سيظل كذلك طالما أنّ التطور التقني لا يزال في بداياته و لم يصل بعد إلى منتهاه.

على أنّه لا تنكشف لنا حقيقة التعارض القائم بين التّفتيش الإلكتروني و الحرّيّات الفرديّة إلاّ عند تحليل الضمانات القانونية المقرّرة للأفراد حال تفتيش أنظمتهم المعلوماتيّة و التنقيب في محتوياتها بحثا عن عناصر الحقيقة، بيد أنّ مثل هذه المعاجلة تعتبر بمثابة مصادرة على المطلوب، لأنّه من غير المنطقي بحث مدى شرعيّة التّنظيم القانوني للعمل الإجرائي قبل تحديد المعيار التّشريعي الّذي على ضوئه يتم تكييف الإجراء الجزائي، و لا مرية في أنّ التّفتيش التّقليدي يقوم على معيار واحد بقي محل اجماع فقهي مؤداه "الاطلاع على محل له حرمة بحثا عن الحقيقة"، بحيث أنّ الدخول إلى المسكن و الاطلاع على محتوياته ثم مغادرته يشكل النهج المسلم به للتفتيش، و كل إجراء سابق عن دخول المسكن أو لاحقا للخروج منه لا يعد بمثابة تفتيش بالمعنى الّذي يريده القانون.

غير أنّ هذه المسلمات لدى فكر التّفتيش التّقليدي تثير معها تحدّيات قانونية فرضتها القدرات التخزينية الضخمة في البيئة الرقمية نتيجة اختلاط البينات و تشابكها و تعذر فرز الملفات البريئة عن الملفات المجرّمة، بحكم لجوء المجرمين إلى جعل الملف البريء ستارا للملف المجرّم، ما يُلزم السلطة الإجرائيّة على ضبط الحاويات المادية لهذه البيانات ثم إخضاع هذه الأخيرة للتفتيش الإلكتروني لاحقا، و هو ما جلب معه تساؤلات عدة حول مفهوم التّفتيش في البيئة الرقمية طالما أنّ شعور الفرد بتقييد حريته و انتهاك حقه في الخصوصيّة يقع بمجرد ضبط البيانات و لو لم تتكمن سلطة التحقيق من الاطلاع عليها، فهل يقع التّفتيش الإلكتروني بمجرد ضبط هذه البيانات أم يُشترط تحقق الاطلاع البشري عليها، فإذا كان الجواب بـ (لا) فمتى يقع التّفتيش الإلكتروني إذن؟ أو بالأحرى ما هو المعيار الفاصل بين الضبط الرقمي

العرضي و التّفتيش الالكتروني؟ متى ينتهي التّفتيش الالكتروني، هل بمغادرة النظام المعلوماتي كما هو الشأن بالنسبة إلى تفتيش المساكن الّتي لا يجوز إعادة تفتيشها بعد مغادرتها إلاّ بعد استصدار إذن قضائي جديد أم أنّ عملية التّفتيش الإلكتروني بحكم ما تستنفذه من وقت طويل تبيح للمحقق إعادة الولوج إلى النظام المعلوماتي مجددا دون مراعاة هذه المقتضيات؟ هل إهمال الضوابط الإجرائيّة للتّفتيش الإلكتروني حال عدم تمكن المحقق من النّفاذ إلى النظام المعلوماتي لا يرتب لصاحب الشّأن الحق في المطالبة بالتّعويض عن الإجراء غير المشروع طالما لم يتحقّق انتهاك التّوقع المعقول للخصوصيّة بمفهوم التّفتيش التّقليدي؟ من هنا تتجلى الإشكالية الرئيسية واضحة تبحث عن الحل: إلى مدى ينجح مفهوم التّفتيش المادي في إرساء معيار واضح لتكييف التّفتيش الالكتروني؟

إنّ التّجاوب مع كافة هذه الإشكاليات يقودنا إلى القول بأنّ فلسفة الحقوق و الحرّيّات في البيئة المعلوماتيّة تحتاج إلى رؤية جديدة تراعي الخصوصيّة الّتي بات يتمتّع بها النّظام المعلوماتي، و أنّ التّعامل معها وفق منظور تقليدي قد تكون عواقبه وخيمة على الحرّيّات الفرديّة، و من ثم فقد استهدفنا من خلال هذه الدراسة وضع التأصيل النظري لمفهوم التّفتيش الإلكتروني و تلك مسألة غاية في الأهمية باعتبارها مفترض أساسي يتم الاتفاق عليه مسبقا لتحديد التّكييف القانوني لهذا العمل الإجرائي، و على ضوئه تتقرّر ضوابط هذا الإجراء منعا من التّعسف و الشطط، و من هنا تتجلى أهميّة البحث في محاولته معاجلة هذه التّساؤلات الّتي ظلت محل استفهام إلى غاية اليوم خاصة لدى القضاء الأمريكي صاحب التجديد المستمر في الفكر القانوني.

و للوصول إلى هدف البحث سوف نستعين بالمنهج التحليلي و المقارن للتّعرف على جزئيات المشكلة و ردها إلى عناصرها الأولية لاستخلاص القواعد و الأحكام ذات الصلة، على أن يكون التركيز بشكل كبير على منهج الاستقراء بالانتقال من الجزئيات إلى الكليات سعيا لاستنباط الأحكام العامة لموضوع البحث، و هو ما يفرض علينا معاجلة "إشكالية المفهوم" بتحديد ماهية هذا الإجراء من خلال المبحث الأول، و معاجلة "اشكالية التّكييف" بتحديد معيار التّمييز بينه و بين أهم إجراء يشتبه به و هو الضّبط الرقمي، من خلال المبحث الثاني[1].

المبحث الأول: ماهية التّفتيش الإلكتروني

ينطلق بحث مفهوم التّفتيش الإلكتروني من حقيقة لا تقبل الجدل مفادها أنّ مُستهدف هذا الإجراء هو مكون رقمي مرهون وجوده بوجود حاوية مادّيّة له لا ينفصل عنها، تشكل وسيلة الاتصال بين البيئة المادّيّة و البيئة الرّقميّة، و هو ما يجعل هذا الإجراء ينفرد بأوجه من الذّاتية من حيث مفهومه و خصائصه، لذا وجب إلقاء الضوء على مدلول هذا الإجراء (مطلب أول) و مميّزاته (مطلب ثاني).

المطلب الأوّل: التّفتيش الإلكتروني بالمعنى القانوني

من البديهي أن يسبق إجراء التّفتيش الإلكتروني تفتيش تقليدي بمفهوم مادّي يستهدف البحث عن الحاوية المادّيّة للدّليل المعلوماتي، و من ثم فإنّه لا مناص من التّطرق إلى تعريف التّفتيش المادي (فرع أول)، ثم نردفه بتعريف التّفتيش الإلكتروني، اتساقا مع خطوات تنفيذ هذا الإجراء في الواقع (فرع ثاني).

الفرع الأوّل: مدلول التّفتيش المادي

من المسلّم به في اطار الفقه التّقليدي أنّ التّفتيش مرتبط بموضوع مادي "مستهدف التّفتيش"، و محل مادي "مكان التّفتيش"، و ذلك بحثا عن دليل "ذا بعد مادي"، لذا فضّلنا إلحاق الطّبيعة المادّيّة على هذا الإجراء تمييزا له عن التّفتيش الإلكتروني الّذي يفتقد لهذه الصّفة من حيث مستهدفه و محله و حتّى أسلوب تنفيذه، و على العموم لم تتضمّن التّشريعات تعريفا للتّفتيش التقليدي غير أنّ الفقه أورد تعريفات متعدّدة له و إن اختلفت صياغاتها فقد تطابقت مضامينها، فيعرّفه الفقيه سامي حسني الحسيني بأنّه "إجراءات من إجراءات التّحقيق تقوم به سلطة حدّدها القانون، يستهدف البّحث عن الأدّلة المادّيّة لجناية أو جنحة تحقّق وقوعها، في محل خاص يتمتّع بالحرمة بغض النّظر عن إرادة صاحبه"[2]، بينما يرى الفقيه توفيق محمد الشّاوي أنّ التّفتيش "هو إجراء تقوم به السّلطة القضائية للاطلاع على محلّ يتمتّع بحرمة خاصّة للبّحث عن الأدّلة اللاّزمة للتّحقيق الجنائي"[3].

في حين تطرّق الفقه المقارن إلى تعريف هذا الإجراء بتعاريف لا تختلف كثيرا عمّا جاء به الفقه العربي بسبب تأثر الفقهاء العرب بالفقه اللاّتيني و أيضا لكون التّشريعات العربية مستوحاة من هذا النّظام القانوني، فيُعرّف الفقيه الفرنسي Serge Guinchard التّفتيش بأنّه "بحث بوليسي أو قضائي على عناصر الدّليل عن جريمة ما، و يمكن وفقا لقواعد قانونيّة خاصّة أن يُنفَذ في المسكن الخاص بأيّ شخص أو في أيّ مكان آخر حيث يمكن أن توجد أشياء يكون اكتشافها مفيدا في إظهار الحقيقة "[4].

و قد ساهم القضاء بدروه في تحديد مدلول التّفتيش المادّي، فعرّفته محكمة النّقض المصرية بقولها "التّفتيش كما هو معروف في القانون هو ذلك الإجراء الّذي رخّص الشّارع فيه التّعرض لحرمة الشّخص بسبب جريمة وقعت أو ترجّح وقوعها، و ذلك تغليبا للمصلحة العامة على مصالح الأفراد الخاصّة و احتمال الوصول إلى دليل مادّي يكشف الحقيقة"[5]. و في سياق مقارب عرّفته محكمة النّقض الفرنسية بأنّه "إجراء يراد به البحث في مكان مغلق عن أدلة ارتكاب الجريمة ونسبتها إلى مرتكبها"[6]، أمّا المحكمة العليا الفيدرالية الأمريكية فقد تعرّضت لمدلول هذا الإجراء في قضية Smith v. Maryland، معتبرة إيّاه "إجراء ينتهك التّوقع المعقول أو المشروع للحق في الخصوصيّة"[7].

فالتّفتيش المادي إذن هو "السّعي للحصول على الأدّلة لدى المتّهم ذاته أو مسكنه أو حيثما تكون تحركاته، شريطة إتباع إجراءات شكلية يتطلبها القانون، و تكمن الفكرة الأساسية للتّفتيش في إباحة انتّهاك الحق في الخصوصيّة طالما أنّ هناك مبرّر في القانون لهذا الانتهاك، و من ثم يعدّ التّفتيش أحد مظاهر تقييد الحرّيّات الإنسانيّة الّتي ساهمت التّشريعات الكبرى الأساسية في دعم المحافظة عليها[8]، فهو إجراء من إجراءات التّحقيق يستهدف البحث عن أدلة مادية لجريمة تحقّق وقوعها و ذلك في محل يتمتّع بالحرمة، أي أنّه إطلاع استثنائي على مستوع السر ابتغاء كشف حقيقة الواقعة الإجرامية بأشخاصها.

