خصوصية التحقيق في الجريمة المعلوماتية

Private investigation of cyber crime

د. عيدة بلعابد – جامعة د. مولاي الطاهر– سعيدة

الملخص:

أصبحت في الوقت الحالي المجتمعات مجتمعات معلوماتية بالدرجة الأولى في ظل التطور التكنولوجي المعلوماتي، في نفس الوقت ظهرت جرائم مستحدثة منها الجريمة المعلوماتية المتميزة بطبيعتها الخاصة من حيث طريقة ارتكابها و اعتمادها على البيانات المعلوماتية وسرعة تنفيذها، أمام إلزامية وحتمية التصدي لها ومكافحتها فإنّه ومن اللاّزم إتباع إجراءات خاصة تتماشى و طبيعة هذه الجريمة المستحدثة في إطار هذا المقال سيتم البحث في خصوصية التحقيق في الجريمة المعلوماتية.

الكلمات المفتاحية: الجريمة المعلوماتية، التحقيق الجنائي، المعلوماتية، الدليل الرقمي، إجراءات التحقيق.

Abstract:

The societies has became currently a digital societies on the first degree because of data's technological development .In addition at the time a new crimes has been appeared especially cyber crime which it is known by a particular characteristics like the way of committing and it is depending on data and the quickness of doing it .However it must fight it so it should follow a particular investigation 's procedures in which these measures are agreeable with the nature of this new crime. In this report our research is about investigation 's privacy in cyber crime.

Key words : cyber crime, criminal investigation, data, the digital proof, Investigation's measures.

المقدمة:

العالم خلال فترة زمنية أقل ما يُقال عنها بالوجيزة و السهولة من خلال كبسة زر، من جانب آخر ونظرا للاستغلال اللاعقلاني و السيئ أصبحت المعلوماتية أبرز ما يُميّز المجتمعات في الوقت الراهن في ظل التطور التكنولوجي المعلوماتي ، الّذي أصبح يتسم بالسرعة من خلال الانتقال عبر لتكنولوجيا المعلومات برزت الجريمة المعلوماتية الّتي تعرف تزايدا مستمرا لا تُستثنى منه مختلف الفئات العمرية، باعتبار الجريمة المعلوماتية ترتب آثار جسيمة تمس بالمصالح العليا للدولة ومؤسساتها و حتى اقتصادها الوطني، بالإضافة إلى مساسها بالخصوصية المعلوماتية و الحياة الخاصة للأفراد، لذا فإنّه من اللازم التصدي لهذه الجريمة و مكافحتها ومتابعة مرتكبيها وتوقيع الجزاء المقرر لهم، نظرا لما تتميّز به هذه الجريمة من طبيعة خاصة تتعلق أساسا بمكان ارتكابها وأساليب وطرق ارتكابها فإنّ الأمر يتطلب مواكبة هذه الطبيعة الخاصة من حيث الإجراءات المتبعة في التحقيق للكشف عنها ومكافحتها.

إنّ أهمية البحث في موضوع خصوصية التحقيق الجنائي في الجريمة المعلوماتية يبرز في تزايد نسبة ارتكاب هذه الجريمة المستحدثة في الوسط الاجتماعي بين مختلف الفئات العمرية مع تعدد أضرارها، كذلك طبيعة الجريمة المعلوماتية من حيث خاصية سرعة تنفيذها وصعوبة اكتشافها و إثباتها.

أمّا فيما يخص أسباب اختيار هذا الموضوع فترجع أساسا إلى القيمة العلمية من خلال تحديد الإجراءات الخاصة في التحقيق الجنائي المعلوماتي، كما يُعد موضوعا احتل مكانة هامة وخاصة في مختلف التشريعات القانونية المقارنة كما تعد أيضا الجريمة المعلوماتية جريمة العصر الحالي ما يجعل الموضوع جدير بالبحث.

من هنا تطرح الإشكالية التالية:

ما هي الإجراءات التحقيقية المتبعة في إثبات الجريمة المعلوماتية أو بصيغة أخرى ما هي الإجراءات المتبعة في التحقيق الجنائي المعلوماتي للحصول على الدليل الرقمي لإثبات الجريمة المعلوماتية؟.

لإثراء الموضوع تمت الاستعانة بالمنهج الوصفي في تحديد تعريف الجريمة المعلوماتية و إبراز خصائصها كذلك تعريف التحقيق الجنائي المعلوماتي ، كما تمت الاستعانة أيضا بالمنهج التحليلي فيما يتعلق بتحليل إجراءات التحقيق في الجريمة المعلوماتية.

بالنسبة لتقسيم موضوع الدراسة تم إتباع تقسيم ثنائي؛ المبحث الأول (ماهية التحقيق الجنائي المعلوماتي في الجريمة المعلوماتية) تم تقسيمه إلى مطلبين؛ المطلب الأول مفهوم الجريمة المعلوماتية المعلوماتية، المطلب الثاني مفهوم التحقيق الجنائي المعلوماتي.

المبحث الثاني (الإجراءات التحقيقية في الحصول على الدليل الرقمي) تم تقسيمه إلى مطلبين؛ المطلب الأول الإجراءات التحقيقية في الجريمة المعلوماتية ، المطلب الثاني الدليل الرقمي كوسيلة إثبات في الجريمة المعلوماتية.

المبحث الأول: ماهية التحقيق الجنائي في الجريمة المعلوماتية

لا يمكن إنكار دور التطور التكنولوجي المعلوماتي في إضفاء التجديد و النمو على جميع الأصعدة، بما في ذلك ميدان البحث و التحري عن الجريمة وتعقب مرتكبيها خاصة إذا تعلق الأمر بالجريمة المرتكبة في الوسط المعلوماتي الإلكتروني أو المرتكبة بواسطة الأنظمة التكنولوجية المعلوماتية، لما كانت الجريمة المعلوماتية ذات طبيعة خاصة من حيث محيط ارتكابها والوسيلة المستعملة تبعا لهذا أخذ التحقيق الجنائي فيها طابعا خاصا غير التحقيق المتعارف عليه في الجرائم العادية، إذ أصبح التحقيق فيها يُعرّف بالتحقيق الجنائي المعلوماتي.

