إجراء التفتيش في التزوير الإلكتروني

لامية مجدوب

جامعة باجي مختار – عنابة، lamia.meha@yahoo.fr

تاريخ الإيداع: 2014/11/02 **تاريخ المراجعة:** 2016/11/07 **تاريخ القبول:** 2017/02/28

ملخص

أحدث المشرع الجزائري جملة من التعديلات ضمن القوانين الجزائية لمواجهة الإجرام الإلكتروني، أو الجريمة المعلوماتية ونظرا لحداثة وخصوصية هذه الجريمة فقد عمل على تحديد الإطار القانوني الذي يوفر الحماية الجزائية اللازمة للحد من مخاطر التزوير الإلكتروني باعتباره أهم صور الجريمة الإلكترونية، هذه الأخيرة أثارت العديد من المشكلات القانونية من بينها إجراء التفتيش في البيئة الإلكترونية الذي يعد من أدق إجراءات التحقيق المادية المرتبطة بسير الدعوى العمومية، حيث طرح العديد من التساؤلات فيما يخص إمكانية تفتيش نظم الحاسوب والمعلوماتية لذلك لابد من دراسة ضوابطه وأثاره في البيئة الإلكترونية.

الكلمات المفاتيح: جريمة معلوماتية، حماية جزائية، تفتيش، بيئة إلكترونية.

Inspecting electronic forgery

Abstract

The Algerian legislator introduced a set of amendments in the penal law to prevent electronic crimes or cybercrimes. The specificity of such crimes requires a legal framework to provide penal protection and to limit the risk of the electronic forgery. The latter led to a lot of legal problems such as searching procedures taken in the electronic environment which are the main step in forensic investigation related to public action. Therefore, a lot of queries raised regarding the possibility of the operating systems as well as the computer data. Thus, it is necessary to study the standards of this search and its impact on the cyber environment.

Key words: Cybercrimes, criminal-law protection, searching, cyber environnement.

L'inspection de la fraude électronique

Résumé

Le législateur Algérien a introduit des amendements dans la législation pénale pour faire face aux criminalités électroniques ou la cybercriminalité. La spécificité de ce crime a nécessité un cadre légal définissant les mesures de protection pénales pour limiter les risques liés à la fraude électronique. Ces derniers ont engendré plusieurs problèmes juridiques tels que les procédures d'inspection prises dans l'environnement électronique qui sont parmi les mesures d'investigation matérielle les plus précises relatives au déroulement de l'action publique. De ce fait, plusieurs questionnements ont été posés quant à la possibilité d'inspecter le système d'exploitation ainsi que les données informatiques. Par conséquent, il faut étudier les normes de cette inspection et son impact sur l'environnement électronique.

Mots-clés: Cybercriminalité, protection pénale, inspection, environnement électronique.

المؤلف المرسل: لامية مجدوب، lamia.meha@yahoo.fr

مقدمـــة

اتسمـت حضـارة هذا العصـر بقفـزات تكنولوجيـة مذهلـة في شتى المجـالات وتحـديـدا في مجـال الإعلام والاتصالات، غير أنه كما هو شأن كل تقدم علمي، أدى تطور تكنولوجيا المعلوماتية في البيئة الإلكترونية إلى إفراز نوع مستحدث من الإجرام الإلكتروني أو المعلوماتي، ونظرا لخصوصية هذه الجرائم وتشعبها وتنوع صورها على غرار جريمة التزوير الإلكتروني أو التلاعب بالمعطيات في المجال الإلكتروني، بمعنى تغيير الحقيقة تغييرا من شأنه إحداث ضرر بالغير في البيئة المعلوماتية مثل ما هو حال جريمة التزوير التقليدية ظهرت العديد من المشكلات القانونية سواء الموضوعية منها أو الإجرائية المتعلقة بتحديد العناصر المشكلة الركن المادي لهذه الجريمة، أما على المستوى الإجرائي فأضحت الأساليب التقليدية للبحث والتحري والتحقيق غير مجدية للبحث عن الجريمة وملاحقة مرتكبيها مما استلزم ضرورة دمج التكنولوجيا الحديثة في التحقيق الجنائي في مختلف إجراءاته، ولعل من أهم المشكلات الإجرائية التي عرقلت سير الدعوى العمومية إجراء التفتيش في البيئة الإلكترونية باعتباره من أدق إجراءات التحقيق، حيث يتطلب البحث عن الأشياء والمستندات التي لها علاقة بالجريمة في غالب الأحيان، اللجوء إلى إجراء التفتيش بهدف ضبط أدلة مادية عن جريمة التزوير الإلكتروني، والإشكال الذي يمكن طرحه: ما مدى صلاحية النظم الالكترونية أو المعلوماتية للتفتيش؟هل خص المشرع الجزائري إجراء التفتيش في البيئة الالكترونية بقواعد خاصة؟

للإجابة على هذه الإشكالية انتهجنا المنهجين التحليلي والوصفي لتحليل النصوص القانونية المتعلقة بالتفتيش ووصف هذا الإجراء الشكلي والضمانات المتعلقة به،إضافة إلى الاستعانة بالمنهج المقارن كلما تطلب الأمر ذلك مقسمين هذه الدراسة إلى مبحثين الأول بعنوان: ضوابط التفتيش في البيئة الإلكترونية، والثاني بعنوان: الآثار المترتبة عن التفتيش في البيئة الالكترونية.

المبحث الأول: ضوابط التفتيش في البيئة الإلكترونية.

يعرف التفتيش بأنه": البحث والاستقصاء بمعنى الاطلاع على ما منح له القانون حرمة خاصة باعتباره من خصوصيات الشخص"[1] ويعتبر التفتيش[2] من أهم إجراءات التحقيق المادية لضبط الأدلة والوصول إلى حقيقة الجريمة ومرتكبيها[3]، سواء أنصب على تفتيش الأشخاص أو مساكنهم فقد يكون التفتيش عملا من أعمال التحقيق تقوم به السلطات القضائية المختصة وإما من أعمال الاستدلال يقوم به ضباط الشرطة القضائية وبذلك يعتبر إجراءً خطيراً لمساسه بالحريات الشخصية للأفراد وحرمة مساكنهم والتي كفلها الدستور الجزائري بالحماية، وهذا ما ورد ذكره في نص المادة 40 منه: "تضمن الدولة عدم انتهاك حرمة المنزل والتفتيش إلا بمقتضى القانون وفي إطار احترامه لا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة"، إن التفتيش في المنظومة المعلوماتية يساهم في ظهور حقيقة الجريمة الالكترونية أو الجرائم المعلوماتية أو جرائم الحاسوب والانترنت أو كما سماها المشرع الجزائري جرائم المساس بأنظمة المعالجة الآلية للمعطيات[4]، وقد عرفها بموجب نص المادة 02 من الفصل الأول من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في2009/08/05 تحت عنوان مصطلحات: "فهي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحدد في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية"[5]، أما عن جريمة التزوير الإلكتروني أو التلاعب بالمعطيات[6] فعرفها الفقه بأنها: "كل تغيير للحقيقة يمس نظم المعالجة الآلية للمعطيات سواء تم بإدخال أو محو

أو تعديل لها بطريق الغش"[7]، ونظر لصعوبة إجراء التفتيش في البيئة الافتراضية كون محل التفتيش هو نظم الحاسوب والانترنت، فقد خصه المشرع الجزائري بقواعد خاصة ورد ذكرها بنص المادة 05 من القانون 09-04 إلى جانب القواعد العامة المتعلقة بالتفتيش الوارد ذكرها في قانون الإجراءات الجزائية، وعليه سوف تتطرق إلى مدى قابلية مكونات وشبكات الحاسوب للتفتيش ثم شروطه في البيئة الإلكترونية.