الفرع الثاني: مدلول التّفتيش الإلكتروني

إنّ التّطور المتسارع لتقنية المعلومات جعل المشرّع العربي و المقارن يتفادى الخوض في إيراد تعريف محدّد لهذا الإجراء المستحدث خشية صيرورة التّعريف الّذي يصاغ عتيقا لا يتوائم مع التّطور التّقني[9]، و يميل الفقه عموما إلى اعتبار التّفتيش الإلكتروني "مجرّد تفتيش تقليدي ينصب على الأجهزة الإلكترونية"[10]، لذا يعرّفه جانب من الفقه بكونه

"إطلاع على البيانات المخزّنة في النظام المعلوماتي"[11]، فهو "إجراء ينصّب على المعلومات و يسمح بجمع الأدّلة المخزّنة أو المسجّلة في شكل إلكتروني"[12]، أي أنّ "كل ولوج إلى نظام معلوماتي من قبل السّلطة هو بمثابة تفتيش إلكتروني باستثناء بعض الحالات المنصوص عليها قانونا"[13].

و إن اختلفت التّشريعات في المصطلح المستعمل للدلالة هذا الإجراء، فإنّ كلمة "تفتيش" تترجم فكرة ممارسة الدّولة لسلطة قسرية، و هي نظيرة لمصطلح التّفتيش التّقليدي الّذي يعني البحث، القراءة، التّمحيص، و فحص البيانات المعلوماتيّة، و إن كان مصطلح "الولوج" أو "النّفاذ" هو الأدق لأنّه أكثر ارتباطا بالمصطلحات المعلوماتيّة[14]، لذا فإنّ غالبية الفقه العربي يرجّح انطباق المفهوم التّقليدي على هذا الإجراء، فعرّفه البعض بكونه "تنقيب في وعاء السّر بقصد ضبط ما يفيد من الأسرار في كشف الحقيقة، فجوهر التّفتيش هو كشف نقاب السّرية عما تحتويه نظم الحاسوب من خفايا و أسرار و نوايا إجرامية، و بالتّالي إزاحة ستار الكتمان عنها في معرفة الحقيقة، و هذا المعنى لا يتقيّد بالمكان المادّي لوعاء السّر سواء كان مسكنا أو شخصا أو جهاز حاسوب أو نظاما أو برنامجا، أو أية أجهزة ملحقة بالحاسوب"[15].

و بهذا المعنى فنحن نرى أنّ التّفتيش الإلكتروني هو إطلاع استثنائي لسلطة التّحقيق على معلومات مخزّنة تتمتّع بالحرمة بهدف ضبط ما يفيد من الأسرار في كشف الحقيقة، على أنّه ينبغي الإشارة إلى مسألة جوهرية مفادها أنّ القول بأنّ لكلا الإجراءين – التّفتيش التّقليدي و التّفتيش الإلكتروني – نفس المفهوم و الجوهر لا يفيد اعتبارهما بمثابة نفس الإجراء، إذ يبقى التّفتيش الإلكتروني إجراء مستقل بذاته عن التّفتيش المادي بما يتميّز به من خصائص، لا مناص من تفصيل البحث بشأنها.

المطلب الثّاني: تمييز التّفتيش الإلكتروني عن التّفتيش المادي

يتميّز التّفتيش الإلكتروني بخصائص قد تتوفر في التّفتيش المادي، إلاّ أنّها تأخذ بعض سمات الذّاتية حال ارتباطها بالبيئة الرّقميّة، و هي المساس بحرمة المعلومات كحق طغى على باقي الحقوق التقليدية في المجتمع المعلوماتي(فرع أول)، و أيضا لكون التّفتيش المادّي يعتبر مقدمة ضرورية للتّفتيش الإلكتروني و من مستلزمات تنفيذه (فرع ثاني).

الفرع الأول: المساس بحق الخصوصيّة المعلوماتيّة

يُقال في الفقه إنّ تفتيش الشّخص يعدّ قيدا على حصانته أو" حرمته الذّاتية"، و تفتيش المسكن يعد قيدا أو استثناء يرد على "حرمة المسكن" أو "حرمة المراسلات"، بمعنى أنّ التّفتيش هو مساس بقاعدة "الحرمة" l'inviolabilité للشّخص ذاته أو مسكنه أو رسائله[16]، فهل يتمتّع الفرد بهذا الإمتياز على معلوماته أو بياناته المخزنة؟ و إن كان الأمر كذلك فما المقصود بـ "حرمة المعلومات"؟ ما هو الحق الّذي تقوم على حمايته؟

جرى الفقه قديما على الإكتفاء بالقول بأنّ التّفتيش يقيّد حرمة المسكن، و هو قول أجوف لا معنّى له، فالحرمة في نظر القانون هي الحماية و الإحترام[17]، و قد أضفى المشرّع حمياته على هذا المحل باعتباره مكنونا لسر الفرد، و لذلك فإنّ المشرّع لم يستهدف رعاية الشّخص كجسم معيّن و لا المسكن كبناء خاص، و إنما السّر الّذي يحمله فقط [18]، فإن كانت الحصانة المقرّرة قانونا تتعلق بالحرّية الفرديّة في عمومها، فلا مناص من القول إذن بأنّ "حق السّر" لا يتقيد بالمكان

المادّي لوعائه فيستوي أن يكون مسكنا أو شخصا أو رسائل، لأنّ هذا الحق يرتبط بالأصل الّذي يبنى عليه مبناه "الحرّية الفرديّة بمعناها الواسع"، و هذا المبدأ هو الّذي يحول دون إرساء قاعدة عامة تضبط التّوقع المعقول للخصوصية و يجعل بذات الوقت توقعات الخصوصيّة بعيدة عن تحديد ثابت بل تتغيّر التّوقعات مع تقدم التّكنولوجيا و الأعراف و الممارسات الاجتماعية السّائدة أو الّتي تطرأ على الهيئة الاجتماعية، و من ثمّ فهي تشمل حرمة المعلومات لأنّها مستودّع لسّر الفرد في الوقت الرّاهن، و الّذي بات يعرف بالحق في الخصوصيّة المعلوماتيّة[19].

و في هذا الصّدد ذكرت الدّائرة الأمريكية الاستئنافية الثّانية أنّ "التّقدم التّكنولوجي و اعتماد الأفراد على أجهزة الحاسوب في حياتهم أمر جعل القرص الصّلب أقرب إلى مقر الإقامة من حيث نطاق و كمية المعلومات الخاصّة الّتي قد تحتّوي عليها هذه الأجهزة "[20]، و قد لاحظ هذا القضاء أيضا أنّه "بالنسبة لمعظم أفراد المجتمع، فإنّ أجهزة الحاسوب الخاصّة بهم هي أكثر الأماكن خصوصيّة بالنّسبة إليهم، بل هي أكثر خصوصيّة من غرف نومهم[21]، إذ "غالبًا ما يكون الحاسوب الشّخصي مستودعا للمعلومات الخاصّة الّتي لا ينوي مالك الحاسوب مشاركتها مع الآخرين، ففي نظر أغلب الأفراد فإنّ أجهزة الحاسوب الشّخصية هي المساحات الأكثر خصوصية"[22].

لذا نحن لا نؤيّد التوجه الفقهي الّذي يطالب إطلاق لفظ "المنزل الرّقمي" domicile numérique على "النّظام المعلوماتي" بمنطق الدعوة إلى المساواة بينهما في الحماية الإجرائيّة[23]، لأنّ حرمة هذا الأخير تفوق بكثير حرمة المسكن التّقليدي، ذلك أنّ ما يكشفه التّفتيش التّقليدي من أسرار يبقى منحصرا في إطار ضيق نسبيا لا يخرج عن حدود الحيز المكاني و الزّماني لتنفيذ التّفتيش، أي ضمن نطاق محدّد كالمسكن أو الجسم، و ضمن المدّة المحددة لتنفيذ التفتيش فقط و الّذي يتحدد في ضوئه نطاق وعاء السر الخاضع للتفتيش. أمّا التّفتيش الإلكتروني فهو لا يتقيّد في ما يكشفه من أسرار بحدود الزّمان و المكان لحظة تنفيذه، بل يزيح ستار الكتمان عن كافة أوجه الحياة الخاصّة الّتي بات وعاؤها فعلا يشكّله النّظام المعلوماتي، الّذي تحفظ فيه كل وقائع حياة الفرد اليومية بأدّق تفاصيلها و تسلسلها الزّمني و هذه الحتميّة مقتضى طبيعي للتّحول نحو مجتمع معلوماتي[24]، لذا من الصّعب إعطاء هذا الحق وصفا قانونيا محددا في الوّقت الحالي، لأنّ أوصافه تتعدّد بتعدّد الضّمانات القانونية الّتي ينبغي أن تقرّر لهذا الحق بحسب ما تفضي إليه تكنّولوجيا الإعلام و الاتصال من معلومات مستقبلا.

و يترتّب على كون التّفتيش الإلكتروني يتضمّن مساسا بالخصوصيّة المعلوماتيّة، فإنّه يخرج عن نطاقه كلّ إجراء لا يمسّ بالخصوصيّة، فالأصل في القانون أنّ الاطلاع على المعلومات مباح متّى لم يتعارض هذا الفعل مع حقّ صاحبه، و من البدّيهي أنّه ما يباح للأفراد الاطلاع عليه يباح للهيئات القضائية أيضا معاينته، لأنّ المعلومات المحوسبة و المكشوفة لا تتمتّع بحرمة خاصّة فهي تفقد هذا الامتّياز القانوني أيّا كانت درجة خصوصيتها، و مثال ذلك إطّلاع سلطة التّحقيق على أخصّ شؤون الحياة الخاصّة للأفراد و المتاحة للجميع عبر مواقع التّواصل الاجتماعي و إن كانت هذه المعلومات مذهلة للغايّة من حيث درجة حرمتها كأصل عام، فإنّ ذلك لا يضفي عليها حماية إجرائية طالما تخلّى صاحب الشّأن عن هذه الحرمة و كشف عن خبيئته.

الفرع الثاني: التّفتيش المادي مقدمة للتّفتيش الإلكتروني

تتميّز مراحل تنفيذ عملية التّفتيش عن الأدّلة المعلوماتيّة في مظاهرها بطابع خاص يضفي عليها طابعا من الذّاتية إذا ما قورنت بخطوات التّفتيش عن الأدّلة المادّيّة، ففي عمليات التّفتيش التّقليدية تحصل الضّبطية القضائية القائمة بالتّفتيش على إذن بالاطلاع على مكان مادي معيّن، بحثا عن دليل مادي ما و هو ما يعرف بآلية التّفتيش ثم الاسترجاع "Mechanism Search-and-Retrieve"[25]، أي الدّخول إلى المسكن و تفتيشه و ضبط الدّليل المادي المحدّد في الإذن القضائي، و هذه الخطوات في تنفيذ عملية التّفتيش تسري على المسكن و الشّخص و مراسلاته، مؤدى ذلك أنّ تنفيذ التّفتيش يتمّ عبر خطوة واحدة و هي أن يكون الضّبط معاصرا للتّفتيش، و هي من المسلمات في فكر الإثبات التّقليدي و تجد لها تنظيما في القانون و استقرارا في التّعامل القضائي معها.