المطلب الأول: مفهوم الجريمة المعلوماتية

تُعد الجريمة المعلوماتية من بين الجرائم المستحدثة كما يُطلق عليها مسميات مختلفة إذ تُعرّف بجرائم الكمبيوتر والإنترنت، جرائم التقنية العالية، الاحتيال المعلوماتي، احتيال الحاسوب، غش الحاسوب، الغش المعلوماتي، جرائم هاكرز، الاختراقات التقنية، cyber crime، أصحاب الياقات البيضاء.

بالرغم من هذه المسميات المتعددة إلاّ أنّها تجتمع في نقطة محددة تتعلق بالاعتماد على المعلوماتية كأساس لها ، هذا ويتميّز هذا النوع من الجرائم بطبيعة خاصة و خصائص تميزها عن باقي الجرائم.[1]

الفرع الأول: تعريف المعلوماتية

تندرج المعلوماتية ضمن علم المعلومات هذا الأخير الّذي يهتم بالموضوعات و المعارف المتصلة بأصل المعلومات و تجميعها، تنظيمها، تخزينها، تغييرها، استرجاعها و استخدامها، ورد تعريف لعلم المعلومات بأنّه:" علم التعامل العقلاني بواسطة آلات أوتوماتيكية مع المعلومات باعتبارها دعامة للمعارف

1. توبة عبد الحكيم رشيد، جرائم تكنولوجيا المعلومات، دار المستقبل للنشر و التوزيع، الأردن، 2008، ص 108.

الإنسانية و عمادا للاتصالات في ميادين التقنية و الاقتصاد و الاجتماع"[1]، هذا من جهة ومن جهة أخرى؛ وباعتبار المعلوماتية تستند إلى المعلومات فإنّه لابّد من الإشارة إلى تعريف المعلومات و الّتي تعني بأنّها: " مجموعة الرموز أو الحقائق أو المفاهيم أو التعليمات الّتي تصلح لأن تكون محلا للتبادل و الاتصال أو التفسير أو التأويل أو المعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية و الّتي تتميّز بالمرونة من حيث تغييرها ، تجزئتها، جمعها ونقلها بوسائل و أشكال مختلفة".[2]

كما تُعرّف المعلومات أيضا بأنّها :" بيانات و كلمات و صور و أصوات ووسائل و برامج الكمبيوتر و البرامج المضغوطة و الموضوعة على الأقراص المرنة و قواعد البيانات أو ما شابه ذلك"، من ثمة فالمعلومات كشيء مادي يقع عليه وصف المال قابل للقياس و التحديد بهذا تكون منقولات معنوية.[3]

هذا وتنقسم المعلومات إلى ثلاث فئات:

أ- المعلومات الاسمية: تشمل معلومات شخصية تتعلق بالشخص المخاطب بها مثل الاسم، الموطن، الحالة الاجتماعية كما تشمل معلومات موضوعية مثل المقالات الصحفية و الملفات الإدارية لدى جهة معينة.

ب- المعلومات الخاصة بالمصنفات الفكرية: مصنفات محمية بموجب قوانين الملكية الفكرية إذ تشمل الاختراعات ، الابتكارات، التسجيلات الفنية، المؤلفات الأدبية.

ت- المعلومات المتاحة: معلومات متاحة للجميع للحصول عليها دون مالك مثل تقارير البورصة و النشرات الجوية[4].

1. سعيداني نعيم، "آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري"، رسالة ماجستير في العلوم الجنائية، جامعة باتنة، الجزائر، 2013/2012، ص 12.
2. المرجع نفسه، ص 13.
3. العزمي فهد عبد الله العبيد، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2016، ص 34.
4. المرجع نفسه، ص 35.

الفرع الثاني: تعريف الجريمة المعلوماتية

تُعرّف الجريمة في المفهوم القانوني بأنّها: " كلّ عمل أو امتناع يعاقب عليه القانون بعقوبة، لقد تباينت التعريفات الفقهية للجريمة المعلوماتية بين تعريف موسع و آخر مضيّق، من التعريفات الموسعة للجريمة الإلكترونية ، نذكر التعريف الّذي يرى بأنّها:" كلّ فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال المادية أو المعنوية"[1].

كما تُعرّف بأنّها:" كلّ سلوك إجرامي يتم بمساعدة الكمبيوتر أو كلّ جريمة تتم في محيط أجهزة الكمبيوتر"[2]. أمّا فيما يتعلق بالتعريفات الّتي تُضيّق من تعريف الجريمة المعلوماتية نذكر ما ذهب إليه الفقيه Ros blat في تعريفها بأنّها :" كلّ نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي و إلى تحويل طريقه"[3].

عرّفها الأستاذ Terdmann بأنّها :" الجريمة المرتكبة ضدّ المال مرتبطة باستخدام المعالجة الآلية للمعطيات"[4]، أمّا الأستاذ Robert فقد عرّفها بأنّها:" جريمة يستخدم فيها الحاسوب كوسيلة أو أداة لارتكابها أو جريمة يكون الكمبيوتر نفسه ضحيتها"[5].