المطلب الأول: مدى قابلية مكونات وشبكات الحاسوب للتفتيش.

يتكون الحاسوب من مكونات مادية مثل وحدات التشغيل والإدخال والإخراج والتخزين وغيرها إضافة إلى مكونات معنوية كالبرامج والبيانات بمختلف صورها[8]، ترتبط بغيرها من الحواسب بشبكات اتصال بعدية أهمها شبكة الانترنت[9] وللوقوف على مدى صلاحية مسرح جرائم نظم الحاسوب للتفتيش لا بد من التفرقة بين ثلاث حالات هي:

الفرع الأول: تفتيش المكونات المادية للحاسوب.

إن تفتيش المكونات المادية للحاسب الآلي مثل الذاكرة الصلبة أو المعالج الإلكتروني أو الكابلات أو لوحة المفاتيح أو الطابعات بحثا عن دليل ما يتصل بجريمة التزوير الإلكتروني لا يشكل أي عائق إذ إن من السهولة بمكان ضبط الأجهزة المادية وتفتيشها وحجزها وإتلافها، كل ذلك يخضع لإجراء التفتيش طبقا للقواعد العامة الإجرائية[10] إضافة إلى ما ورد ذكره بنص المادة 05 من القانون 09-04 التي تجيز تفتيش منظومة معلوماتية أو جزء منها، أو منظومة تخزين معلوماتي في إطار قانون الإجراءات الجزائية وبالرجوع إلى هذا الأخير نجده قد أورد قاعدة عامة بموجب نص المادة 81 منه، التي تجيز التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة، كما تقرر المادة 64 من نفس القانون بعض الضمانات حيث تنص على أنه لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة، إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات مكتوب بخط يد صاحب الشأن فإن كان لا يجيد الكتابة يمكنه الاستعانة بشخص يختاره بنفسه مع ذكر ذلك بالمحضر، وتطبق فضلا على ذلك أحكام المواد 44 إلى 47 من قانون الإجراءات الجزائية.

غير أن المشرع أورد استثناء على هذه المادة بموجب القانون 06-22 المؤرخ في 2006/02/20، حيث استثنى تطبيق هذه الضمانات على طائفة من الجرائم المذكورة بنص المادة 47 فقرة (03) والمادة 47 مكرر ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات حيث أجاز إجراء التفتيش في كل محل سكني أو غير سكني وفي كل ساعة من النهار والليل، وذلك بناء على إذن مسبق من وكيل الجمهورية المختص دون الإخلال بقواعد ضمان احترام السر المهني من قبل بعض الأشخاص كالمحامين، والموثقين والأطباء إضافة إلى مقرات وسائل الإعلام والاتصال وهذا ما ورد ذكره في المادة 45 في فقرتها الأخيرة من ق.إ.ج.ج[11]، إن مسالة تفتيش الأشخاص ورد ذكرها ضمن أحكام قانون الجمارك بنص المادة 42 منه في إطار التحقيق الجمركي، كما أنه يجوز تفتيش الشخص حالة القبض عليه في حالة جناية أو جنحة متلبس بها أو تنفيذا لأمر القبض، كما يجوز تفتيش الشخص كإجراء مكمل لتفتيش المسكن كلما دعت مقتضيات إجرائية أو قامت دلائل قوية على حوزته أدلة تتعلق بالجريمة الإلكترونية.

أما فيما يتعلق بمسألة تفتيش الأنثى فلم يفرق المشرع الجزائري بين الجنسين، وقد جرى العرف أن يتم تفتيش الأنثى بواسطة الأنثى،احتراما لحيائها وحفاظا على عورتها وإلا ترتب على ذلك قيام المسؤولية الجنائية، عن هتك العرض حسب ما جاء في نص المادة 335 من قانون العقوبات الجزائري[12].

الفرع الثاني: مدى خضوع المكونات المعنوية لنظم الحاسوب للتفتيش.

أثارت هذه الصورة جدلا فقهيا كبيرا بين مؤيد ومعارض لإمكانية تفتيش المكونات المعنوية أو المنطقية للحاسوب، فهي تعد المشكلة الأكثر تعقيدا في هذا الموضوع[13]، لأنها تتعلق ببيانات الحاسوب وبرامجه، الذي يتطلب تفتيشها الكشف عن الرقم السري الكود للمرور للملفات أو كلمات السر أوالشفرة أو ترميز البيانات[14]، هناك جانب من الفقه يرى تعارض غرض التفتيش وعدم انطباقه على البيانات الإلكترونية، حيث يذهب إلى إن النبضات أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة، وهذا ما دفع المشرع الفرنسي إلى تعديل نصوص التفتيش بالقانون رقم 2004-545 المؤرخ في 21 جوان 2004 حيث أضاف عبارة المعطيات المعلوماتية بنص المادة 94 من ق.إ.ج الفرنسي[15].

هذا التوجه أخذت به معظم التشريعات بجواز إمكانية تفتيش المكونات المعنوية، استنادا إلى عمومية نصوص التفتيش وتوسيع عبارة "ضبط أي شيء" لتشمل جميع مكونات الحاسوب، أضف إلى ذلك أن البيانات والبرامج الإلكترونية المتمثلة في النبضات أوالإشارات الممغنطة قابلة لتسجيلها أو تخزينها على وسائط إلكترونية معينة، يمكن قياسها ومن بين التشريعات التي أكدت ذلك التشريع الكندي في نص المادة 487 من قانونه الجنائي إضافة الى التشريع اليوناني في نص المادة 251 من قانونه الجزائي وكذلك القانون الجزائي الاتحادي الإماراتي رقم 87 لسنة 1992[16].

أما عن موقف المشرع الجزائري فقد حذا حذو التشريعات السابقة، إذ أقر تفتيش المعطيات المعلوماتية بموجب نص المادة 05 من القانون 09-04 التي تجير تفتيش منظومة معلوماتية أو جزء منها أو منظومة تخزين معلوماتية وفي هذا الصدد صرحت الاتفاقية الأوروبية في شأن جرائم تقنية المعلومات، بحق الدول الأعضاء في تفتيش النظم المعلوماتية في إطار القوانين الجزائية وذلك من خلال نص الفقرة الأولى من المادة 19 من القسم الرابع لها[17].