في مقابل ذلك يؤدي تنفيذ الإذن بالتّفتيش عن الدّليل المعلوماتي إلى إضافة خطوة ثانية، إذ تسعى هذه السّلطة للحصول على إذن بالتّفتيش ضمن مساحة مادية يحدّدها و يصفها الإذن القضائي بحثا عن أجهزة التّخزين الرّقميّة (دعامات التّخزين الإلكترونية)، ثم تستحوذ السّلطة الإجرائيّة على هذه الأجهزة الّتي تمّ العثور عليها خلال التّفتيش المادي للتّحليل خارج الموقع"Off-Site" في وقت لاحق، و ذلك ضمن مخابر التّحليل الحاسوبي و هي عملية قد تستغرق عدة أسابيع أو أشهر و هو ما يعرف بآلية الاسترجاع ثم التّفتيش" Retrieve-And-Search Mechanism"[26].

و من هذا المنطلق فإنّ التّفتيش الإلكتروني يتمّ عبر خطوتين"Two-Stage Approach"، تعرف الخطوة الأولى بمرحلة "التّفتيش المادي" (Physical Search Stage)، عندما تدخل السّلطة الإجرائيّة المختصّة بالتّحقيق الموقع المطلوب تفتيشه تسترجع أجهزة التّخزين الرّقميّة المحدّدة في الإذن القضائي و ينصّب الضّبط على الأجهزة الإلكترونية الّتي يُرجح أنّها قد تحتوي على أدلّة ذات صلة بالجريمة موضوع التحقيق، و في معظم الحالات، تقوم هذه السّلطة الإجرائيّة إمّا بإنشاء "نسخة رقمية " للقرص الصّلب "Digital Duplication" أو ضبط الدّعامات المادّيّة، و تُعرّف الخُطوة الثّانية بمرحلة التّفتيش الإلكتروني (Electronic Search Stage) و الّتي تتعلّق بالبحث عن الأدّلة المعلوماتيّة، و الّتي عادة ما تتم بعد فترة طويلة من البحث عن الأدّلة المادّيّة، و يبدو هنا من الواضح أنّ فعالية التّفتيش الإلكتروني تفرض ضرورة التّفتيش المادي أولا يعقبه الضّبط المادي أو الرقمي و يليه التّفتيش الإلكتروني، و هو ما يوضّح حجم التّباين بين "آلية التّفتيش عن الأدّلة المادّيّة" و "آلية استرجاع الأدّلة المعلوماتيّة"[27].

في حين يرى جانب من الفقه أنّه من الخطأ التّفكير في "عملية الاسترداد ثم التّفتيش" كنموذج فريد من نوعه للتّفتيش المعلوماتي، و أنّ معظم عمليات التّفتيش لا تتطلب خروجا عن عملية التّفتيش و الاسترداد المعتادة باستثناء بعض الحالات النّادرة الّتي تختلط فيها الوثائق بحيث لا يمكن تصنيفها عمليا في الموقع، و يقوم هذا النّقد على أن تطبيق هذه القاعدة يجرّ إلى الضّبط الشّامل قبل إجراء التّفتيش على نحو يؤدي إلى انتهاك صارخ لحق المتّهم في الخصوصيّة نتيجة استبقاء سلطة التّحقيق لهذه البيانات بحوزتها[28]، و هو رأي شاذ نخالفه لعدم وجود أي بديل آخر يسمح باسترجاع الدّليل المعلوماتي دون الاستناد إلى هذه القاعدة لسهولة و سرعة تدمير هذا النّوع من الأدّلة، أمّا

بشأن تشابك و اختلاط البيانات فهي من الأمور المسلّم بها في الوقت الرّاهن نتيجة القدرة الهائلة للتّخزين الرّقمي الّذي تتمتّع به الأجهزة الرّقميّة الحديثة زيادة على التّعقيد التّقني الّذي يفرضه المجرم على نظامه المعلوماتي منعا من الوصول إليه.

و قد أبدى القضاء الأمريكي تمسكه بهذه القاعدة مشيرا إلى أنّ خصوصيّة عمليات التّفتيش المعلوماتي تتطلّب اتخاذ "خطوات معاكسة لعمليات التّفتيش التّقليديّة"[29]، إلى غاية تبني هذا الاجتهاد الفقهي بتعديل نص المادة 41 من قانون الإجراءات الجنائية الفيدرالي سنة 2009 تحت وطأة الطّبيعة الفرديّة للأدلّة المعلوماتيّة الّتي اقتضت إتباع هذا النّهج[30]، لأنّه من المتعذّر فحص كلّ البيانات الّتي يحتويها وسيط التّخزين الرّقمي لحظة التّفتيش المادي، خاصة إذا تمّ التّفتيش في مسكن المتّهم و تعدّدت وسائط التّخزين أو شملها التّشفير بحيث تستغرق عملية التّفتيش أوقات طويلة جدا فتتعدّد صور الانتهاك و تزداد خطورة، لأنّه يطال حرمة المسكن و سكينة شاغليه طيلة فترة التّفتيش، فضلا على انتهاك حرمة المعلومات، و لا ريب أنّ هذا الإجراء غير مشروع تماما و لا يحتاج إلى نص يقرّر عدم مشروعيته، و إجمال ما تقدم أنّ تزايد سعة التّخزين الرّقمي تفرض تغيير عملية تنفيذ التّفتيش الإلكتروني من خطوة واحدة إلى خطوتين، مما يجعل تحديث القواعد القانونية حتميّة طبيعية لتغيّر الحقائق الّتي أفقدت التّوازن بين حق المجتمع في مواجهة الجريمة و حق الفرد في صون حريته.

المبحث الثّاني: معيار التّمييز بين التّفتيش الإلكتروني و الضّبط الرّقمي

توصلنا فيما سبق إلى أنّ انتهاك التوقع المعقول للخصوصية المعلوماتيّة قد يقع في مرحلة سابقة على التّفتيش الالكتروني و هي مرحلة الضبط العرضي للبيانات Incidental seizure، و تلك نتيجة تدفعنا إلى بحيث معيار تكييف التّفتيش الإلكتروني، و لا سبيل إلى ذلك إلاّ من خلال بحث معيار التّمييز بين التّفتيش و الضّبط في البيئة الرقمية باعتبار أنّ كليها يشكل تقييدا للحرّية الفردّيّة، و من الطّبيعي أنّ يفرض علينا بحث هذه المسألة الإحاطة علما بمفهوم الضّبط الرقمي (فرع أول)، حتى يتحدّد الأساس الّذي على ضوئه يمكن التّفريق بين الإجراءين (فرع ثاني).

المطلب الأوّل: مدلول الضّبط الرقمي

إنّ تحديد مدلول الضّبط الرقمي (فرع أول) لا يُستكمل إلاّ بتحديد الأساس القانوني الّذي يُبرّر اعتبار نسخ البيانات داخلا في دائرة الضبط، على الرغم من بقاء أجهزة التّخزين الرّقميّة و كذا البيانات الأصلية بحوزة المتّهم (فرع ثاني).

الفرع الأول: تعريف الضّبط الرقمي

يعرّف الضّبط عموما بأنّه إجراء من إجراءات التّحقيق يرمي إلى "وضع اليد على الشّيء و استبقاؤه تحت تصرّف المحقق لمصلحة التّحقيق"، و مصلحة التّحقيق الّتي تبرّر الضّبط هي الإثبات و هو يستوي في ذلك مع غيره من إجراءات جمع الأدّلة و منها التّفتيش[31]، فيتحصّل الضّبط إذن في وضع اليد على ما يصلح "دليلا" أو "قرينة" في الجريمة لتقديمه إلى القضاء، فالمقصود به التّحفظ على الأشياء "المادّيّة" الّتي تشكّل الجريمة أو تكون قد نتجت عنها أو تكون قد وقعت عليها الجريمة و بعبارة أدق التّحفظ على كل ما يفيد في كشف الحقيقة[32].

و هذا المفهوم التّقليدي 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 التّخزين الإلكتروني لأنّ المعلومات لا توجد مستقلة عن وعائها المادي، إلاّ أنّه مع مرور الوقت تبيّن عدم مشروعيته هذا الإجراء إلى حد كبير جدا، نتيجة ما قد ينجم عنه من أضرار عديدة للأفراد بحكم حاجاتهم إلى الأجهزة المادّيّة طيلة فترة الضّبط و خاصة المؤسّسات الاقتصادية إذ ينجرّ عنه شلل لنشاط هذه المؤسّسات.

أمام هذه المعضلة تمّ تبني ممارسة حديثة تتجاوب من واقع التّخزين الرّقمي تقوم على النّسخ الرّقمي للبيانات المستهدفة بالتّفتيش، إذ أنّ معظم عمليات التّفتيش تتمّ من خلال نسخ المواد المخزّنة في نظم المعالجة الآلية للبيانات بقصد تفتيشها لاحقا مع ترك الأجهزة المادّيّة و النّسخة الأصلية للبيانات بحوزة المتّهم، و هو ما يعتبر عنصر من عناصر الموازنة بين فاعلية العدالة الجنائية و احترام الحقوق الفردية[33].

و إجمال ما تقدم أنّ قيام السّلطة الإجرائيّة بالنّسخ الرّقمي لبيانات المتّهم يمثّل "ضبطا"، بحكم أنّ هذا الإجراء يمكّنها من الحصول على نسخة من البيانات الّتي تحتفظ بها لاستعمالها في المستقبل كدليل جنائي و من المؤكد أنّ عرض و استكشاف هذه البيانات المنسوخة يشكّل تفتيشا و لكن الحصول على النّسخة نفسها يخدم الوظيفة التّقليدية الّتي تنظّمها إجراءات الضّبط، فبمقتضى هذا الإجراء يتم تجميد أي معلومات يتمّ نسخها تماما مثل التّحفظ على الممتلكات المادّيّة للمتّهم، فإنشاء 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 الّذي يرجح أن تكون له قيمة إثباتية[34].

غير أنّ هناك فارق بين الضّبط المادي و الضّبط الرّقمي، فالضّبط 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 هذه النّسخ لا يؤدي بالضّرورة إلى إلغاء حيازة المتّهم للنّسخة الخاصة به، بل يبقى متمتّعا بكافة حقوقه على النّسخة الأصلية، و من هنا نتوصّل إلى أنّه يراد بالضّبط الرقمي استبقاء بيانات رقمية قد تفيد في كشف الحقيقة تحت تصرّف سلطة التّحقيق ريثما يتمّ تقديمها للقضاء، و إن كانت هذه القاعدة هي قضائية المنشأ فقد تم تبنتها الاتفاقيات و التّشريعات عموما.