الفرع الثالث: خصائص الجريمة المعلوماتية

تختلف الجريمة الإلكترونية عن الجريمة العادية ويرجع هذا إلى مجموعة من الخصائص والمميزات وهذا بفعل ارتباطها بنظام المعلومات و التقنيات التكنولوجية هذا ما جعلها تأخذ طابعا خاصا ومنفردا بجملة من الخصائص نذكرها في النقاط التالية:

أولا: الجريمة المعلوماتية جريمة عابرة للحدود

لا مجال للحديث عن الحدود الجغرافية في الجريمة الإلكترونية ، إذ عرف العلم الإنترنت وهي عبارة عن شبكة عالمية يطلق عليها مصطلح الشبكة العنكبوتية أو شبكة الشبكات تتعدم الحدود الدولية ،

1. عبد القادر المومني نهلا، الجرائم المعلوماتية، دار الثقافة للنشر و التوزيع، الأردن، 2008، ص 49.
2. الديبري عبد العالي، صادق إسماعيل محمد، الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 40.
3. المرجع نفسه، ص 41.
4. عبد القادر المومني نهلا، المرجع السابق، ص 48.
5. محدي عماد عبد الملك، جرائم الكمبيوتر و الإنترنت، دار المطبوعات الجامعية، القاهرة، 2011، ص 33.

فقد يرتكب المجرم المعلوماتي جريمته من مكان يبعد عن تواجد الضحية بآلاف الكيلومترات[1].

ثانيا: صعوبة اكتشاف الجريمة الإلكترونية

ترجع صعوبة اكتشاف الجريمة الإلكترونية إلى عدم ترك آثار مادية خارجية لهذه الجريمة ، فالخاصية الأولى السابق ذكرها تعد عاملا في صعوبة كشفها، كما أنّ المجرم المعلوماتي باستطاعته تدمير دليل الإدانة في أقل من ثانية بالإضافة إلى قيام الجريمة الإلكترونية تتم في عالم افتراضي ممّا يجعلها تتم خفية عن طريق التلاعب في الذبذبات الإلكترونية[2].

ثالثا: سرعة التنفيذ

لا تتطلب الجريمة الإلكترونية وقتا طويلا لتنفيذها، إذ تتم بمجرد كبسة زر لذا أطلق عليها الفقهاء تسمية الجرائم الناعمة للسرعة الفائقة لتنفيذها وعدم اللجوء للعنف فيها.

رابعا: صعوبة إثبات الجريمة المعلوماتية

تُشكل سهولة محو الدليل الرقمي وصعوبة اكتشاف الجريمة الإلكترونية ، نقص الخبرة لدى المكلفين بالتحقيق أسباب مباشرة في صعوبة إثبات الجريمة الإلكترونية هذا ما يؤدي إلى إفلات المجرم المعلوماتي من الجزاء[3].

خامسا: الجريمة المعلوماتية جريمة منظمة

إنّ تتابع الاعتداءات على الشبكات الدولية المعلوماتية و أنظمة المعالجة الآلية للمعطيات جعلها ذات حيز دولي يقوم به عصابات متعددة ومنظمة ، كجريمة تبيض الأموال عن طريق الوسائط الإلكترونية ، قرصنة المعلومات و الحقوق الفكرية و الفنية ، الغش في البطاقات البنكية[4].

الفرع الرابع: الطبيعة القانونية للجريمة المعلوماتية

إنّ البحث عن الطبيعة القانونية للجريمة المعلوماتية يتطلب تحديد محل هذه الجريمة، فإذا كان محل الجريمة يتعلق بمكونات مادية للحاسوب الآلي فلا يشكل هذا إشكالا ، إذ تطبق القواعد العامة المطبقة على جرائم الأموال ؛ في حين يطرح الإشكال إذا ما وقعت الجريمة على المكونات غير المادية

1. بيومي الحجازي عبد الفتاح، الجريمة في عصر العولمة ، دار الفكر الجامعي، 2008، ص 16.
2. عبد القادر المومني نهلا، المرجع السابق، ص 54.
3. الديربي عبد العالي و صادق إسماعيل محمد ، المرجع السابق، ص 56.
4. أحمد مسعود مريم، "آليات مكافحة جرائم تكنولوجيا الإعلام و الاتصال في ضوء القانون رقم 04/09"، رسالة مقدمة لنيل شهادة الماجستير، جامعة ورقلة، الجزائر، 2013، ص 12.

للجهاز و المقصود بهذه المكونات البيانات و البرامج الّتي يحتويها الفضاء الإلكتروني داخل هذا الجهاز[1]، في هذا الإطار انقسم الفقه إلى اتجاهين اتجاه مؤيد في اعتبار المعلومات مال ؛ اتجاه آخر يعارض فكرة المعلومات مال.

أولا: الاتجاه المؤيد لاعتبار المعلومات أموال

يعتبر هذا الجانب من الفقه البيانات و المعلومات الإلكترونية مال وهي قابلة للاعتداء ،سندهم في ذلك أنها لصيقة بالحقوق الشخصية كما أنّ البيانات قابلة للانتقال لشخص آخر فليس لها كيان ملموس لكن ذات قيمة اقتصادية بهذا تعتبر مالا [2] .

ثانيا: الاتجاه المعارض لاعتبار المعلومات مال

يرى هذا الاتجاه أنّ المعلومات لا تعد أموال باعتبار المعلومة مجرد فكرة وبالتالي عدم قابليتها للتملك ، فتداولها و الانتفاع بها موجه لكافة الناس من غير تمييز[3].

المطلب الثاني: مفهوم التحقيق الجنائي المعلوماتي

يقصد بالتحقيق الجنائي:" مجموعة الإجراءات الّتي تباشرها الجهة المكلفة بالتحقيق لدى وقوع جريمة بغية البحث و التنقيب عن الأدلة الّتي تفيد في الكشف عن الحقيقة"[4]، باعتبار الجريمة المعلوماتية جريمة ذات خصائص وطبيعة خاصة هذا ما يجعل التحقيق الجنائي فيها مختلفا عن التحقيق الجنائي في الجرائم العادية، إذ يكون التحقيق في الجريمة المعلوماتية تحقيقا جنائيا معلوماتيا باعتبار مسرح ومحيط هذه الأخيرة هو الفضاء الإلكتروني والبيانات التقنية.