أما فيما يخص الإشكال الذي طرح حول مدى مشروعية تفتيش وضبط المراسلات أو الاتصالات الإلكترونية[18]؟ هل يمكن أن تخضع للتفتيش وما مدى مشروعية ذلك؟

يتضح أن المشرع الجزائري قد تنبه إلى هذه المسألة بمعنى عدم جدوى الأساليب التقليدية في البحث والتحري والتحقيق، حيث استحدث إجراءات جديدة ألا وهي اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وذلك بموجب نص المادة 65 مكرر5 بمناسبة تعديل قانون الإجراءات الجزائية بموجب القانون 06-22 السالف الذكر وفقا لضمانات موضوعية وإجرائية خاصة لضمان عدم المساس بحرمة الحياة الخاصة[19]، كما أنه أجاز بموجب نص المادتين 03 و04 من القانون09-04 وضع الترتيبات التقنية لمراقبة الاتصالات الالكترونية، وأحاطها بضمانات خاصة تعد ضرورية لحماية الحريات الفردية، كالحق في سرية الاتصالات والمراسلات الإلكترونية الخاصة وتجدر الإشارة إليه أنه بالنظر إلى تقارب هذه الإجراءات المستحدثة واشتباهها بالتفتيش، حدث خلاف فقهي حول طبيعتها فهناك من اعتبر التنصت الإلكتروني نوعا من التفتيش وهناك من اعتبرها ضبطا للرسائل الإلكترونية، لكن الراجح أن إجراءات التحري الخاصة سواء تعلق الأمر باعتراض المراسلات الإلكترونية وتسجيل

الأصوات والتقاط الصور أو حتى إجراء المراقبة الإلكترونية، هي إجراءات خاصة مستقلة ذاتية أي ذات طبيعة خاصة وأن كان مضمونها يقترب نوعا ما من التفتيش[20].

الفرع الثالث: مدى خضوع شبكات الحاسوب للتفتيش.

تعد هذه المسألة من المشكلات العالقة التي تواجه إجراء التفتيش نتيجة لطبيعة التكنولوجيا الرقمية، التي تعمل على توزيع المعلومات المحتوية على أدلة عبر شبكات حاسوبية في أماكن مجهولة بعيدة كلياعن الموقع المادي للتفتيش، فقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد أجنبي[21]، وعليه فهل يمتد تفتيش حاسوب إلى الأجهزة المرتبطة به سواء كانت موجودة داخل الإقليم أو خارجه؟

للإجابة على هذا الإشكال علينا التفرقة بين الفرضيتين الآتيتين:

أولا: اتصال حاسب المتهم بحاسب آخر موجود في مكان آخر داخل إقليم الدولة.

لا تزال هذه المسألة عالقة في بعض القوانين الإجرائية العربية كمصر وسوريا ولبنان، في حين وجدت الكثير من التشريعات حلا لها كالتشريع الأمريكي والفرنسي[22]، وكذلك الجزائري حيث أجاب القانون 09-04 على هذه المسألة بموجب المادة 05 في فقرتها الثانية، التي أقرت أنه إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وإن هذه المعطيات يمكن الولوج إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة بعد إعلام السلطة القضائية المختصة مسبقا بذلك[23].

ثانيا: اتصال حاسب المتهم بحاسب أخر موجود خارج الدولة.

قد يقوم الجناة بتخزين بياناتهم في أنظمة تقنية خارج الدولة التي يقيمون فيها، مستخدمين في ذلك شبكة الاتصال البعدية بغية إخفاء جرائمهم أو إعاقة التحقيق بشأنها أو عرقلة الوصول إلى الدليل التقني الخاص بها[24]، أما عن موقف المشرع الجزائري من مسألة التفتيش عن بعد، فقد تدارك الأمر بموجب دائما نص المادة 05 في فقرتها الثالثة من القانون 09-04 وذلك بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية وفقا لمبدأ المعاملة بالمثل مقتديا بذلك بالمشرع الفرنسي[25].

تجدر الإشارة إليه أن بعض الفقه تحفظ على القيام بإجراء التفتيش عن بعد، لأنه انتهاك صريح لسيادة الدولة الأجنبية[26].

المطلب الثاني: شروط التفتيش في البيئة الإلكترونية.

أحاطت معظم التشريعات إجراء التفتيش بجملة من الشروط والضمانات، بهدف تحقيق الموازنة بين مصلحة المجتمع في العقاب وحقوق الأفراد وحرياتهم وعليه فما هي هذه الشروط؟

الفرع الأول: الشروط الموضوعية للتفتيش.

يقصد بها الضوابط اللازمة لإجراء تفتيش صحيح في البيئة الإلكترونية وهي سابقة له عادة ويمكن حصرها في النقاط التالية: السبب، والمحل إضافة إلى السلطة المختصة به[27]، وفيما يلي توضيح كل شرط على حدة:

أولا: سبب التفتيش في البيئة الإلكترونية.

يتمثل سبب التفتيش في السعي نحو الحصول على دليل ضمن تحقيق قائم، من أجل الوصول إلى حقيقة الحدث ويتحقق هذا السبب بوقوع جريمة إلكترونية بالفعل، سواء كانت جناية أو جنحة مثل جريمة التزوير الإلكتروني أو التلاعب بالمعطيات، وهي الجنحة المقررة بموجب المادة 394 مكرر 01 من قانون العقوبات الجزائري[28]، وكذلك اتهام شخص أو أشخاص معينين بارتكاب هذه الجريمة، أو المشاركة فيها ومثال ذلك ارتباط

عنوان انترنت بروتوكول الخاص بجهاز الحاسوب الذي يحتوي على صور وبيانات مزورة، برقم حساب المتهم لدى مزود الخدمات ووجود رقمين للهاتف لديه يستخدمان في ذلك[29]، يتحقق سبب التفتيش أيضا بتوافر أمارات قوية أو قرائن على وجود بيانات أو معدات معلوماتية تفيد في كشف الحقيقة[30]، ذلك ما تستوجبه دواعي المراقبة الإلكترونية وتفتيش المنظومة المعلوماتية حتى قبل وقوع الجريمة كإجراء وقائي يستهدف مراقبة الاتصالات الإلكترونية[31] مثال ذلك تواجد مستندات إلكترونية مزورة لدى المتهم.

ثانيا: محل التفتيش في البيئة الإلكترونية.