و مثل هذا الأمر لاحظه المشرّع الجزائري فنصّ في المادة 6 من القانون 09-04 المتعلّق بالوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام و مكافحتها "عندما تكتشف السّلطة الّتي تباشر التّفتيش في منظومة معلوماتية معطيات مخزّنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و أنّه ليس من الضّروري حجز كل المنظومة، يتمّ نسخ المعطيات محل البحث و كذا المعطيات اللاّزمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحراز وفقا للقواعد المقرّرة في قانون الإجراءات الجزائية" [35]، و بدورنا لا نماري في أنّ النّسخ الرّقمي إجراء من إجراءات جمع الأدّلة و أنّ التّكييف القانوني السّليم لهذا الإجراء هو الضّبط، غير أنّ السّؤال الّذي يفرض نفسه هنا يتعلّق مضمونه بالاعتبارات

الواقعية أو القانونية الّتي على أساسها يُكيّف النّسخ الرّقمي على أنّه بمثابة "ضبط" طالما أنّ النّسخة الأصلية للبيانات تبقى بحوزة المتّهم بما فيها وسائط التّخزين المادّيّة؟

الفرع الثاني: الأساس القانوني لاعتبار النّسخ الرّقمي بمثابة ضبط

إنّ الجواب على هذا التّساؤل غاية في الأهمية، فهو يحدّد الإطار القانوني الّذي تقوم عليه نظرية التّفتيش الجنائي المعلوماتي، لأنّه لا يتمّ تفتيش نظم المعلومات بغير ضبط رقمي مسبق نهائيا، حتّى و لو افترضنا أنّ الضّبط انصب على الدّعامة المادّيّة لأسباب تقنية كوجود تشفير حال دون الضّبط الرقمي في موضع التّفتيش المادي، فإنّ الغاية من الضّبط المادي في هذه الفروض ذاتها و هي الكيانات المعنوية ممثلة في البيانات و ليست الكيانات المادّيّة على الإطلاق، لذا فإنه من غير المنطقي التّمييز بين "الضّبط المادي للدّعامة الإلكترونية" الّتي تحتوي على البيانات و "الضّبط الرقمي المباشر".

إنّ القضاء الأمريكي ينظر إلى عملية نسخ البيانات على أنّها عملية ضبط تخضع للقواعد الإجرائيّة الاتحادية المنصوص عليها بنص المادة 41 من قانون الإجراءات الجنائية الفيدرالي و كذا مقتضيات التّعديل الدّستوري الرّابع، 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 التّاسعة على "إعادة" نسخ من البيانات الّتي أجريت أثناء تنفيذ عملية التّفتيش إلى أصحابها، و أشارت المحكمة إلى المعلومات على أنّها "بيانات مضبوطة" data seized و "المواد المضبوطة" seized materials[36]، دون أن تبيّن في قضائها الأسباب الّتي حذت بها إلى ما انتهت إليه بهذا الخصوص[37]، و إذا كان القانون أيضا في غيبة من التّعرض لهذه المسألة فإنّ الفقه الانجلوسكسوني قد ذهب مذاهب شتى في معالجة الأساس المعتمد في اعتبار النّسخ الرّقمي بمثابة ضبط و هناك ثلاثة مقاربات فقهية في هذا الموضوع:

الاتجاه الأوّل: الضّبط الرقمي يتعارض مع الحق في الحذف

اقترح بعض الفقهاء أنّ النّسخ الرّقمي ينبغي اعتباره ضبطا لأنّه ينطوي على تعارض مع حق الفرد في "حذف البيانات"The right to delete، فهذا الحق يخوّل للفرد سلطة التّحكم في ملكيته و متابعة ما قد يعتريها بما فيها النّسخ، ومن هذا المنطلق فإنّ الضّبطية القضائية لا يكون بمقدورها تدمير البيانات أو حذفها ما لم تقم بضبطها مسبقا[38].

و هذا التّوجه لا يخلوا من النّقد لأنّ الاعتماد على "الحق في الحذف" كأساس لهذه المقاربة يقيم ضرورة تحديد ما يرتّبه 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 بحذفه أم أنّ هذا الحق قائم فقط حال محاولة سلطة التّحقيق عمل نسخة من الملفات؟[39]، علاوة على ذلك فأيّ معنى يبقى لهذا الحق إذا كانت هذه البيانات مكشوفة للعامة حتّى ولو افترضنا أنّ قصد هذا الفقه يقتصر على البيانات المجرّمة فهذه الأخيرة أيضا قد تتاح لغير صاحب الشّأن بشكل أو بآخر كما هو حال البينات المنشورة على مواقع التواصل الاجتماعي.

الاتجاه الثّاني: الضّبط الرقمي يتعارض مع الحق في الحيازة الحصرية للمعلومات.

أمّا المعيار الثّاني الّذي اعتمده جانب كبير من الفقه فيرجع إلى "الحق في الحيازة الحصرية" من منطلق أن حصول السّلطة القائمة بالتّفتيش على نسخة من بيانات المتّهم يعارض الحق في الحيازة المطلقة للفرد على معلوماته الشّخصية "right to exclusive possession" أي بمعنى آخر استئثاره بهذه المعلومات على نحو يحقّق استبعاد الغير عنها، فعندما تقوم سلطة التّحقيق بنسخ البيانات أو المعلومات الّتي هي في الأصل ليست في حيازتها و غير متاحة لها، فهي تنتزع حقوق استخدام البيانات بشكل حصري عن صاحبها و يصبح لها بذلك سلطة استغلال تلك البيانات، صحيح لا يزال لدى المالك نسخة من البيانات لكن حقه في استبعاد الغير قد تم انتزاعه[40]، و هذا التّفسير اعتمدته الدّائرة الاستئنافية الفيدرالية الثّانية الأمريكي في قضية Ganias v. States United[41].

و يضيف هذا الجانب من الفقه أنّ مفهوم الحيازة المطلقة و الحصرية و الّتي تجعل النّسخ ضبطا يقتصر على النّسخ الدّقيقة فحسب، لأنّ الحق في استبعاد الغير عن البيانات يجب أن يقتصر على النّسخ الدّقيقة و لا يمتد إلى الملخصات باعتبار أنّ درجة التّعارض مع الحيازة الحصرية في هذه الفروض تكون بنسبة أقل[42]، و في ذات السّياق يرى بعض الفقهاء المناصرين لهذا النّهج أنّ إجراء نسخ البيانات على الرّغم من أنّه لا يؤثر على النّسخة الأصلية من البيانات الّتي تبقى بحوزة المالك، فإنّه يحرم هذا الأخير من شيء ذي قيمة و يتداخل مع الاستخدام الحصري لصاحب الشّأن تماما كما هو الحال حين التّعرض لسرقة البيانات[43].

الاتجاه الثّالث: الضّبط الرقمي تجميد للأدلة المعلوماتيّة

أما المقاربة الثّالثة فهي تقوم على منطق بسيط لا يخرج عن حدود منطق الضّبط التّقليدي، فالنّسخ الرّقمي يعتبر بمثابة ضبط لأنّ الوسيلة الإجرائيّة المعروفة بالضّبط في التّعديل الدّستوري الرّابع أو القاعدة التّقليدية بشكل عام، هي ذاتها الوسيلة الإجرائيّة الحديثة الّتي تعرف بـ" التّجميد" The reason is that the Fourth Amendment power to seize is the power to freeze، فالهدف من الضّبط هو السّيطرة و التّحكم في مسرح الجريمة و الأدّلة الّتي 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 المادّيّة إلى تجميدها، فهو يضيف إلى سيطرة سلطة التّحقيق أدلّة لم تكن تحت سيطرتها قبل النّسخ، فإنشاء نسخة إلكترونية لا يختلف كثيراً عن ضبط المنزل أو الخنجر فجميع هذه الأنواع من المضبوطات في نهاية المطاف تضمن سيطرة القائم بالتّحقيق على الشّخص أو المكان أو الأشياء الّتي يرجح أنّها ذات قيمة إثباتية[44].

نحن نرى أنّ النّسخ المعلوماتي ضبطا لأنّه إجراء من إجراءات جمع الأدّلة يرمي إلى المحافظة على مسرح الجريمة و تأمينا له و منع الغير من العبث به، لما قد يوجد عليه من آثار تشكل عنصرا للدّليل المعلوماتي، لا جدال في أنّه قد يتعارض مع حق المتّهم في حذف بياناته و قد يتعارض مع حقه في حيازته المطلقة و الحصرية عليها، لكن في جميع الأحوال يبقى تكييف هذا الإجراء مستمدّ من الغاية منه و هو التّحفظ على كل البيانات الّتي يُعتقد أن تكون مفيدة في كشف الحقيقة، فإنّ كان الضّبط المادي يقيّد حقوق الأفراد المادّيّة على الشّيء الّذي يقع عليه الضّبط، فإنّ الضّبط

الرقمي يقيّد الحق في الحيازة المادّيّة المطلقة للفرد على معلوماته و ينتزع منه حقه في استبعاد الغير من وضع يده عليها أو على نسخة منها.

المطلب الثاني: التّمييز بين التّفتيش الإلكتروني عن الضّبط الرقمي

قد يظهر للوهلة الأولى أنّ تبني المفاهيم التّقليدية للتّفتيش في البيئة الرّقميّة 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 الحرّيّات الفرديّة، الأمر الّذي حذا بالفقه الأمريكي إلى لفت النّظر إلى إشكالية أثارت جدالا خصيبا بين الفقهاء حول معيار التّمييز بين الضّبط و التّفتيش متسائلا عن العمل الّذي يعد منطلقا لوقوع التّفتيش و الحد الفاصل بينهما.

الفرع الأول: الاتجاه المضيق لتكييف التّفتيش الإلكتروني

من السّهل تحديد متى يبدأ التّفتيش المادي (التّقليدي) و متى ينتهي، لأنّ القاعدة الإجرائيّة التّقليدية كانت مبنية دائما على الفرضية المادّيّة لمحل التّفتيش، فتفترض ارتباط هذا الإجراء الجنائي بشيء يشغل حيّزا ذا بُعد مادي، محدّدا بشكل ناف للجهالة سواء كان هذا المحل مسكنا أو شخصا أو مراسلات، إذ يتمّ الشّروع في التّفتيش باستكشاف معلومات حول المحل الّذي جرى تفتيشه، فتحديد اللّحظة الّتي يستهل فيها التّفتيش في إطار هذا النّهج التّقليدي أمر بسيط للغاية، و المعيار المعتمد في ذلك هو تعيين اللّحظة الّتي يحدث فيها انتهاك الخصوصيّة على سبيل المثال فإنّ تفتيش المسكن يحدث في الوقت الّذي يتمّ فيها فتح باب هذا المبنى و ينتهي بمغادرة القائم بالتّفتيش له، و هذه الحقائق هي من البديهيات لدى فكر الإثبات التّقليدي[45].

غير أنّ ترجمة هذا المعيار –القائم على انتهاك التّوقع المعقول للخصوصية كنقطة لانطلاق التّفتيش في البيئة الرّقميّة– يضع المشكلة في إطار عدة افتراضات أخذت شكل اتجاهات في الفقه مؤداها إمكانية حدوث التّفتيش المعلوماتي عند معالجة الحاسوب للبيانات و قراءتها، أو عندما يقوم الحاسوب بإخراج هذه البيانات إلى شاشة العرض أو الطابعة،[46]، أو قد يقع التفتيش عندما مغادرة القائم بالتّفتيش و بحيازته وسيط التّخزين الرقمي، أو عند فقدان المالك القدرة على تغيير و حذف البيانات، أو حال عزل البيانات ذات الصّلة بموضوع التّحقيق عن تلك الّتي لا علاقة لها بالموضوع[47]، أو قد يقع أيضا عند مجرّد الولوج إلى النّظام المعلوماتي و لو انصب الاطلاع فقط على بيانات الملف في شكلها الخام (bit)، أو قد يحصل في الأحوال الّتي يقتصر فيها الاستعراض فقط على بيانات سطحية كحجم الملف أو طبيعته (نصوص أو صور) دون الاطلاع على فحواه.