الفرع الأول: تعريف التحقيق الجنائي المعلوماتي

يُشكل التحقيق الجنائي المعلوماتي أو التحقيق الجنائي في البيئة المعلوماتية تحديا كبيرا للدول بالنظر إلى طبيعة هذا التحقيق و طبيعة هذه الجرائم التقنية ما جعل معظم الدول تستحدث أجهزة متخصصة تتولى مهمة التحري و الكشف عن هذه الجرائم المعلوماتية ، ففي الولايات المتحدة الأمريكية تم إنشاء شرطة الواب webpolice، مركز تلقي شكاوى جرائم الإنترنت، أمّا على المستوى الوطني

1. نوفل علي عبد الله، "جريمة إنشاء موقع أو نشر معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات"، المجلة المصرية للدراسات القانونية و الاقتصادية، العدد الثالث، مصر، جانفي 2015، ص 20.
2. قارة آمال، "الجريمة المعلوماتية"، رسالة مقدمة لنيل شهادة الماجستير، جامعة الجزائر، 2002، ص 78.
3. المرجع نفسه، ص 79.
4. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2010، ص 18.

أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة إذ يحتوي على مخبر خلية الإعلام ، بالإضافة إلى مخبرين جهويين بكل من وهران و قسنطينة، كما توجد على مستوى مركز الأمن الولائي فرق متخصصة في التحقيق في الجريمة المعلوماتية بالتنسيق مع المخابر السابق ذكرها ، كما يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي قسم الإعلام و الإلكترونيك يختص بالتحقيق في هذا النوع من الجرائم[1].

برأينا يمكن تعريف التحقيق الجنائي المعلوماتي بأنّه: مجموعة من الإجراءات القانونية المتخذة للتنقيب و الكشف عن الجريمة المعلوماتية ومرتكبيها في الفضاء الرقمي بالاستعانة بالخبراء التقنيين في ميدان الإعلام الآلي بغية الحصول على أدلة رقمية.

الفرع الثاني: خصائص التحقيق الجنائي المعلوماتي

يتميز التحقيق الجنائي المعلوماتي لمجموعة من الخصائص التالية:

أولا: التخطيط استراتيجي المسبق

هو عبارة عن تخطيط بعيد المدى يهتم بحماية البنية التحتية لشبكات الحاسبة الإلكترونية الوطنية ،من خلال تحديد مصادر الخطر المحتملة للتصدي لها كما يهتم أيضا بوضع تصورات كفيلة للتصدي لهذه الجريمة قبل وقوعها أو الحد من آثارها في حال وقوعها.

ثانيا: التخطيط التكتيكي

ينبثق هذا التخطيط من الخطة الاستراتيجية و يدعم غايات وأهداف الخطة الإستراتيجية مع تميزه بالتفصيل المعمق.

ثالثا: تحديد خطة العمل

يتم خلالها تحديد الأسلوب الأمثل في التعامل مع الواقعة وما يتوافق مع خصوصيات وملابسات الواقعة ومن أبرز ما يتم مراعاته في ذلك:

1- تحديد حجم ونوع الواقعة ليتم تعين أعضاء الفريق حسب الكفاءة و المهارات الفنية؛

2-تحديد أهمية الشبكات الإلكترونية المتضررة؛

3-مدى حساسية البيانات الإلكترونية الّتي قد تكون محل الجريمة المعلوماتية؛

4-المتهمون المحتملون؛

1. سعيداني نعيم، المرجع السابق، ص- ص 105 - 106.

5-مستوى الاختراق الأمني المعلوماتي المتسبب فيه؛

6-مستوى المهارة الفنية الّتي يتمتع بها الجاني؛

7-تحديد طبيعة مسرح الجريمة محل إجراءات التحقيق الجنائي المعلوماتي[1].

الفرع الثالث: صعوبات التحقيق الجنائي المعلوماتي

يواجه التحقيق الجنائي المعلوماتي صعوبات تعرقل من سير التحقيق الجنائي وتؤثر على الأهداف المحددة من وراء إجراء هذا التحقيق ، ممّا يُشكل صعوبة في الكشف عن الجريمة المعلوماتية ومعرفة مرتكبها، تتدرج هذه الصعوبات في عوائق تتعلق بالجريمة في حد ذاتها، عوائق تتعلق بالجهات المتضررة، عوائق تتعلق بالجهة المكلفة بالتحقيق وعوائق تتعلق بإجراءات الحصول على الدليل الرقمي[2].

أولا: العوائق المتعلقة بالجريمة المعلوماتية

1- إخفاء الجريمة وغياب الدليل المرئي ؛

2- صعوبة الوصول إلى الدليل بسبب وسائل الحماية الفنية كاستخدام كلمة السر وتشفيرها؛

3- سهولة محو الدليل أو تخريبه؛

4- ضخامة المعلومات و البيانات المتعيّن فحصها مع إمكانية خروجها عن النطاق الإقليمي للدولة بسبب البعد الجغرافي بين مرتكب الجريمة والضحية[3].

ثانيا: العوائق المتعلقة بالجهات المتضررة

1-عدم إدراك خطورة الجريمة المعلوماتية من قبل المسئولين بالمؤسسات؛

2-إغفال الجانب التوعوي لإرشاد المستخدمين إلى خطورة الجرائم المتعلقة بشبكة الإنترنت؛

3-تسابق الشركات في تسهيل استخدام البرامج و الأجهزة الإلكترونية وملحقاتها الخاصة بالحاسب الآلي وزيادة الإنتاج دون مراعاة الجانب الأمني.

4-الإحجام عن الإبلاغ عن حدوث الجريمة تفاديا للمساس بسمعة ومصداقية المؤسسات؛

5-خوف المؤسسات والشركات التجارية العاملة في ميدان الإنترنت من حجز الجهات المكلفة بالتحقيق

1. عدنان الفيل علي، المرجع السابق، ص – ص 14-16.
2. خالد ممدوح إبراهيم، المرجع السابق، ص 64.
3. المرجع نفسه، ص 66.