يقصد بمحل التفتيش في التزوير الإلكتروني الحاسوب بمكوناته المادية والمعنوية إضافة إلى شبكات الاتصال التي قد تكون متواجدة في أماكن عامة أو خاصة، كالشوارع، والحدائق والمنازل أو مقاهي الانترنت أو قد تكون بحوزة مالكها مثل الحاسوب المحمول والهاتف النقال وغيرها حيث أجاز المشرع تفتيش جميع الأماكن التي تفيد في إظهار الحقيقة كما سبق بيانه في نص المادة 81 من ق.إ.ج.ج[32]، غير أنه لا يجوز تفتيش مقرات الموظفين الدبلوماسيين والقنصليين وهذا ما نصت عليه المادة 31 من اتفاقية فينا "العون الدبلوماسي يتمتع بحصانة الجهة القضائية الجزائية للدولة المعتمد لديها".

ثالثا: السلطة المختصة بإجراء التفتيش.

تختلف الجهة المختصة بالقيام بإجراء التفتيش باختلاف الأنظمة الجزائية، ففي التشريع المصري مثلا يعهد بها إلى النيابة العامة بخلاف التشريع الجزائري والفرنسي اللذين يعهدان بها إلى قاضي التحقيق كقاعدة عامة، إلا انه هناك استثناء حيث يمكن لضباط الشرطة القضائية القيام بالتفتيش في حالتين وهما:

– حالة التلبس أو ما يعرف بالجرم المشهود في الجنايات والجنح.

– حالة الإنابة القضائية[33]، أو في حالة الإذن[34]، من قبل قاضي التحقيق أو وكيل الجمهورية لضباط الشرطة القضائية بتفتيش منزل المتهم وهذا ماجاء في نص المادة 44 من ق.إ.ج.ج،كما أن هذه المادة في فقرتها الثالثة قد حددت شروط إذن التفتيش حتى يكون صحيحا، في أن يكون مكتوبا يتضمن تكييف الجريمة موضوع البحث وتحديدها بدقة وعنوان الأماكن التي سيتم تفتيشها وإجراء الحجز أو الضبط تحت طائلة البطلان ولعل أهم إشكال في مسألة الإذن[35]، بتفتيش نظم الحاسوب هو شرط تحديد الحاسوب ومعطياته المزورة بدقة التي تخلق بعض الصعوبات العملية، ذلك أن نظم المعلومات تحتوي على عدد كبير من الملفات، فهل يعتبر كل ملف "صندوقا أو حاوية مغلقة" مفردة تحتاج كل واحدة إلى إذن قضائي خاص بها؟

تضاربت أحكام القضاء الأمريكي حول هذا التساؤل حيث اعتبرت، من جهة أن الديسك بما فيه من ملفات مخزنة حاوية واحدة مغلقة وعليه لا يشترط صدور إذن قضائي مستقل لكل ملف على حدة على خلاف ذلك، اتجهت أحكام أخرى إلى أن كل ملف في الحاسوب يتطلب إذنا خاصا به حفاظا على سرية الحياة الخاصة، أما عن موقف المشرع الجزائري فلم يقدم حلا[36]، ونعتقد الراجح جواز تفتيش كل ملفات الحاسوب بإذن واحد نظرا لخصوصية هذه الجريمة وإمكانية تدمير ومحو المعلومات في ثوان، أضف إلى ذلك قد يصادف أثناء تفتيش نظم الحاسوب جريمة عرضية أخرى مثل حيازة صور جنسية فاضحة خاصة بأطفال قصر، وتجدر الإشارة إلى أن القانون الإنجليزي المعدل لقانون الشرطة والأدلة الجنائية لسنة 2006 أصدر قانونا يسهل الحصول على إذن بالتفتيش انسجاما مع ما جاء في الاتفاقية الأوروبية الخاصة بالجريمة المعلوماتية لسنة 2001[37].

الفرع الثاني: الشروط الشكلية للتفتيش في البيئة الإلكترونية.

إضافة إلى الشروط الموضوعية لصحة إجراء تفتيش نظم المعلوماتية، يجب مراعاة الشروط الشكلية والمتمثلة في ما يأتي:

أولا: الحضور الضروري لبعض الأشخاص أثناء التفتيش.

وهو من أهم الشروط الشكلية لضمان الاطمئنان وسلامة التفتيش وصحة حجز وضبط الأدلة، بالنسبة لتفتيش الأشخاص لم يشترط القانون ذلك أما تفتيش المساكن وما في حكمها، فقد أكد القانون الإجرائي على ضرورة حضور شاهدين، وإذا كان القائم بالتفتيش قاضي التحقيق أو ضابط الشرطة القضائية من غير الموظفين الخاضعين لسلطتهما متى تعذر حضور المتهم أو ممثله أو أمتنع أو كان هاربا غير أن التفتيش في البيئة الإلكترونية لا يتطلب هذا الشرط، حيث إن المشرع الجزائري استغنى عن هذا الشرط في مجال تفتيش الجريمة المعلوماتية وذلك ما ورد بموجب نص المادة 45 من ق.إ.ج.ج في فقرتها الأخيرة[38].

ثانيا: الميعاد الزمني لإجراء التفتيش في البيئة الإلكترونية.

إذا كانت القاعدة العامة في التشريع الإجرائي الجزائري أن إجراء تفتيش المساكن يتم في وقت محدد، من الساعة الخامسة صباحا حتى الثامنة مساء وهذا مانصت عليه المادة 47 من ق.إ.ج.ج غير أنه ورد استثناء يجيز إجراء التفتيش ليلا ونهارا في بعض الجرائم منها جرائم نظم المعلومات وهذا ما جاء في نص المادة 47 من القانون السالف الذكر في فقرتها الثالثة حفاظا على خصوصية هذه الجريمة[39].

ثالثا: محضر التفتيش في البيئة الإلكترونية.

لم يستلزم القانون شكلا معينا في محضر التفتيش لذلك لا يشترط لصحته سوى ما تتطلبه بقية المحاضر القضائية كأن يكون مكتوبا باللغة الرسمية، وأن يحمل تاريخ تحريره وتوقيع محرره وأن يحوي كافة الإجراءات التي تم القيام بها سواء تم الحصول على أدلة أم لا، كما يستلزم تحريره إحاطة قاضي التحقيق بتقنية المعلومات وان يستعين بذوي الاختصاص وأهل الخبرة الفنية وكذلك مقدمي الخدمات في تحرير مسودة محضر التفتيش، إضافة إلى المحافظة على الأدلة الإلكترونية من أي تلف أو ضياع[40].

المبحث الثاني: الآثار المترتبة عن التفتيش في البيئة الإلكترونية.

إن النتيجة الطبيعية للتفتيش هي حجز أو ضبط الأدلة المتحصل عليها، وهذا هو الأثر المباشر والأساسي للتفتيش، ويقصد بالضبط وضع اليد على الشيء أو حبسه والمحافظة عليه لمصلحة التحقيق، وقد أحاطه المشرع الجزائري بجملة من الضمانات طبقاً لنص المادة 84 من قانون الإجراءات الجزائية، ويعد الضبط إجراء من إجراءات التحقيق قائما بذاته، فقد يكون نتيجة لذلك أهم النتائج المترتبة عن التفتيش في جريمة التزوير الإلكتروني الحصول على الدليل الإلكتروني، والسؤال الذي يمكن طرحه هو مدى حجية الدليل الإلكتروني أمام القضاء الجزائي؟ وما هو الجزاء المترتب عن مخالفة إجراء التفتيش؟ هذا ما سيأتي في المطلبين الآتيين:

المطلب الأول: حجية الدليل الإلكتروني.