في ضوء هذه الفروض جميعا يرى جانب بارز من الفقه الأمريكي أنّ الحد الفاصل بين وقوع التّفتيش الإلكتروني من عدمه هو مدى قيام الاطلاع البشري على البيانات المخزّنة، إذ تتمّ عمليات التّفتيش 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 للاطلاع البشري – السّلطة القائمة بالتّفتيش– فإنّه في هذه اللّحظة على وجه التّحديد يحدث التّفتيش الإلكتروني بالمعنى الّذي يريده القانون، و هو ما يسمى بالنّهج القائم على الاستعراض أو الكشف

"exposure-based approach"[48]، فوفقا لهذا الجانب من الفقه إذا لم تخضع البيانات للملاحظة البشرية المباشرة بالعين المجرّدة، فإنّ كافة الإجراءات السّابقة الّتي تتخذها السّلطات الإجرائيّة لا تعتبر تفتيشا.

واقع الأمر نحن لا نؤيّد مطلقا مسلك هذا الجانب من الفقه، لأنّه يقيّد التّكييف القانوني للإجراء بتحقق انتهاك "حق السّر" وفقا لمنظور هذا الحق بمفهوم تقليدي أو مادي و ليس من منطلق المفهوم الواسع "للحرية الفرديّة" و ما يتفرع عنه من حق الفرد في الأمن و السكينة، و محاولة إسقاط هذا المفهوم على التّفتيش المعلوماتي يقودنا إلى القول أنّه عند النّفاذ إلى النّظام المعلوماتي مع استحالة فتح الملفات الّتي يحتويها لا يعدّ بمثابة تفتيش لأنّه لا يتحقّق معه الاطلاع البشري على أيّة معلومات، و نفس الوضع يتحقّق فيما لو تمّ فعلا الولوج إلى القرص الصّلب و تبيّن في نهاية المطاف أنّه خال تماما من أيّ معلومات أو أنّ صاحب الشأن لم يسبق له استعمال ذاكرة الجهاز نهائيا، ألا يعدّ الإجراء في هذه الفروض تفتيشا دقيقا لمستودع السّر، 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 مستمدّة من حرمة الحياة الخاصة لصاحبها، وجب أن لا يقتصر مدلولها على"الحق في السّر" بمفهوم ضيّق فالنّافذ إلى النّظام المعلوماتي يعتبر تدخلا في الحياة الخاصّة أيّا كان محتوى دعامة التّخزين الرّقمية و لو كانت خالية من البيانات أو لم تتضمن أيّة بيانات محرجة أو غير قانونية.

و من مظاهر الدّلالة على التّوسع في تكييف التّفتيش في سياق التّفتيش عن الأدّلة المعلوماتيّة ما يكشف عنه حكم المحكمة العليا ببنسلفانيا في قضية Commonwealth v. Fulton، و الّذي خلصت من خلاله المحكمة إلى أنّ الفعل البسيط المتمثل في تشغيل الهاتف المحمول يشكّل تفتيشا وجب خضوعه للمقتضيات الّتي يفرضها التّعديل الدستوري الرّابع، من منطلق أنّ هذا الاطلاع ينطوي على مساس بالحرية الفرديّة بحكم الكم الهائل من البيانات الشّخصية الموجودة على الجهاز و الّتي تعتبر العامل الحاسم في تحديد التّكييف الصّحيح لهذا الإجراء، و ذكرت المحكمة أنّه لا يوجد فرق بين رصد شاشة العرض الدّاخلية و الخارجية للهاتف المحمول و بين تفتيش سجل المكالمات إذ يؤدي كلا الإجراءين للوصول ليس فقط إلى "مجرّد 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 المعيّن للمتصل أو مرسل الرّسالة النّصية[49].

الفرع الثاني: الاتجاه الموسع لتكيف التّفتيش الإلكتروني

و هناك اتجاه فقهي سلك مسلك التّوسع المبالغ فيه، مدفوعا باعتبارات واقعية تبرّر عدم انطباق المفاهيم القانونية التّقليدية على المستجدات الّتي أفرزتها الثّورة الرّقميّة، فيرى هذا الاتجاه أنّ التّفتيش إجراء استثنائي يقيّد حقا فرديا هو الحق في الخصوصيّة، أمّا الضّبط فهو يقيّد حقا فرديا ماليا على الشّيء محل الضّبط كحق الملكية و الحيازة لما فيه من تعطيل لحق المالك في استعمال ملكيته، إلاّ أنّ ترجمة هذا المفهوم في البيئة الرّقميّة يجعل نسخ الملفات– الّتي درج القضاء الأمريكي على اعتباره يدخل في خانة الضّبط– هو بمثابة تفتيش، لأنّ الحق الّذي يقيّده الضّبط المعلوماتي لا يقتصر على حق الملكية طالما أنّ الأجهزة الرّقميّة و كذا النّسخة الأصلية من البيانات المضبوطة تبقى بحوزة المالك، بل يمتد هذا التّقييد إلى الحق في الخصوصيّة و حرمة البيانات الّتي وقع عليها الضّبط[50].

و تدعيما لموقفه يرى هذا الجانب من الفقه أنّه إذا ما اعتبرنا أنّ الخصوصيّة تقوم على السّرية و استقلال الفرد بأسراره فإنّ هذه الحقوق تصبح عرضة للخطر متى تم النّسخ الرّقمي، و يستند في دعم موقفه إلى أحكام قضائية عديدة اعترفت بوضوح بخطر الضّبط المعلوماتي على الحق في السّرية[51]، مبرّرا موقفه بحجة أخرى مؤداها أنّ حصول الحكومة على نسخة من بياناته الشّخصية يناقض حق الفرد في استقلاليته بأسراره المعلوماتيّة، بحيث يزداد هذا الانتهاك كلما تواصل الضّبط من حيث النّطاق الزّماني، بدليل ذلك التّوجس السّائد لدى الأفراد خيفة من إطلاع الحكومة على محتوى المضبوطات الّتي في حيازتها، لذا من الطّبيعي في نظره اعتبار الضّبط في هذه الحالة بمثابة تفتيش لانطوائه على تقييد لحق شخصي.

في الحقيقة إنّ هذه الحجة لقيت صداها لدى القضاء الأمريكي الّذي بات يعترف بخطر الضّبط المعلوماتي على الحرّيّات الفرديّة، و من تطبيقات ذلك ما قضت به المحكمة الابتدائية لمنطقة كولومبيا في قضية Klayman v Obama أين خلصت إلى أنّ مجرّد عملية "جمع البيانات الوصفية" تشكّل تفتيشا، و أمرت الحكومة ليس فقط بوقف عملية تحليل البيانات، بل و محوّ مجمل المعلومات الّتي في حيازتها[52]، بيدا أنّ معظم الاتجاهات القضائية و إن اعترفت مؤخرا بخطر الضّبط المعلوماتي على الحق في الخصوصيّة إلاّ أنّ القضاء الأمريكي لم يتراجع عن سوابقه في هذا الشّأن.

و من هنا يبدو جليا أنّ طبيعة البيانات الرّقميّة قد أضفت نوعا من الغموض على الحدود الفاصلة بين الضّبط و التّفتيش إذا لم تؤدي في الحقيقة إلى طمسها بشكل كلي، و في تقديرنا ينبغي التّسليم بكون كل من الضّبط و التّفتيش في البيئة المعلوماتيّة يقيّدان حقا شخصيا هو الحق في الخصوصيّة من منطلق ما تتمتّع به المعلومات من حرمة تجاوزت بكثير حرمة المساكن و المراسلات التّقليدية[53]، غير أنّهما يختلفان في درجة هذا التّقييد، فبينما يمثّل الضّبط المعلوماتي مجرّد تهديد لهذا الحق، فإنّ التّفتيش المعلوماتي يتعدى ذلك إلى درجة أخطر و هو انتهاك هذا الحق.

و لو تأمّلنا جيدا نص المادة 19 من الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتيّة و الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتيّة، لوجدنا أنّ دلالتها تقطع بكون المعيار الفاصل بين وقوع التّفتيش من عدمه هو "النّفاذ إلى النّظام المعلوماتي"، و قد عبّرت عن ذلك صراحة في قولها "تلتزم كلّ دولة طرف بتبني الإجراءات الضّرورية لتمكين سلطاتها المختصّة من **التّفتيش أو النّفاذ**" إلى النّظام المعلوماتي perquisitionner ou à accéder d'une façon similaire[54]، و نلمس ذات التّوجه لدى المشرّع الفرنسي ذلك أنّ مدلول عبارات نص المادة 57 فقرة أولى من قانون الإجراءات الجزائية كانت واضحة، و اعتبرت أنّ التّفتيش يقع بمجرّد النّفاذ و الولوج إلى النّظام المعلوماتي[55]، أمّا بالنّسبة إلى التّشريع الجزائري فالملاحظ أنّ صياغة النّص في نسخته العربية لا تعكس نية و إرادة المشرّع، حيث نصّت المادة 5 من القانون الجزائري 09/04 على أنّه "يجوز للسّلطات القضائية المختصّة و كذا ضباط الشّرطة القضائية المختصّة في إطار قانون الإجراءات الجزائية ... الدّخول بغرض التّفتيش و لو عن بعد، إلى: (أ) منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتيّة المخزّنة فيها.(ب) منظومة تخزين معلوماتية..."[56].

إذ المستفاد من هذا النّص أنّ النّفاذ إلى النّظام المعلوماتي إجراء تقني مستقل عن التّفتيش، أي بمثابة إجراء يسبق وقوع التّفتيش و من مستلزماته، يقتصر المقصود منه على الوصول إلى محل التّفتيش (البيئة المعلوماتيّة)، أمّا التّفتيش بالمعنى

القانوني فيراد به وسيلة لجمع الأدّلة يتمّ من خلالها الاطلاع على هذه المعلومات باعتبارها محلا له حرمة الأسرار، و هذا التّفسير ينطوي في حقيقته على قدر من التّجاوز في فهم جوهر "قاعدة الحرمة" إذ لا يقف مدلولها على "الحق في السّر"، بل كل ما يحيط "بأمن الفرد و هدوئه و استقلاله ببياناته"، فيتحقّق التّفتيش متى طال محلا له حرمة خاصة و لو لم يفض إلى الاطلاع على أي شيء معاقب عليه، إذ لو أجزنا حكم نص المادة 5 المشار إليها أعلاه لأصبح النّفاذ إلى النّظام المعلوماتي طليقا من غير أيّ قيد على السّلطة الإجرائيّة و يصبح حينئذ من العبث الحديث عن الحرّية الفرديّة، و موقفنا هذا يجد له تأييدا في حكم هذا النص في نسخته باللغة الفرنسية، فالنّص الإجرائي العربي بصيغته الحالية مخالف لمقتضى المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[57]، لذا يتعيّن إعادة صياغته على نحو يوسع من مفهوم التّفتيش المعلوماتي الّذي يراد به في نظرنا " النّفاذ إلى النّظام المعلوماتي بحثا عن عناصر الحقيقة".