للحواسب الآلية أو تعطيل شبكاتها لفترة أطول تساهم في تحميلها خسائر مالية أكثر[1].

ثالثا: العوائق المتعلقة بجهات التحقيق

تتعلق هذه العوائق في عدم توفر الكفاءة البشرية المؤهلة للتحقيق و الّتي تتمثل في:

1-شخصية المحقق الّتي قد ترجع إلى التهيب من استخدام جهاز الكومبيوتر واستخدام الإنترنت، عدم الاهتمام بمتابعة آخر المستجدات في مجال الجرائم المعلوماتية؛

2-نقص المهارة الفنية المطلوبة في التحقيق الجنائي المعلوماتي؛

3-قلة الخبرة في مجال التحقيق الجنائي المعلوماتي وقلة المعرفة باللغة الإنجليزية و المصطلحات التقنية؛

4-عدم رصد ميزانية مالية كافية لاستقطاب النخبة المتميزة في مجال المعلوماتي[2].

رابعا: العوائق المتعلقة بإجراءات الحصول على الدليل الرقمي

1-صعوبة الوصول إلى الدليل الرقمي لإثبات الجريمة المعلوماتية ؛

2-ترميز وتشفير المعلومات المخزنة إلكترونيا و المنقولة عبر شبكات الاتصال؛

3-سهولة محو الدليل الرقمي؛

4-مساس إجراءات الحصول على الدليل الرقمي بالخصوصية المعلوماتية للأفراد[3].

المبحث الثاني: الإجراءات التحقيقية في الحصول على الدليل الرقمي

تتم الجريمة المعلوماتية في بيئة رقمية إلكترونية يستدعي البحث عنها و إثبات وقوعها ومعرفة مرتكبيها إتباع إجراءات محددة بدءا من معاينة الوسط المرتكبة فيه هذه الجريمة وتكون هذه المعاينة الكترونية ، القيام بإجراءات التفتيش ، المراقبة الالكترونية وكآخر إجراء ضبط الدليل الرقمي.

المطلب الأول: الإجراءات التحقيقية في الجريمة المعلوماتية

تعد المعاينة الالكترونية، التفتيش، المراقبة و ضبط الدليل الرقمي إجراءات تحقيق هامة نظرا لمساهمتها في توضيح اللبس لدى المحقق ومعرفة أبعاد الجريمة و الظروف المحيطة بارتكابها، ممّا يسهل على الجهات المكلفة بالتحقيق برسم مسار منهجي للكشف عن الأدلة الجنائية الرقمية.

1. علي عدنان الفيل، المرجع السابق، ص- ص 82-83.
2. خالد ممدوح إبراهيم، المرجع السابق، ص - ص 69-70.
3. سعيداني نعيم، المرجع السابق، ص 190.

الفرع الأول: المعاينة الالكترونية

تختلف المعاينة في الجرائم العادية عن غيرها في الجرائم الالكترونية؛ إذ الأولى تكون معاينة مسرح ارتكابها في العالم الواقعي أمّا الثانية فتكون في عالم افتراضي.

أولا: تعريف المعاينة الالكترونية

عرّف الفقه الجنائي المعاينة بأنّها:" إثبات لحالة الأماكن و الأشخاص وكلّ ما يُفيد في كشف الحقيقة"[1]. كما تعرّف أيضا بأنّها:" إجراء ينتقل بمقتضاه المحقق إلى مسرح الجريمة يشاهد ويفحص بنفسه مكانا أو شخص أو شيئا له علاقة بالجريمة ، لإثبات حالته و التحفظ على كلّ ما قد يفيد من الآثار في كشف الحقيقة"[2].

أمّا المعاينة الالكترونية أو ما يُعرف بمصطلح المعاينة التقنية في الفضاء الالكتروني بأنّها:" المشاهدة و الرؤية بالعين لمكان أو شخص أو شيء له علاقة بالجريمة لإثبات حالته و الآثار المادية الّتي خلفها ارتكاب الجريمة المعلوماتية ، وضبط كلّ ما يلزم و يفيد من الأشياء لكشف الحقيقة عن الجريمة المعلوماتية ومرتكبيها بهدف المحافظة على الأدلة التقنية من التلف أو المحو أو التعديل"[3]. هذا وتتم المعاينة الإلكترونية في الجرائم المعلوماتية من خلال الكمبيوتر أو الخادم إلاّ أنّ الانتقال هنا لا يكون إلى العالم المادي و إنّما إلى العالم الافتراضي أو الفضاء الإلكتروني cyber space [4].

ثانيا: خطوات إجراء المعاينة الإلكترونية لمسرح الجريمة المعلوماتية

لتُحقق المعاينة الإلكترونية هدفها في الكشف عن الحقيقة لابدّ من مراعاة خطوات و إرشادات محددة نذكرها في النقاط التالية:

1- تصوير الكمبيوتر وما يتصل به من أجهزة و ملحقات و المحتويات و الأوضاع العامة بصورة دقيقة مع التركيز على الأجزاء الخلفية للحاسب مع تسجيل وقت وتاريخ التقاط الصور؛

1. بيومي حجازي عبد الفتاح، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الإنترنت، دار الكتب القانونية، مصر، 2008، ص 179.
2. براهيمي جمال، "التحقيق الجنائي في الجرائم الالكترونية"، أطروحة لنيل شهادة الدكتوراه في العلوم، جامعة تيزي وز، 2018، ص 56.
3. فهد عبد الله العبيد العازمي، المرجع السابق، ص 241.
4. المرجع نفسه، ص 246.