نظراً لتشعب جريمة التزوير الإلكتروني فإن كشفها وإثباتها يحتاج إلى أدلة مختلفة عن تلك الأدلة التقليدية، ومن نفس الطبيعة الإلكترونية للجريمة وعليه فما هو مفهوم هذا الدليل الإلكتروني؟ وما هي خصائصه؟ وهل يخضع لاقتناع القاضي الجزائي؟

الفرع الأول: تعريف الدليل الإلكتروني.

تعددت تعاريفه بين التوسع والضيق[41] شأنه شأن الجريمة الإلكترونية ومن بين أهم التعاريف الفقهية: "كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث يمكن الحاسوب من إنجاز مهمة معينة"، وعرف أيضا "الدليل الذي يجد له أساسا في العالم الافتراضي"، وعليه فالدليل الإلكتروني عبارة عن معلومات مخزنة في أجهزة الحاسوب وملحقاته من دسكات وأقراص مرنة وغيرها من وسائل تقنية المعلومات، كالطابعات والفاكس أو متنقلة عبر شبكات الاتصال بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبها[42]، وحتى يتضح تعريفه أكثر لابد من تحديد خصائصه مقارنة بالدليل التقليدي.

الفرع الثاني: خصائص الدليل الإلكتروني.

قد تكون الأدلة الإلكترونية مخرجات ورقية يتم إنتاجها عن طريق الطابعات أو الراسم، وإما تكون مخرجات غير ورقية، وقد تكون وسائل إلكترونية كالأشرطة والأقراص والأسطوانات وغيرها كما قد تظهر في شكل بيانات على الشاشة الخاصة بالحاسوب أو وحدة العرض المرئي، الظاهر أن البنية الإلكترونية التي يعيش فيها الدليل الإلكتروني تميزه عن غيره من الأدلة، ومن أهم مميزاته أنه دليل علمي تقني، كما يصعب التخلص منه، كما أنه قابل للنسخ والاسترجاع، وهو كذلك ذو طبيعة ديناميكية بسبب الاتساع العالمي لمسرح هذه الجريمة[43]، ومنهجها الخاص لاشتقاق الدليل الإلكتروني الجنائي[44].

الفرع الثالث: حجية الدليل الإلكتروني.

يقصد بذلك قوته الاستدلالية على صدق نسبة الفعل إلى شخص معين أو كذلك قيمة ما يتمتع به الدليل المتحصل من الكمبيوتر والإنترنت بأنواعه المختلفة، فما مدى قناعة القاضي الجزائي به وحريته في الأخذ به ضمن أدلة الإثبات[45].

تجدر الإشارة إلى أن أنظمة الإثبات اختلفت في تقديرها لحجية الدليل الجزائي، فهناك نظام الأدلة القانونية أو المقيد السائد في النظم الأنجلوسكسونية، أين يحدد المشرع أدلة الإثبات حصراً التي يجوز للتقاضي اللجوء إليها وتقدير قوتها الإقناعية وطرق التعامل معها وشروطها، وتعد بريطانيا من التشريعات التي أخذت بهذا النظام حيث أصدرت سنة 1990 قانون إساءة استخدام الحاسوب، وقد نص قانونها للإثبات على قبول الدليل الإلكتروني، وكذلك الولايات المتحدة الأمريكية أقر قانونها بأن النسخ المستخرجة من البيانات الحاسوبية تكون مقبولة بوصفها أفضل أدلة الإثبات كما يمكن قبول السجلات الحاسوبية متى توافرت شروط معينة طبقا للتشريع الكندي[46].

أما فيما يخص نظام الإثبات الحر أو نظام الاقتناع الشخصي السائد في النظم اللاتينية، فيتمتع القاضي بدور إيجابي[47]، بمعنى أن القاضي الجزائي يملك حرية تقدير الدليل الإلكتروني تبعا لمبدأ حرية الإثبات، فله رغم توافر شروط حتمية لهذا الدليل أن يطرحه جانبا تحت مبرر عدم الاقتناع والعكس، ففي ظل هذه الأنظمة لا تثور مسألة مدى مشروعية الدليل الإلكتروني من حيث الوجود، كما أن مسألة قبوله لا ينال منها سوى مدى اقتناع القاضي بهذا الدليل، ومن بين الدول التي أخذت بهذا النظام، فرنسا، وسوريا والجزائر وذلك بموجب المادة 212 ق.إ.ج.ج، وباستقراء هذه المادة يتضح أن مبدأ حرية الإثبات يعد إقرارا ضمنيا من المشرع بحجية الأدلة العلمية الحديثة كقزحية العين، وبصمة الصوت، والبصمة الوراثية (DNA) والدليل الإلكتروني[48].

أما نظام الإثبات المختلط الذي يجمع بين مزايا النظامين السابقين فقد طبق في اليابان والشيلي وبعض دول العالم الثالث[49]، وعموما فإن مسألة حجية الدليل الإلكتروني في الإثبات تبقى مرتبطة بمشروعيته وشروطه من حيث الحصول عليه وقيمته القانونية.

المطلب الثاني: بطلان التفتيش في البيئة الإلكترونية.

يخضع التفتيش كباقي إجراءات التحقيق لمبدأ الشرعية الإجرائية وتبعا لذلك، فإن مخالفة الضمانات المقررة له قانونا، قرر لها المشرع جزاء مخالفتها يتمثل في البطلان[50] وعليه فما هو تعريفه، وما هي حالاته؟ وما هي طبيعة البطلان في البيئة الإلكترونية؟

الفرع الأول: تعريف البطلان وحالاته.

يعرف البطلان بأنه: "جزاء إجرائي على العمل المخالف لبعض القواعد الإجرائية فيهدر آثارها القانونية"، كما عرف أيضا: "بأنه جزاء يلحق إجراء نتيجة مخالفته أو إغفاله لقاعدة جوهرية في الإجراءات ترتب عنه عدم إنتاجه لأي أثر قانوني" وعليه يتضح أن البطلان هو الوسيلة القانونية لمراقبة شرعية الإجراءات والجزاء المترتب على عدم احترام القواعد التي فرضها القانون أو أقرها سواء الفقه أوالقضاء[51]، فمن المتصور بطلان إجراء التفتيش في البيئة الإلكترونية بسبب عدم توفر شروط صحته كالإذن مثلا، أو أن القائم به لا يملك الصفة القانونية والاختصاص أو السلطة القانونية لمباشرته كذلك عدم قيام حالة التلبس أو أنه أنصب على جريمة معلوماتية غير معاقب عليها في التشريع الوطني، أو أن ضباط الشرطة قد خالفوا أحكام الإنابة القضائية المتعلقة بالتفتيش الإلكتروني ومن أهم حالاته البطلان المتعلق بالنظام العام والبطلان النسبي المتعلق بمصلحة الخصوم، كما أن لمعظم التشريعات مذهبين في البطلان هما: البطلان النصي والبطلان الجوهري أو الذاتي ويقصد بالأول أن البطلان مقرر قانونا مسبقا كجزاء بمعنى "لا بطلان بدون نص". أما الثاني فهو البطلان الذي تبناه الفقه والقضاء كجزاء ورتبه على مخالفة الإجراءات الجوهرية خارج الحالات التي أقرها القانون، وقد أخذت معظم التشريعات بحالتي البطلان[52]، ومن أمثلة نصوص البطلان في التشريع الجزائري المادة 44 فقرة 03 من ق.إ.ج المتعلقة بشروط إذن التفتيش والمادة 48 المتعلقة بمراعاة إجراءات التفتيش المنصوص عليها في المادتين 45 و47 من نفس القانون.