و من التّطبيقات القضائية الحديثة الّتي تؤكد التّفسير الّذي توصلنا إليه، ما يكشف عنه الحكم الحديث الصّادر عن المحكمة العليا الفيدرالية الأمريكية في قضية Carpenter v. United States الّتي توصّلت إلى "أنّ المعلومات المتعلّقة بالتّحديد الجغرافي لموقع المتّهم الّتي تمّ الحصول عليها من خلال سجلات شركات الاتصالات اللاّسلكية كانت نتاج عملية تفتيش"[58]، و في تعليقه على هذا الحكم يرى الفقه أنّ التّفتيش قد وقع في مرحلة من مراحل العملية بحيث يمكن القول أنّ التّفتيش تسبب في الحصول على المعلومات، و أنّ المهم وفق نظر المحكمة هو "النّتيجة" و ليست "العملية" أي يحدث التّفتيش بمجرّد الحصول على المعلومات[59].

غير أنّ هذا الحكم من جهة أخرى يكتنفه الكثير من الغموض و يطرح تساؤلا عميقا مؤداه هل يقع التّفتيش عند "الحصول على المعلومات" أو عند "النّفاذ إلى المعلومات"؟

حقيقة الأمر أنّ أجابت المحكمة بكلتا الفرضيتين، ففي نظر المحكمة فإنّ التّفتيش المعلوماتي يحدث عند النّفاذ إلى سجلات موقع الهاتف access to cell-site، و يظهر ذلك بجلاء في بعض أشطر الحكم على سبيل المثال نذكر منها قول المحكمة[60]: "تعرض هذه الحالة السّؤال عما إذا كانت الحكومة تجري تفتيشا بموجب التّعديل الدّستوري الرّابع عندما تقوم بالنّفاذ إلى سجلات الهاتف المحمول الّتي تتيح حقائق شاملة لتحركات المستخدم في تاريخ سابق"، "السّماح للحكومة بالنّفاذ إلى هذه السّجلات يتعارض مع التّوقع المعقول للحق في الخصوصيّة"، "بمجرّد نقرة زر، يمكن للحكومة النفاذ إلى مستودع من معلومات المتعلقة بالموقع الجغرافي دون أي تكاليف تقريبًا"، "وبناءً عليه، عندما تمكنت الحكومة من النّفاذ إلى هذه السّجلات، انتهكت توقعات المتّهم المعقولة بالخصوصيّة في جميع تنقلاته"، "نحن نرفض منح الدّولة سلطة النّفاذ غير المقيّد إلى قاعدة بيانات شركة الاتصالات اللاّسلكية الخاصة بمعلومات الموقع الفعلي".

و على نقيض ذلك اعتبرت المحكمة في شطر لآخر من الحكم أنّه بمجرّد حصول سلطة التّحقيق على المعلومات يكون التّفتيش واقعا دون حاجة إلى النّفاذ إلى هذه السّجلات و استطلاع محتوياتها و يستفاد ذلك من قول المحكمة[61]: "تتضمّن القضية المعروضة علينا استحواذ الحكومة على سجلات موقع الهاتف اللاّسلكي الّتي تكشف عن موقع المتّهم وقت إجراء أو تلقي مكالمات"، "كان استحواذ الحكومة على سجلات موقع الهاتف بمثابة تفتيش بالمعنى المقصود بمقتضى التّعديل الدّستوري الرابع "، "بعد أن وجدنا أنّ الاستحواذ على سجلات موقع الهاتف يشكّل عملية تفتيش

نستنتج أيضًا أنّ الحكومة يجب أن تحصل عمومًا على إذن بناء على أسباب محتملة قبل الحصول على مثل هذه السجلات"،"كان حصول الحكومة على سجلات موقع الهاتف هنا عبارة عن تفتيش بموجب التّعديل الدّستوري الرابع"، "قبل إجبار شركة الاتصالات اللاّسلكية على تسليم سجلات موقع الهاتف الخاصة بالمشترك، يكون التزام الحكومة قائما بوجوب الحصول مسبقا على إذن قضائي".

و بمعزل عن هذا التّعارض الّذي شاب الحكم، فمع التّسليم جدلا بكون الحصول أو ضبط النّظام المعلوماتي لا يشكل تفتيشا في اعتقادنا، فإنّه على خلاف ذلك يعتبر مجرّد النّفاذ إليه تفتيشا بالمعنى الّذي يريده القانون و لو لم يتم استعراض المحتوى المعلوماتي الّذي تضمّنه، و هذه الإشكالية لم تطرح في البيئة المادّيّة لسبب بسيط يجد أساسه في كون الضّبط كان دوما أثرا للتّفتيش، أي يجري لاحقا للمساس بالسّر، فضبط شيء في المسكن يوجب دخوله و تفتيشه، و عند محاولة تطبيق هذا النّهج على التّفتيش المعلوماتي نصطدم بحقيقة فرضتها التّقنية و هي لزوم وقوع الضّبط أولا قبل التّفتيش، و هو ما يقودنا إلى القول بأن التّفتيش الإلكتروني يحتاج إلى تنظيم خاص حتى يتفاعل هذا الإجراء مع البيئة الرّقميّة التزاما بالشّرعيّة الإجرائيّة.

الخاتمة:

من خلال ما سبق نستطيع أن نخلص إلى عدّة ملاحظات ختامية و توصيات حول جزئية تعالج أوّل لبنة في نظرية التّفتيش الإلكتروني نجملها فيما يلي :

أولا: النتائج

1. يعتبر أمن الفرد في نظامه المعلوماتي من أقوى مظاهر الحماية الاجتماعية الّتي يجب أن تُكفل له، باعتباره المستودع الطبيعي الّذي يغلب أن يحفظ الإنسان فيه أسراره، و قد استقر في ضمير الجماعة تمتّعه بقدر من الحرمة تتجاوز المفهوم الرّاسخ لخصوصية المساكن و غرف النّوم، و هو ما يجعل تفتيشه من أخطر الإجراءات تهديدا للحرّيات الفرديّة.
2. إذا كان مفهوم التّفتيش التقليدي يقوم على معيار الاطلاع على محل يتمتع بالحرمة بهدف ضبط ما يفيد في كشف الحقيقة، فإنّ هذا المعيار بات محل جدال فقهي و قضائي خصيب بعد أن أصبح مجرّد ضبط النظام المعلوماتي يشكل تقييد للحق في الخصوصيّة و لو لم يتم الاطلاع على البيانات الّتي يخزنها، و يزداد هذا التهديد ضراوة كلّما طال أمد الضبط من حيث النطاق الزماني.
3. إذا كان الضّبط في البيئة المادّيّة يُقيّد حقوق الأفراد المادّيّة على الشّيء الّذي يقع عليه الضّبط، فإنّ الضّبط الرقمي يقيّد الحق في الحيازة المادّيّة المطلقة للفرد على معلوماته و ينتزع منه حقه في استثناء الغير من وضع يده عليها أو على نسخة منها، و هو ما يجعل الضّبط الرّقمي ينطوي على تهديد للحق في الخصوصيّة و ليس الملكية.
4. تقوم نظرية التّفتيش التقليدي على مبدأ عتيد يقوم على خطوة واحدة يعرف بـ"آلية التّفتيش ثم الاسترداد"، على خلاف الواقع الّذي فرضته ظاهرة اختلاط البيانات و تعذر فرزها في موقع التّفتيش المادّي و الّتي توجب اعتماد آلية

"الاسترداد ثم التّفتيش"، و لا سبيل إلى ذلك إلا بالتّفتيش عن أجهزة التّخزين الرّقميّة قبل تفتيشها، فالتّفتيش المادي مقدمة ضرورية للتفتيش الإلكتروني.

5. لا توجد معالم واضحة فاصلة بين التّفتيش و الضبط في البيئة الرّقميّة، ففي الأحوال الّتي تعجز فيها السلطة الإجرائيّة عن الولوج إلى النظام المعلوماتي بسبب وجود نظام التشفير، يظل التّساؤل قائما فيما إذا كان التّفتيش قد وقع فعلا أم أنّ العمل الاجرائي ظل في هذا النطاق الضبط الرقمي.

6. يعتبر النّسخ الرقمي ضبطا لأنّه إجراء من إجراءات جمع الأدّلة يرمي إلى المحافظة على مسرح الجريمة و تأمينا له و منع الغير من العبث به، قد يتعارض مع حق المتّهم في حذف بياناته، و قد يتعارض مع حقه في حيازته المطلقة على بياناته، لكن يبقى تكييف هذا الإجراء مستمد من الغاية منه و هو التّحفظ على البيانات الّتي لها قيمة إثباتية محتملة.

ثانيا: التوصيات

1-التزاما بالمفهوم السليم و التّكييف الصحيح لإجراء التّفتيش الإلكتروني يحسن بالمشرع إعادة صياغة الفقرة 1 من المادة 5 من القانون 29-04 المتعلّق بالوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام و مكافحتها على النحو التالي "يجوز للسّلطات القضائية المختصّة و كذا ضباط الشّرطة القضائية المختصّة في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عليها في المادة 4 أعلاه التفتيش أو الولوج و لو عن بعد..".

2-دعوة المشرع إلى إعادة تنظيم مراحل تنفيذ التّفتيش الإلكتروني من خطوة واحدة تقوم على "آلية التّفتيش ثم الاسترجاع" إلى خطوتين تعرف الخطوة الأولى بمرحلة التفتيش المادي و تعرّف الخطوة الثّانية بمرحلة التّفتيش المعلوماتي أي اعتماد "آلية الاسترجاع ثم التفتيش".

3- ضرورة تخويل جهات التحقيق المختصة سلطة الضبط العرضي الأولي لبيانات المتهم قبل تفيشها، و إلا كانت سلطة التّفتيش عبثا لا جدوى منها لاستحالة اجراء التّفتيش الإلكتروني في موقع التّفتيش المادي.

4-نهيب بالمشرع الجزائري على ضرورة إرساء معيار يحدد من خلاله بشكل جلي متى تبدأ إجراءات تنفيذ التّفتيش الإلكتروني و متى تنتهي، على نحو يراعي فكرة ذاتيّة هذا الاجراء الجزائي بشكل كامل بما يضع فاصلا واضح المعالم بينه و بين ما يلتبس به من إجراءات في البيئة الرّقميّة.

قائمة المراجع :

أوّلا: المراجع باللغة العربية:

I.النصوص القانونية:

- **الإتفاقيات الدولية:**

1.الإتفاقية الأوروبية لمكافحة الجرائم المعلوماتية و المسماة "بإتفاقية بودابست" الّتي تمّ إعتمادها و تقريرها التّفسيري من لدن لجنة وزراء مجلس أوروبا في دورتها التّاسعة بعد المائة (8 نوفمبر 2001) و فتح باب التّوقيع على الإتفاقية في بودابست المجرية في 23 نوفمبر 2001 بمناسبة المؤتمر الدّولي حول الجريمة الإلكترونية.