2- مراعاة الطريقة الّتي تمّ بها إعداد النظام و الآثار الإلكترونية بما في ذلك السجلات الإلكترونية الّتي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الّذي تمّ عن طريقه الولوج إلى النظام أو الموقع؛

3- ملاحظة و إثبات حالة التوصيلات و الكابلات المتصلة بكلّ مكونات النظام لإجراء المقارنة و التحليل لعرض الأمر على القضاء؛

4- عدم إجراء أي نقل للمعلومات من مسرح الجريمة قبل إجراء اختيارات للتأكد من خلو المحيط الخارجي لموقع الكمبيوتر من أي مجالات لقوى مغناطيسية يمكن أن تكون سببا في محو أو إتلاف البيانات المسجلة؛

5- التحفظ على محتويات سلة المهملات من أوراق ممزقة و أوراق المستعملة و الشرائط و الأقراص الممغنطة وغير السليمة لفحصها ورفع البصمات الّتي قد تكون له صلة بالجريمة المرتكبة[1]؛

6- التحفظ على مستندات الإدخال و المخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد من بصمات؛

7- وضع مخطط تفصيلي للمنشأة الّتي وقعت بها الجريمة؛

8- فصل الكهرباء عن موقع المعاينة لمنع الجاني من القيام بأي عملية محو أو إتلاف على آثار الجريمة؛

9- جعل المعاينة الإلكترونية سرية ومقتصرة على فئة الباحثين و المحققين ذو الكفاءة العلمية و الخبرة الفنية [2].

الفرع الثاني: التفتيش الإلكتروني

يُعد التفتيش إجراء تحقيقي الغاية منه الحصول على أدلة جنائية تفيد في لإثبات أو نفي الجريمة المرتكبة ومعرفة مرتكبيها لإعمال الإجراءات التحقيقية ؛ من جهة أخرى فإنّ التفتيش بوجه عام يمس في أصله بالحياة الخاصة للأفراد و بالأخص الحياة المعلوماتية المتواجدة عبر مختلف مواقع التواصل الاجتماعي من بريد الكتروني، تويتر، التغريدات، الفيسبوك؛ غير أنّ حماية المصلحة الخاصة والعامة كلّها تبرر اللّجوء إلى التفتيش بما في ذلك التفتيش الإلكتروني.

1. علي عدنان الفيل علي، المرجع السابق، ص 32.
2. خالد ممدوح إبراهيم، المرجع السابق، ص 172.

بالرجوع إلى القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها[1] نجد المادة 3 منه و الّتي جاء في نصها:" مع مراعاة الأحكام القانونية الّتي تضمن سرية المراسلات و الاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية ، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون ، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية"، كما جاءت المادة 5 من القانون رقم 09-04 بنصها: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها؛
- منظومة تخزين معلوماتية"، من خلال نص المادتين يتضح أنّ المشرع الجزائري التفتيش الإلكتروني.

أولا: تعريف التفتيش الإلكتروني

يعني التفتيش بوجه عام :"إجراء من إجراءات التحقيق الابتدائي الهدف منه البحث في مستودع سر الإنسان عن دليل متعلق بجريمة وقعت ينصب إمّا على الأشخاص أو المساكن أو الممتلكات المادية وفق ضوابط قانونية"[2]، أمّا التفتيش الإلكتروني أو ما يُعرّف بولوج نظم المعالجة الآلية للبيانات في العالم الافتراضي فيُعرّف بأنّه:" إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني للبحث و التنقيب عن الجريمة المعلوماتية و أدلتها الرقمية" [3] .

كما يُعرّف التفتيش الإلكتروني أيضا بأنّه:" الدخول إلى الأنظمة المعلوماتية للبحث و التنقيب في البرامج المستخدمة و في ملفات البيانات المخزنة لإيجاد ما يفيد بارتكاب الجريمة ومرتكبيها وفق ما يقتضيه التحقيق"[4].

1. القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 أوت سنة 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، الجريدة الرسمية الجزائرية، العدد 47، الصادر بتاريخ 25 شعبان عام 1430 الموافق 16 أوت سنة 2009.
2. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الإنترنت، دار الكتب القانونية، مصر، 2007، ص 355.
3. فهد عبد الله العبيد العازمي، المرجع السابق، ص 253.
4. علي عدنان الفيل، المرجع السابق، ص 38.

ثانيا: محل التفتيش الإلكتروني

يحتوي الحاسب الآلي على مكونات مادية Hard Ware ومكونات منطقية Softe Ware وبرامج تطبيقات application programs بالإضافة إلى شبكات اتصالات بصرية سلكية ولاسلكية ، ولما كانت الغاية من التفتيش هو ضبط الأدلة المادية فإنّ ذلك يمتد ليشمل البيانات الإلكترونية[1]، بالتالي فالتفتيش يرد على البيانات غير المحسوسة عن طريق الوسائط الإلكترونية لحفظها وتخزينها كالبريد الإلكتروني، البريد الصوتي، الفاكس كما يرد على الأسطوانات ، الأقراص الممغنطة ، مخرجات الحاسب، لذا أجاز الفقه الجنائي إمكانية تفتيش البيانات المعالجة آليا، الوسائط الإلكترونية، حاملة البيانات لضبطها والتحفظ عليها[2].

ثالثا: شروط التفتيش الإلكتروني

تنقسم شروط التفتيش في البيئة الرقمية إلى شروط موضوعية و أخرى شكلية:

1-الشروط الموضوعية في التفتيش الإلكتروني:

أ- وقوع جريمة معلوماتية بمعنى كلّ فعل غير مشروع مرتبط باستخدام الحاسبة الإلكترونية لتحقيق أغراض غير مشروعة [3]؛

ب- نسب ارتكاب الجريمة المعلوماتية لشخص أو أشخاص محددين؛

ت- توفر دلائل و إمارات قوية يتطلب التفتيش الإلكتروني توفر دلائل كافية باعتبار التفتيش في جميع حالاته يمس بالحياة المعلوماتية للأفراد على غرار الأسرار و المعلومات الشخصية أو المهنية ، كما تعني الدلائل علامات معينة تستند إلى العقل وتبدأ من ظروف أو وقائع يستنتج منها الفعل تعرض للوهلة الأولى بأنّ جريمة ما قد وقعت ليبقى تقدير هذه الدلائل في يد السلطة المختصة بإصدار الإذن بالتفتيش[4].