الفرع الثاني: طبيعة بطلان تفتيش نظم الحاسوب والإنترنت.

هناك خلاف فقهي حول تحديد طبيعة بطلان التفتيش تبعا للقواعد العامة وقد ذهب جانب من الفقه إلى اعتبار بطلان التفتيش مطلقا أو نسبيا، حيث يترتب الأول على مخالفة الشروط الموضوعية للتفتيش أما الثاني فيترتب على مخالفة القواعد الشكلية، بينما يرى جانب آخر من الفقه أن بطلان التفتيش متعلق بالنظام العام، ويرى جانب ثالث أن القواعد التي تنظم التفتيش تتعلق بمصلحة الأطراف وبالتالي فإن مخالفتها يترتب عنها البطلان النسبي[53].

بالرجوع إلى ق.إ.ج.ج وتحديدا نص المادتين 44 فقرة ثالثة و48 منه، يتضح أن بطلان التفتيش في البيئة الإلكترونية هو بطلان قانوني أو نصي وهو كذلك بطلان نسبي متعلق بمصلحة الأطراف وهو نفس التوجه الذي أخذ به المشرع الفرنسي الذي ورد ذكره في نص المادة 59 فقرة ثالثة من ق.إ.ج.ف. ويترتب على ذلك مجموعة من النتائج:

لا يقبل الدفع ببطلان إجراء التفتيش الواقع على الكمبيوتر والإنترنت، إلا ممن شرع البطلان لمصلحته وهو صاحب جهاز الحاسوب أو البيانات التي جرى تفتيشها أو الشخص الذي فتش شخصيا أو مسكنه، يجب التمسك به أمام قضاة الموضوع إذ لا يجوز لقضاة الحكم القضاء به من تلقاء أنفسهم كما لا يجوز الدفع به لأول مرة أمام المحكمة العليا.

كما أن بطلان إنابة قضائية متعلقة بتفتيش نظم الحاسوب والإنترنت هو بطلان جوهري وهذا يستخلص من نص المادة 138 ق.إ.ج.ج. وما يليها.

الفرع الثالث: أثر بطلان التفتيش في نظم الحاسوب والإنترنت.

يترتب على بطلان إجراء التفتيش في جريمة التزوير الإلكتروني، نتائج هامة تتمثل في عدم إنتاجه لآثاره القانونية، غير أنه يمكن الحد من آثار البطلان بتصحيح الإجراء الباطل أو إعادته بطريقة قانونية صحيحة، وفي حالة الحكم بإلغاء إجراء التفتيش فإنه يسحب من الملف ويمنع الرجوع إليه لاستنباط أدلة الاتهام منه وهذا ما سيأتي توضيحه تفصيلا.

أولا: تجريد إجراء التفتيش الباطل من إنتاج آثاره القانونية.

إن الإجراءات المتبعة خلال مراحل الدعوى العمومية تعد صحيحة ومنتجة لآثارها القانونية إلى غاية صدور حكم أو قرار قضائي بإلغائها أو بطلانها، فبطلان إجراء التفتيش الواقع على الحاسوب والإنترنت، لا يتقرر بقوة القانون تلقائيا بل إن الجهة القضائية المختصة، هي التي تفصل في مسألة البطلان المثار أمامها بقبوله أو رفضه وهي التي تحدد أثره أو مداه[54].

يترتب البطلان على تفتيش نظم الحاسوب والإنترنت وما نتج عنه من دلائل إذا لم تراع فيه أحكام المواد 45، 47 و47 مكرر من ق.إ.ج.ج. طبقا لما جاء في نص المادة 48 من ذات القانون ويؤدي بطلان إجراء التفتيش إلى تجريده من أي حجية أو آثار قانونية، كعدم جواز استناد المحكمة عليه في قرار الإدانة استنادا إلى قاعدة ما بني على باطل فهو باطل[55].

أما عن أثر بطلان إجراء التفتيش على الإجراءات السابقة له، فالأصل أن الحكم ببطلان إجراء التفتيش المعيب لا يمتد أساسا إلى الإجراءات السابقة عليه، بل تبقى صحيحة منتجة لجميع آثارها القانونية المترتبة عنها أصلا، كما أن قانون الإجراءات الجزائية الجزائري لم يتضمن أي حكم يتعلق بامتداد أثر البطلان في التفتيش إلى الإجراءات السابقة عليه، غير أن بعض من الفقه يرى إمكانية امتداد أثر بطلان تفتيش نظم الحاسوب إلى الإجراءات السابقة عليه متى كان هناك ارتباط مباشر بينهما وهذا الارتباط يقدره قاضي الموضوع[56].

أما عن أثر بطلان إجراء التفتيش على الإجراءات اللاحقة عليه، فيمكن أن يلحقها البطلان حسب الظروف، فمتى كانت ناتجة عن الإجراء الباطل ومرتبطة به ارتباطا وثيقا أصبحت باطلة استنادا على قاعدة "ما بني على باطل فهو باطل" غير أن استقلال الإجراءات اللاحقة على إجراء التفتيش الباطل الواقع على الحاسوب والإنترنت يحميها من البطلان، وبالرجوع إلى نص المادة 48 من ق.إ.ج.ج، التي رتبت البطلان النسبي على مخالفة إجراءات التفتيش المذكورة في نص المادتين 45، 47 من نفس القانون، لم ينص المشرع فيها على امتداد أثر بطلان إجراء التفتيش على الإجراءات اللاحقة له، وترك هذه المسألة لتقدير غرفة الاتهام والتي تؤسس قرارها القاضي، بامتداد أثر البطلان إلى الإجراءات اللاحقة له تبعا لنوع البطلان، فإذا كان نسبيا كما هو حال بطلان التفتيش المقرر بالمادة 48 ق.إ.ج.ج، تعين حصره على الإجراء الباطل نفسه، أما إذا كان البطلان مطلقا فيجب

أن يمتد أثره جزئيا أو كليا إلى الإجراءات اللاحقة، تبعا لتقدير غرفة الاتهام تحت رقابة المحكمة العليا طبقا لنص المادة 201 من ق.إ.ج.ج. هذا على مستوى جهات التحقيق، أما على مستوى جهات الحكم فمتى كان الحكم باطلا لخرقه أو إغفاله لنص القانون فإن هذه الجهة تتصدى للمسألة وتحكم في الموضوع(57).