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

- **الدساتير:**

1.التعديل الدستوري لسنة 2016، الصادر بموجب القانون رقم 16-01 مؤرخ في 6 مارس 2016، الجريدة الرسمية عدد 14، بتاريخ 7 مارس 2016.

- **القوانين:**

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

3.القانون الجزائري رقم 09-04 المؤرخ في 5 أوت 2009 المتضمّن القواعد الخاصة للوقاية من الجرائم المتصّلة بتكنولوجيا الإعلام و الاتصال و مكافحتها الجريدة الرّسمية عدد 47، بتاريخ 16 أوت 2009.

II.الكتب:

1.توفيق محمد الشّاوي، حرمة الحياة الخاصّة و نظرية التّفتيش، الطّبعة الأولى، منشأة المعارف، مصر، 2006.

2.سامي حسني الحسيني، النّظرية العامة للتّفتيش في القانون المصري و المقارن، الطّبعة الأولى، دار النهضة العربية، مصر، 1972.

3.علي حسن محمد الطوالبة، التّفتيش الجنائي على نظم الحاسوب و الأنترنت دراسة مقارنة، الطبعة الأولى، عالم الكتاب الحديث أربد، الأردن، 2004.

4.محمود محمد محمود جابر، الأحكام الإجرائية للجرائم النّاشئة عن استخدام الهواتف النقال، بدون رقم الطّبعة، المكتب الجامعي الحديث، مصر، 2018.

III.المقالات:

1.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 ص 177-225.

IV. الرسائل الجامعية:

1. عمر محمد أبو بكر بن يونس، الجرائم النّاشئة عن استخدام الأنترنت، رسالة دكتوراه، جامعة عين شمس، مصر، 2004.

ثانيا: المراجع باللغة الإنجليزية:

I. Articles:

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.p.49-94

2.James T. Stinsman, computer seizures and searches rethinking the application of the plain view doctrine, Temple Law Review, Vol. 83, (2011), p.p.1097-1120.

3.Josh Goldfoot, The Physical Computer and the Fourth Amendment, Berkeley J. Crim. L. Vol 16, Issue 1, (2011), p.p.112-167.

4.Mark Taticchi, Note, Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures, Geo Wash L Rev, Volume 78, (2010), p.p.476-511.

5.Note: «Digital Duplications and the Fourth Amendment», HARV. L. REV. Vol. 129, (2016), p.p.1046-1076.

6.Orin S. Kerr, Fourth Amendment Seizures of Computer Data, Yale Law Journal, Vol. 119, Issue 4, (2010), p.p.701-724.

7.Orin S. Kerr, Search Warrants in an Era of Digital Evidence, Mississippi Law Journal, Vol 75, Issue 1, (2005), p.p.85-145.

8.Orin S. Kerr, Searches and Seizures in a Digital World, Harvard Law Review, Vol 119, Issue 2, (2005), p.p.531-585.

9.Paul Ohm, the Fourth Amendment Right to Delete, Harvard Journal of Law. Vol 119, (2005), p.p.13-17.

10. Recent Case Fourth Amendment search and seizure and evidence retention Second Circuit Creates a Potential "Right to Deletion" of Imaged Hard Drives .United States v. Ganias, 755 F.3d 125 (2d Cir. 2014) Harvard Law Review: Volume 128, Number 2, (2014), p.p. 743-750.

11. Susan W. Brenner & Barbara A. Frederiksen, Computer Searches and Seizures: Some Unresolved Issues, Michigan Telecommunications and Technology Law Review, Vol. 8, Issue 39, (2002), p.p.93-114.

A.Jurisprudences :

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

2.In re Search of 3817 W. West End, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004)

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

4.Smith v. Maryland, 442 U.S. 735, 739–40 (1979)

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

6.United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007)

7.United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010).

8.United States v. Galpin, 720 F.3d 436, 446 (2d Cir. 2013)

9.United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001)

10. United States v. Gourde, 440 F.3d 1065, 1077 (9th Cir 2006).

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

12. United States v. Payton, 573 F.3d 859, 861-62 (9th Cir. 2009).

ثالثا: المراجع باللغة الفرنسية:

I.Les dictionnaires:

1.Thierry Debard, Lexique des termes juridiques 2017-2018, 25e éd, Dalloz, France, 2018.

II.Les Codes et les Lois:

1. la Loi française n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, JORF n°129 du 5 juin 2003.

III.Les ouvrages :

1.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.

2.Catherine Forget, La collecte de preuves informatiques en matière pénale, in Pas de droit sans Technologie (dir. JF Henrotte et F Jongen), CUP, Larcier, Bruxelles, 2015.

IV.Les Articles :

1. Larguier Jean, Larguier 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.p.95-161.

2. Lorena Bachmaier Winter, Section III – Procédure pénale. Societé de l'information et droit pénal. Rapport Général, Revue internationale de droit pénal, Vol 85, N 1, (2014), p.p.15-74.

3. Olivier Decima, les investigations numériques en procédure pénale francais: du piratage informatique aux réquisitions et saisie numériques ? Revue la faculté de droit, université de Galatasaray, N 1, (2017), p.p.3-10.

V.Les Documents Internationaux:

1. 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, p.p.1-64.

VI.*La Jurisprudence:*

1. Cass crim. 26fivr 2014, N° 13-87.065, Bull. Crim. N°61.

2. CEDH, arrêt S. et Marper c. Royaume Uni, 4 décembre 2008nos 30562/04 et 30566/04, §67.

([1]) يثير موضوع مفهوم التفتيش الإلكتروني كإجراء جنائي لتحصيل الدليل المعلوماتي عدة قضايا معقدة و شائكة تفيض عن حدود دراستنا، و يضيق المقام عن مناقشتها بإسهاب، لذا سنركز هنا على مفهوم هذا الإجراء بالمعني القانوني، أمّا بالنسبة لتكييف التفتيش وفق موضوعه (مستهدفه)، أو امتداده فتلك مسائل تحتاج إلى دراسات مستقلة هي موضوع الأجزاء الأخرى من البحث، و إن كانت في الأصل لا تنعق من المقاربة القائمة على ارتباط التكييف بالمفهوم، إلا أنّ هناك اجتهادات قضائية ترى خلاف ذلك و لها من الوجاهة ما يتطلب معالجتها بالتحليل و النقد بإسهاب.

(2) سامي حسني الحسيني، النّظرية العامة للتّفتيش في القانون المصري و المقارن، الطّبعة الأولى، دار النهضة العربية، مصر، 1972، ص 37.

(3) توفيق محمد الشّاوي، حرمة الحياة الخاصّة و نظرية التّفتيش، الطّبعة الأولى، منشأة المعارف، مصر، 2006، ص 28.

(4) Serge Guinchard, Thierry Debard, Lexique des termes juridiques 2017-2018, 25e éd, Dalloz, France, 2018, terme « perquisition ».

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

(6) Cass crim. 26fivr 2014, N° 13-87.065 Bull. Crim. N°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 ".

(7) 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."

(8) عمر محمد أبو بكر بن يونس، الجرائم النّاشئة عن استخدام الأنترنت، رسالة دكتوراه، جامعة عين شمس، مصر، 2004، ص 852.

(9) Lorena Bachmaier Winter, « Section III – Procédure pénale. Société de l'information et droit pénal. Rapport Général », Revue internationale de droit pénal 2014/1 (Vol. 85), p 20.

(10) 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, 2017/1, p 3.

(11) Catherine Forget, La collecte de preuves informatiques en matière pénale, in Pas de droit sans Technologie (dir. JF Henrotte et F Jongen), CUP, Larcier, Bruxelles, 2015, p 253.

(12) 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.

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

(14) عند محاولة مواءمة القوانين الإجرائية التّقليدية مع البيئة التّكنولوجية الجديدة، نشأت مسألة المصطلحات المناسبة و شملت الخيارات الإبقاء على اللّغة التّقليدية " التّفتيش "و" الضّبط "، أو استخدام مصطلحات حاسوبية جديدة وأكثر توجها من النّاحية التّكنولوجية " النّفاذ "و" النّسخ"، بصيغتها المعتمدة في نصوص المنتديات الدولية الأخرى بشأن هذا الموضوع مثل الفريق الفرعي المعني بجرائم التكنولوجيا العالية التابع لمجموعة الثّمانية، أو استعمال حل وسط يتمثل في لغة مختلطة " التّفتيش أو النّفاذ بطريقة مماثلة"، و" الضّبط أو التّأمين بطريقة مماثلة"، ولما كانت هناك حاجة إلى تجسيد تطور المفاهيم في البيئة الإلكترونية، فضلا عن تحديد جذورها التّقليدية والحفاظ عليها، تم تبني مقاربة مرنة تتيح استخدام المفاهيم التقليدية " التّفتيش و الضّبط" أو المفاهيم الجديدة " الولوج و النّسخ " ضمن اتفاقية مجلس أوروبا حول الجرائم السيبرانية (إتفاقية بودابست).

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.

(15) علي حسن محمد الطوالبة، التّفتيش الجنائي على نظم الحاسوب و الأنترنت دراسة مقارنة، الطبعة الأولى، عالم الكتاب الحديث أربد، الأردن، 2004، ص 28.

(16) سامي حسني الحسيني، المرجع السّابق، ص ص 40-41.

(17) توفيق محمد الشّاوي، المرجع السّابق، ص 125.

(18) Larguier Jean, Larguier 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, p149.

(19) هذا الحق أصبح يتمتّع بالحماية الدّستورية إذ تنص المادة 46 من الدّستور الجزائري المعدل بالقانون رقم 16-01 المؤرخ في 06 مارس 2016، الجريدة الرّسمية رقم 14، المؤرخة في 7 مارس 2016:

"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 معلّل من السّلطة القضائية، و يعاقب القانون على انتهاك هذا الحكم.

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

(20)United States v. Galpin, 720 F.3d 436, 446 (2d Cir. 2013) (″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.″)

(21) و قد ورد تسبيبا لحكم الدّائرة الاستئنافية قولها " تكمن الأهمّية هنا في أنّ معظم النّاس يعتبرون أجهزة الحاسوب خاصتهم هي مساحة أسرارهم، يتعامل النّاس عادة مع غرف النّوم كمكان خاص جداً، ولكن عند أيّ حفلة، ستجد كل الضّيوف – حتّى الغريب منهم – مدعوون إلى غرفتك حتى أنّهم يضعون معاطفهم على السّرير. لكن ما إن يحاول أحد الضّيوف استكشاف الحاسوب الخاص بالمضيف، فستكون هذه آخر دعوة يتلقاها".

United States v. Gourde, 440 F.3d 1065, 1077 (9th Cir 2006). "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."

(22) United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007) (“Apersonal 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.”