ث- مباشرة التفتيش من السلطة المختصة ليُرّتب التفتيش الإلكتروني هدفه و آثاره لابّد أن يكون صادر عن الجهة المختصة، بالرجوع إلى القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة

1. عبد الفتاح بيومي حجازي، المرجع السابق، ص 378.
2. فهد عبد الله العبيد العازمي، المرجع السابق، ص 253.
3. علي عنان الفيل، المرجع السابق، ص 48.
4. خالد ممدوح إبراهيم، المرجع السابق، ص – ص 211-213.

بتكنولوجيات الإعلام و الاتصال ومكافحتها و تحديدا في المادة 4 الّتي جاء في نصها: "يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية:

أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني و مؤسسات الدولة و الاقتصاد الوطني

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة أ من هذه المادة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه إذنا لمدة ستة (6) أشهر قابلة للتجديد...".

يفهم من هذه المادة أنّ السلطة المختصة بإصدار التفتيش في البيئة الرقمية عندما يتعلق الأمر بالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة يؤول إصدار الإذن بالتفتيش من السيد النائب العام لدى مجلس قضاء الجزائر إلى ضباط الشرطة المنتمين إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحته.

أمّا عدا هذه الحالة فإنّه يتعيّن الرجوع إلى التدابير الّتي رسمها قانون الإجراءات الجزائية في مجال التحري و التفتيش الإلكتروني وهنا تكون الجهة المختصة بإصداره هي النيابة العامة (ممثلة في السيد وكيل الجمهورية) أو قاضي التحقيق[1]، حيث يوجه الإذن إلى ضباط الشرطة القضائية مع مراعاة الأحكام المتعلقة بتمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم المعالجة الآلية للمعطيات ، وفقا ما تضمنه المرسوم التنفيذي رقم 06-348 المؤرخ في 5-10-2006 المتضمن الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

2-الشروط الشكلية في التفتيش الإلكتروني:

يتطلب التفتيش في البيئة الرقمية إلى جانب الشروط الموضوعية شروطا شكلية ، في هذا الإطار تجدر الإشارة أنّ المشرع الجزائري أدرج المادة 5 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها ضمن الفصل الثالث المعنون بالقواعد الإجرائية في تفتيش المنظومة المعلوماتية، بالرجوع إلى هذه المادة جاء في نصها :" يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية...".

1. ربيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011، ص 142.

يفهم من هذه المادة أنّ الإجراءات الشكلية للتفتيش الإلكتروني هي نفسها الإجراءات الخاصة بالتفتيش المنصوص عليها في قانون الإجراءات الجزائية ، منه تتمثل هذه الشروط الشكلية في:

أ- وجود إذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق؛

ب- تضمن الإذن بيان وصف الجريمة موضوع التفتيش؛

ت- تحديد الأماكن المراد تفتيشها؛

ث- استظهار الإذن قبل البدء بعملية التفتيش[1]؛

ج- حضور الشخص المعني بالتفتيش أو حضور من ينوب عنه وفي حالة الرفض يستدعي ضابط شرطة قضائية شاهدين من غير الموظفين الخاضعين لسلطته[2].

الفرع الثالث: المراقبة الإلكترونية

تُعد الرقابة على الاتصالات الإلكترونية أو كما يطلق عليها بمصطلح "المراقبة الإلكترونية للاتصالات" من أهم مصادر التحري الّتي يستعان بها في التقصي عن مختلف الجرائم بما في ذلك الجرائم المتصلة بتكنولوجيات الحديثة ، خاصة في ظلّ لجوء الجناة إلى وسائل التقنية الحديثة للاتصال في تنفيذ مخططاتهم الإجرامية و التواصل فيما بينهم، كما تُعد مراقبة الاتصالات الإلكترونية مصدرا للأدلة الرقمية.

أولا: تعريف المراقبة الإلكترونية

تُعرّف المراقبة الإلكترونية أو Keepwatch بأنّها:" مراقبة شبكة الاتصالات الإلكترونية أو العمل الّذي يقوم به المراقِب باستخدام التقنية الإلكترونية لجمع بيانات و معلومات عن المشتبه فيه أو شيئا حسب طبيعته مرتبط بالزمن أي التاريخ و الوقت لتحقيق غرض أمني أو لأي غرض آخر"[3].

كما تُعرّف أيضا بأنّها:" تعمد الإنصات و التسجيل و محلها المحادثات الخاصة سواء كانت مباشرة أو غير مباشرة أي سواء ما يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الاتصال السلكية

1. المادة 44 من القانون رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون الإجراءات الجزائية المعدل و المتمم، الجريدة الرسمية الجزائرية، العدد 48.
2. المادة 45 فقرة 1 من قانون الإجراءات الجزائية، المرجع نفسه.
3. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص 198.

و اللاسلكية"[1] .

1- تعريف الاتصالات الإلكترونية:

عرّفت المادة الثانية في الفقرة " و" من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ؛ الاتصالات الإلكترونية بأنّها:" أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية".

كما ورد تعريف الاتصالات الإلكترونية في المرسوم الرئاسي رقم 261/15 المحدد لتشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و هذا ضمن المادة الخامسة منه على أنّها:" كلّ تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مهما كانت طبيعتها عن طريق أي وسيلة الكترونية بما في ذلك وسائل الهاتف الثابت و النقال".