ثانيا: تصحيح إجراء التفتيش الباطل أو إعادته.

يهدف البطلان كجزاء يلحق إجراء تفتيش الحاسوب والإنترنت المعيب إلى استقامة وشرعية القواعد الإجرائية، لذلك يمكن تفعيل الإجراء المعيب بتصحيحه أو إعادته، متى لحق التفتيش في البيئة الإلكترونية عيب وترتب بطلانه، ويمكن تصحيحه بعد نشوء الحق في التمسك بالبطلان، ويتم ذلك إما بالتنازل الصريح عن التمسك به طبقا لنص المواد 157، 159 و161 ق.إ.ج.ج وإما بالسكوت عن التمسك به وعدم إثارته، إذ يعد ذلك بمثابة تنازل ضمني، وبالرجوع إلى بطلان تفتيش نظم الحاسب الألي والإنترنت باعتباره بطلانا نسبيا فيجوز تصحيحه سواء على مستوى جهات التحقيق أو الحكم(58).

كما يمكن إعادة إجراء التفتيش الباطل أو إحلال محله إجراء تفتيش آخر صحيح واستبعاد الإجراء الباطل، فإذا كان التصحيح جوازيا قبل القضاء ببطلان إجراء التفتيش في البيئة الإلكترونية المعيب، فإن إعادته تصبح وجوبيه بعد القضاء ببطلانه تبعا لشكله ونموذجه المقرر قانونا وهذا ما أخذ به قانون الإجراءات الجزائية في مسألة بطلان الإجراءات ومثال ذلك نص المادتين 191 و319 من ق.إ.ج.ج، حيث أقرت إمكانية إعادة الإجراءات المعيبة بطريقة سليمة صحيحة وذلك متى توافر شرطان: أن تكون الإعادة ممكنة وضرورية وهذا ما يستعصي القيام به في جريمة التزوير الإلكتروني نتيجة لسرعة التلاعب بالمعطيات وتعديلها ومحوها إضافة إلى إمكانية إخفاء دلائلها وآثارها(59).

أما عن مصير الإجراءات الملغاة، فلقد نصت المادة 160 من ق.إ.ج.ج. على أن تسحب من ملف التحقيق أوراق الإجراءات التي أبطلت ثم تودع لدى كتاب ضبط المجلس القضائي ويمنع على القضاة والمحاميين الرجوع إليها، لاستنباط أدلة الاتهام ضد الخصوم وإلا تعرضوا إلى جزاء تأديبي بالنسبة للقضاة ومحاكمة تأديبية للمحاميين أمام محاكمهم التأديبية(60).

خاتمـــة

بعد إتمام موضوع إجراء التفتيش في جريمة التزوير الإلكتروني باعتبارها من أخطر وأكثر الجرائم الإلكترونية أو المعلوماتية انتشارا وشيوعا خلصنا إلى النتائج الآتية:

بالنسبة لضوابط التفتيش في البيئة الإلكترونية يعد التشريع الجنائي الجزائري، من بين التشريعات العربية السباقة والرائدة في مجال مواجهة هذه الجريمة، حتى أنه لم يترك أي إشكال فيما يتعلق بمدى صلاحية مكونات وشبكات الحاسوب للتفتيش وتحديدا بعد صدور القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، فالنصوص جاءت صريحة ولم تفرق بين المكونات المادية أو معطيات الحاسوب، كما تجاوزت إشكالية التفتيش عن بعد.

أما فيما يتعلق بالضمانات أو شروط التفتيش في البيئة الإلكترونية سواء الشكلية منها أو الموضوعية، فقد خص المشرع إجراء التفتيش في جريمة التزوير الإلكتروني بنوع من الخصوصية كاستثناء على القواعد العامة للتفتيش سواء تعلق الأمر بميعاد التفتيش أو الحضور الضروري لبعض الأشخاص أثناء عملية التفتيش، غير أن الإشكال يبقى مطروحا حول مدى قابلية إذن التفتيش للتطبيق على كل ملفات الحاسوب باعتبارها حاوية أو

صندوقا واحدا أم لابد من إصدار إذن بتفتيش كل ملف على حدة حماية للحقوق والحريات الفردية وسرية معاملاتهم أو علاقاتهم الخاصة؟

فيما يخص الآثار المترتبة عن التفتيش في البيئة الإلكترونية فتخضع للقواعد العامة سواء تعلق الأمر بحجية الدليل الإلكتروني أو الرقمي أو مسألة بطلان إجراء التفتيش الواقع على نظم المعالجة الآلية للمعطيات، كما أن المشرع الجزائري قد حدد طبيعة البطلان واعتبره بطلانا قانونيا ونسبيا متعلقا بمصلحة الخصوم وذلك تفاديا لأي غموض.

أما عن الاقتراحات:

– تكوين وتدريب ضباط شرطة قضائية وكذلك قضاة متخصصين ومحيطين بآلية التفتيش الواقع على مكونات الحاسوب وشبكات الاتصال.

– النص صراحة على تفتيش كل ملفات الحاسوب بإذن واحد.

الهوامش والحواشي:

1- لمزيد من الإيضاح حول تعريف التفتيش راجع: عوض محمد عوض، قانون الإجراءات الجنائية، الجزء الأول، مؤسسة الثقافة الجامعية، مصر، 2005، ص 475.

2- بكرى يوسف بكرى، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011، ص 57.

3- Herbert Maisl, «Les données confidentielles et les données nominatives sur internet», internet saisi par le droit, travaux de L'.A.F.D.I.T, éditions des parques, 1997, p 174.

4- لا فرق في هذه الدراسة القانونية بين مصطلحات الجريمة الإلكترونية، وجرائم الحاسوب والإنترنت أو الجرائم المعلوماتية أو جرائم تقنية المعلومات أو كما سماها المشرع الجزائري جرائم المساس بأنظمة المعالجة الآلية للمعطيات وغيرها من المصطلحات فهي مترادفة انظر في ذلك: محمد بن عبد الله القاسم ورشيد بن مسفر الزهراني: "نموذج مقترح للتعامل مع جرائم المعلوماتية بالمملكة العربية السعودية"، مجلة البحث الأمنية، المجلد 15، العدد 33، مايو 2006، ص 21.

5- رامي متولي القاضي، مكافحة الجريمة المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2011، ص 24 وما يليها.

6- رايس محمد، "الحماية الجنائية للسند الإلكتروني في القانون الجزائري"، مجلة الدراسات القانونية، العدد 01، 2006 – 2008، ص 97.