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

(24) و في سياق مقارب يشير الفقه إلى أنّ الطّوفان التّكنولوجي على اختلاف أنواعه جعل العالم أشبه «بالثّوب الشّفاف»، إذ كشف العموميات والخصوصيات، فكان محقاً الكاتب الأمريكي (آرثر ميللر)، حينما قال: «بأنّ الكمبيوتر، المتميّز بشراهته الّتي لا تشبع للمعلومات، وقدرته على عدم الخطأ أو إمكانية نسيان أي شيء، قد يصبح القلب النّابض لنظام رقابة فعّال، يحوّل مجتمعنا إلى عالم شفاف، ترقد فيه بيوتنا و معلوماتنا المالية و اجتماعاتنا، و حالتنا العقلية و النّفسية و الجسمانية كذلك، عارية تماماً، 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.

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

(26) Orin S. Kerr, Loc.Cit.

(27) Orin S. Kerr, op cit, p 91. (“The dynamic is physical search, physical seizure, and then electronic search”).

(28) James T. Stinsman, computer seizures and searches rethinking the application of the plain view doctrine, Temple Law Review, Vol 83, (2011) , p 1100.

(29) 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”).

(30) Berman Emily, Digital Searches, the Fourth Amendment, and the Magistrates' Revolt, Emory Law Journal, Emory University School of Law, Vol 68, Issue 1, 2018, pp 52 et ss.

(31) توفيق محمد الشّاوي، المرجع السّابق، ص41.

(32) سامي حسن الحسيني، المرجع السّابق، ص 303.

(33) يجب التّنويه في هذا الصدد على المصطلحات القانونية المستعملة، و الّتي لم نجد لها استعمالا لدى الفقه عموما سواء العربي أو المقارن، فقد فضلنا اطلاق لفظ "الضبط الرقمي" على المرحلة التي تسبق التّفتيش، لأنّ الحجز هنا عرضي يسبق الاطلاع على البيانات، فالنسخ الكلي هو المقابل الحقيقي لفكرة البيانات،

أمّا الضبط النهائي للدليل و الذي يأتي في مرحلة لاحقة عن التّفتيش الإلكتروني هو "ضبط معلوماتي" لمجموعة من البيانات المحددة الّتي تشكل مستهدف هذا الإجراء، لذلك فإنّ المفارقة بين الإثنين تعدّ قائمة حقا إذا تأمّلنا دور كل منهما.

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

(35) القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمّن القواعد الخاصة للوقاية من الجرائم المتصّلة بتكنولوجيا الإعلام و الاتصال و مكافحتها الجريدة الرّسمية عدد 47، بتاريخ 16 أوت 2009.

See United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001) (holding that copying computer files was not a seizure because it did not interfere with the owner's ability to access the information).

(36)United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010).

(37) هناك اتجاه قضائي يرى خلاف ذلك، ففي سنة 2001 و في قضية United States v. Gorshkov تناولت المحكمة المحلية في الولايات المتحدة للمنطقة الغربية من واشنطن قضية النسخ الرقمي للمعلومات، و كان مكتب التحقيقات الفيدرالي قد حصل على كلمة السر للمشتبه به من خلال عملية سرية، ثم استخدم كلمة المرور من أجل الوصول عن بعد لخادم المشتبه به و لأنهم يخشون من أن يقوم شركاء المشتبه فيه بحذف المعلومات الموجودة على الخادم، قام مكتب التحقيقات الفيدرالي بنسخ المعلومات عن بعد دون الحصول مسبقا على اذن قضائي بالضبط، أين قضت المحكمة بأنّ هذا العمل الإجرائي لا يشكل ضبطا، مُشيرة إلى أنّ النسخ عن بعد لم يكن له أي أثر على الحق في الحيازة لأنّه لم يمنع الغير من الوصول إلى تلك البيانات.

See United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001) (holding that copying computer files was not a seizure because it did not interfere with the owner's ability to access the information).

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

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

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

(41) في سنة 2014، و في قضية United States v. Ganias اعتمدت الدّائرة الاستئنافية الثّالثة أساس "الحق في الحيازة الحصرية". و في تنفيذ إذن بالتّفتيش المعلوماتي لجهاز كمبيوتر خاص بمحاسب للحصول على أدلّة على احتيال العملاء المحتملين، قام المحقّقون بنسخ ثلاثة محركات أقراص صلبة، و الّتي تضمّنت أيضا الملفات الرّقمية الخاصة بالمحاسب و بعد عامين و نصف العام، حصل المحقّقون على إذن ثان تفتيشا عن تلك الملفات نفسها لدليل على تورط المحاسب نفسه في جريمة منفصلة تماما و قال المحاسب بصفته متهما، إنّ الاحتفاظ المطول لملفاته الرّقمية الّتي لا تستجيب للإذن الأول يشكّل ضبطا غير معقول و وافقت الدّائرة الثّانية على أنّ المصالح الحيازة للمدعى عليه تشمل "السّيطرة الحصرية على ملفاته" و أنّ الاحتفاظ الحكومي بالنّسخة المكرّرة تتدخل بصورة مجدية في تلك المصلحة، و من ثم فهذا التّصرف يشكّل ضبطا و لأن الحكومة احتفظت بتلك البيانات لفترة طويلة دون مبرّر كاف، فإنّ الضّبط كان غير معقول و لم تحدد المحكمة عند أي نقطة تجاوز الضبط نطاق " المعقولية" أو "المشروعية"، و لاحظت أنّ الحكومة قد تكون لها مصلحة مشروعة في الاحتفاظ بالبيانات، مثل المصادقة على القرص الصلب (أصالة الدّليل المعلوماتي) إلا أنّها أكّدت على "الفترة الطويلة" الّتي احتفظت بها الحكومة بالبيانات جعلت الضّبط غير معقول و استجابت لطلب الحذف المعجل.

لمزيد من التفصيل راجع 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. Ganias, 755 F.3d 125 (2d Cir. 2014) Harvard Law Review: Volume 128, Number 2, 2014, p p743-750.

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

(43)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.").

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

(45) و هذا المعيار المادي تضمنته المادة 44 من قانون الإجراءات الجزائية و هو ما نستشفه من عبارة "لا يجوز لضباط الشّرطة القضائية الانتقال إلى مساكن الأشخاص ...مع وجوب الاستظهار بهذا الأمر **قبل الدّخول إلى المنزل والشّروع في التّفتيش**".

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

(47) Josh Goldfoot, The Physical Computer and the Fourth Amendment, Berkeley J. Crim. L. Vol 16, Issue 1, (2011), p 133.

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

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

(50) لمزيد من التّفصيلات بشأن الجدل الفقهي الدّائر حول الحدود الفاصلة بين الضّبط الرقمي و التّفتيش 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.

(51) من بين أهم الأحكام القضائية الّتي تعرّضت إلى أنّ الضّبط الرقمي يقيّد الحق في الخصوصية ما يكشف عنه الحكم الصادر عن محكمة Eastern بنيويورك في حكمها الصادر بتاريخ 17 ماي 2012 في معرض فصلها في مدى مشروعية طول مدة الضّبط الرقمي حيث أشارت في إحدى حيثيات حكمها " تحتوي صورة المستند الإلكتروني على نفس المعلومات الموجودة في المستند الإلكتروني الأصلي، إلى الحد الّذي يكون لدى مالك المستند الإلكتروني 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 الّتي تقع ضمن نطاق إذن التّفتيش، إلى إجراء اتصالات شخصية بين زوج يغش زوجته أو اتصالات بين الفرد و عائلته بخصوص حالة طبية محرجة، تقع هذه الاتصالات الإلكترونية بوضوح خارج نطاق إذن التفتيش في هذه الأحوال و بالتّالي فإنّ احتفاظ الحكومة على المدى الطّويل بصور هذه الرّسائل يمثل نفس المخاوف المتعلّقة بالخصوصية حال احتفاظ الحكومة بالرّسائل الأصلية".

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

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

([53]) إنّ هذه الحقيقة قد سلّمت بها المحكمة الأوروبية لحقوق الإنسان حين اعتبرت "أنّ مجرّد جمع بيانات الاتصال و الاحتفاظ بها يعدّ بمثابة تدخل في الخصوصية سواء أتّم الاطلاع على تلك البيانات و استخدامها لاحقا أم لا و حتّى مجرد احتمال إلتقاط معلومات الاتصالات ينشئ تدخلا في الخصوصية".

CEDH, arrêt S. et Marper c. Royaume Uni, 4 décembre 2008nos 30562/04 et 30566/04, §67.

(54) الجدير بالذكر أن المادة 26 من الاتفاقية العربية مستلهمة من المادة 19 من الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية شكلا و موضوعا، إلاّ أنّ التّرجمة يشوبها عدم الوضوح و الدّقة و يظهر ذلك في عبارة (تمكين السّلطة المختصّة من "التّفتيش" أو "الوصول" إلى تقنية المعلومات)، و لفظ "الوصول" يفيد لغة بلوغ الشّيء، بما يستفاد منه أنّ الوصول إلى المنظومة المعلوماتية الّتي كانت بعيدة عن أنظار سلطات أنفاذ القانون معناه الاستحواذ أي الضّبط، و ذلك خلاف لقصد المشرّع العربي، الّذي انصرفت نيته إلى اعتبار التّفتيش واقع متى تمّ النّفاذ إلى النّظام المعلوماتي و هو ما يتطابق مع مدلول المصطلح المترجم Accès و الفارق بين المصطلحين بليغ فالأول يكيّف على أنّه ضبط و الثّاني يأخذ مدلول التّفتيش.

(55) 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.

(56) الحقيقة أنّ هذا المعيار مفقود لدى التّشريعات العربية، خاصة في ضوء الصّياغة التشريعية الرّديئة للقواعد الإجرائية المعلوماتية، الّتي تثير الغموض و اللّبس بشأن موقف التّشريعات تجاه هذه المسألة، و يكفي الاطلاع على المادة 06 من القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات و الّتي وردت تحت عنوان الأوامر القضائية المؤقتة حتّى يتمّ التّأكد من هذه الحقيقة حيث تنص:" لجهة التّحقيق المختصّة – بحسب الأحوال...2 – البحث و التّفتيش و الدّخول و النّفاذ إلى برامج الحاسب و قواعد البيانات و غيرها من الأجهزة و النّظم المعلوماتية تحقيقا لغرض الضّبط..." و باستقراء الفقرة الأخيرة

يلاحظ الخلط في المفاهيم و التّعبير عن ذات الإجراء بألفاظ مختلفة (البحث و التّفتيش و الدّخول و النّفاذ) بشكل يوحي استقلالها عن بعضها البعض، رغم وحدة المقصود و هو التّفتيش و لا ريب أنّ ذلك يشكل شائبة في الصّياغة الشّرعية لقاعدة إجرائية يفترض فيها الدّقة لتعلقها بالحريات الفردية.

(57) Article 5, alinéa1 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 للسّلطات القضائية المختصّة و كذا ضباط الشّرطة القضائية المختصّة في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عليها في المادة 4 أعلاه، **بهدف التّفتيش، الولوج، و لو عن بعد**"، أنّ النّفاذ إلى النظام المعلوماتي يتحقق به التّفيش و بذات الوقت هو مرادفا له و ليس مستقلا عنه.

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

(59) 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.

(60) 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."

(61) 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."