7- محمد محمود المكاري، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية لجرائم الكمبيوتر والإنترنت، المكتبة العصرية للنشر والتوزيع، مصر، 2010، ص 302.

8- ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة الإسكندرية، 2012، ص 131.

9- عبد العزيز نوري: "المخاطر القانونية للإنترنت على حرية التعبير والحياة الخاصة"، مجلة العلوم الاجتماعية والإنسانية التواصل، عدد 26، جوان 2010، ص 53.

10- Peter sommer, «Digital foot sprints Assessing computer évidence», The criminal law, Review Special, Edition Sweet Maxwell ltd, London, 1998, p 67.

11- أحمد الشافعي، البطلان في قانون الإجراءات الجزائية، دراسة مقارنة الطبعة الرابعة، دار هومة، الجزائر، 2005، ص 262.

12- عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، التحري والتحقيق، دار هومة، الجزائر، 2005، ص 262.

13- هشام محمد فريد رستم: "الجرائم المعلوماتية أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين" مجلة الأمن والقانون، السنة الرابعة، العدد 02 يوليو 1999، ص 84.

14- زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2011، ص 132–133.

15- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، الطبعة الأولى، منشأة المعارف، الإسكندرية، 2009، ص 251.

16- راشد بشير إبراهيم، "التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية على إمارة أبو ظبي"، مجلة دراسات إستراتيجية، العدد 131، ص 59.

17- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2012، ص 398.

18- فتحي محمد أنور عزت، الأدلة الالكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2010، ص .644

19- عرف المشرع الجزائري الاتصالات الالكترونية بموجب نص المادة 02 الفقرة (و) من القانون 09-04 تحت عنوان مصطلحات بأنها":تراسل أو استقبال علامات أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أية وسيلة الكترونية".

20- لمزيد من الإيضاح انظر: جميلة محلق": اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري"، مجلة التواصل في الاقتصاد والإدارة والقانون، جامعة باجي مختار-عنابة، عدد42، جوان 2015، ص177 وما يليها.

21- ياسر الأمير الفاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، 2009، ص 183-184.

22- Mohamed Habhab, «le droit pénal libanais à l'épreuve de la cybercriminalité», Sader éditeurs, éditions juridique, Beyrouth, Liban, p 178-179.

23- زيبحة زيدان، المرجع السابق، ص 139-140.

24- أسامة بن غانم العبيدي: "جرائم الحاسب الآلي والأنترنت الصعوبات التي تعترض المكافحة"، مجلة الإدارة العامة، المجلد 48، العدد 01، يناير 2008، ص 96.

25- لمزيد من الإيضاح حول موقف المشرع الغربي، راجع: يونس عرب، جرائم الكمبيوتر والإنترنت الطبعة الأولى، منشورات اتحاد المصارف العربية، دون مكان نشر، 2002، ص 17.

26- Nidal elchaer, la criminalité informatique devant la justice pénale, sader éditeurs, éditions, juridique, Beyrouth, Liban, 2004, pp 247-248.

27- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات دار الفكر الجامعي، الإسكندرية، 2006، ص 229.

28- حسن بن سعيد بن يوسف الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت، دراسة مقارنة رسالة دكتوراه، جامعة عين شمس، القاهرة، دوت تاريخ، ص 369.

29- عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، دون تاريخ، ص 492.

30- سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية _ دراسة تحليلية_ دار الكتب القانونية، مصر، 2011، ص 117.

31- زيبحة زيدان، مرجع سابق، ص 138.

32- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2020، ص 103.

33- لمزيد من الإيضاح حول الإنابة القضائية انظر: علي حسين محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت – دراسة مقارنة، دون مكان نشر، 2010، ص 108.

34- Mohamed Buzbar ‹La criminalité informatique sur internet», Journal of Law académique publication Council, Kuwait université, N°1, Vol 26,March 2002, p 73.

35- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص 241 وما يليها.

36- انظر في ذلك تفصيلا: عائشة بن قارة، مرجع سابق، ص 106 رشيدة بوبكر، مرجع سابق، ص 411.

37- سامي حمدان الرواشدة، أحمد موسى الهياجنة: "مكافحة الجريمة المعلوماتية بالتجريم والعقاب القانوني الانجليزي نموذجا"، المجلة الأردنية في القانون والعلوم السياسية، المجلد (01)، العدد 03، تشرين الأول، 2009، ص 132.

38- عائشة بن قارة، مرجع سابق، ص 108.

39- رشيدة بوبكر، مرجع سابق، ص 415 وما يليها.

40- حسين بن سعيد بن سيف الغافري، مرجع سابق، 385.

41- زيبحة زيدان، مرجع سابق، ص 148 وما يليها.

42- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2011، ص 229.

43- عبد الناصر محمد محمود فرغلي، الإثبات العلمي لجرائم تزييف وتزوير المحررات التقليدية والالكترونية، رسالة دكتوراه، جامعة القاهرة، 2010، ص .122

44- رضا عبد الحكيم إسماعيل رضوان: "جرائم تزوير بطاقات الدفع الإلكتروني" مجلة البحوث الأمنية، المجلد 17، العدد 39، أفريل 2008، ن ص 247.

45- خالد عياد الحلبي، مرجع سابق، ص 246.

46- محمد أحمد المنشاوي:"سلطات القاضي الجنائي في تقرير الدليل الإلكتروني"، مجلة الحقوق، السنة 36، العدد 02 يونيو 2012، ص 533.

47- منى فتحي أحمد عبد الكريم، الجرائم عبر الشبكة الدولية للمعلومات صور ومشاكل إثباتها، رسالة دكتوراه، جامعة القاهرة، 2008، ص 124.

48- سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الانترنت، رسالة دكتوراه، جامعة الإسكندرية، 2010، ص 318.

49- علي جبار الحسناوي، جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، دون تاريخ نشر، ص 141.

50- علي حسين محمد الطوالبة، مرجع سابق، ص 170.

51- جوهر قوادري صامت، رقابة سلطة التحقيق على أعمال الضبطية القضائية في القانون الجزائري والمقارن، دار الجامعة الجديدة، مصر، ص 236 وما يليها.

52- هلالي عبد الله أحمد، تفتيش نظم الحاسوب والإنترنت وضمانات المتهم المعلوماتي دراسة مقارنة، الطبعة الأولى دار النهضة العربية، القاهرة، 1997، ص 81 وما يليها.

53- عبد الفتاح بيومي حجازي، مرجع سابق، ص 365.

54- هلالي عبد الله أحمد، مرجع سابق، ص 235.

55- أحمد الشافعي، مرجع سابق، ص 205.

56- حسن محمد الطوالبة، مرجع سابق، ص 179.

57- أحمد الشافعي، مرجع سابق، ص 308.

58- المرجع أعلاه، ص 328.

59- علي حسين الطوالبة، مرجع سابق، ص 180.

60- أحمد الشافعي، مرجع سابق، ص 335.