كما تجدر الإشارة إلى أنّ الاتصالات الإلكترونية لا تقتصر على المحادثات الالكترونية فقط بل تعد المراسلات الإلكترونية أيضا من قبيل الاتصالات الإلكترونية و الّتي تتم عبر الاتصال بشبكة الانترنت و نذكر منها:

أ- البريد الإلكتروني Electronic mail

هو أكثر الاستخدامات و يتكون من جزئيين رئيسيين الرأس Header والنص body و يحتوي الرأس على معلومات حول المرسل و المتلقي و المعلومات اللازمة لتوصيل الرسالة إلى العنوان المناسب ، ويحتوي النص على الرسالة الّتي تم تكوينها وعندما يرسل شخص ما رسالة إلى شخص آخر فإنّها تنتقل من كمبيوتر المرسِل عبر خط تيليفون إلى الكمبيوتر الخادم Server mail و الّذي يوجد به صندوق بريد المرسل[2] .

1. أحمد مسعود مريم، "آليات مكافحة جرائم تكنولوجيا الإعلام و الاتصال في ضوء القانون رقم 04/09"، مذكرة لنيل شهادة الماجستير، جامعة ورقلة، الجزائر، 2013/2012، ص 79.
2. محمد أمين الشوابكة، جرائم الحاسوب و الإنترنت الجريمة المعلوماتية، الطبعة الثالثة، دار الثقافة للنشر و التوزيع، عمان، الأردن، 2009، ص 32.

ب- مجموعات الأخبار News groups

عبارة عن مناطق مناقشات عامة عبر الانترنت من خلالها يتم التحدث حول موضوع ما و تبادل المعلومات و الصور.

ت- غرف المحادثات و الدردشة Chat rooms

هي عبارة عن ساحات معروفة في الفضاء الالكتروني تتيح لمستخدميها الاشتراك في محادثات بين بعضهم بإرسال البريد الالكتروني الّذي يمكن قراءته من قبل الشخص المشترك في غرفة المحادثات[1].

من قبيل الاتصالات الالكترونية الاتصالات الّتي تتم عبر شبكات التواصل الاجتماعي على الانترنت و تعرّف هذه الأخيرة بأنّها" شبكات تفاعلية تتيح التواصل لمستخدميها في أي وقت يشاؤون و في أي مكان من العالم وقد اكتسبت اسمها الاجتماعي كونها تعزز العلاقات و الروابط بين البشر، وتعدت في الآونة الأخيرة وظيفتها الاجتماعية لتصبح وسيلة تعبيرية و احتجاجية و أبرز شبكات التواصل الاجتماعي You Tube, Face book,[2].

بالإضافة إلى الاتصالات الإلكترونية الّتي تتم عن طريق الانترنت توجد مراسلات الكترونية تتم عبر تقنيات حديثة غير الحاسوب الآلي تسمح بمباشرة التبادل الإلكتروني و الدخول إلى شبكة الانترنت عبر أجهزة الهواتف النقالة فيتم إرسال و استقبال البيانات على شكل رسائل قصيرة سواء نصية أو صور[3].

2-مبررات اللّجوء إلى المراقبة الإلكترونية:

أ-لجوء الجناة إلى الوسائل التقنية التكنولوجية الحديثة في تنفيذ مخططاتهم الإجرامية خاصة الجريمة المنظمة و العابرة للحدود الوطنية؛

ب-تميز الرقابة الإلكترونية للاتصالات بالسرعة في الوقاية من الجرائم أو الكشف عن مرتكبيها[4]؛

ت-نجاعة المراقبة الإلكترونية في الحصول على الدليل الرقمي؛

1. محمد أمين الشوابكة، المرجع السابق، ص- ص 42-45.
2. حسن السوداني، "تكنولوجيا الإعلام الجديد و انتهاك حق الخصوصية"، مجلة دفاتر السياسة و القانون، العدد الحادي عشر، جامعة ورقلة، الجزائر، 2014، ص 219.
3. محمد أمين الشوابكة، المرجع نفسه، ص 47.
4. نصر شومان، التكنولوجيا الجرمية الحديثة و أهميتها في الإثبات الجنائي، الطبعة الأولى، بدون مكان نشر، 2011، ص 156.

ث- طبيعة و خصوصية الجرائم المعلوماتية الّتي تقتضي اللّجوء إلى المراقبة الالكترونية إمّا للوقاية من حدوثها أو الكشف عن مرتكبيها؛

ج-تحقيق المصلحة العامة في حماية أمن الدولة و الأفراد وممتلكاتهم.

ثانيا: حالات اللّجوء إلى المراقبة الالكترونية

بالرجوع إلى القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها جاءت المادة الثالثة منه بنصها: "مع مراعاة الأحكام القانونية الّتي تضمن سرية المراسلات و الاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية و في هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية...".

من خلال نص هذه المادة يتبيّن أنّ إجراء المراقبة الالكترونية تقتضيه حماية النظام العام أو لمقتضيات التحريات القضائية، بالتالي لا يقتصر اللجوء إلى هذه المراقبة على جرائم معينة.

كما جاء الفصل الثاني من القانون رقم 04/09 تحت عنوان " مراقبة الاتصالات الالكترونية – الحالات الّتي تسمح باللّجوء إلى المراقبة الالكترونية" حيث حددت المادة الرابعة من ذات القانون هذه الحالات بنصها:" يمكن القيام بعمليات المراقبة المنصوص عليها في المادة الثالثة أعلاه في الحالات الآتية:

أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الماسة بأمن الدولة؛

ب-في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني؛

ت-لمقتضيات التحريات و التحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللّجوء إلى المراقبة الالكترونية ؛

ث-في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة".

من خلال ما سبق يتبين أنّ الهدف من مراقبة الاتصالات الالكترونية قد يكون هدفا وقائيا لمنع حدوث جرائم معينة و يتعلق الأمر بالجرائم الموصوفة بأعمال إرهابية أو تخريبية أو تلك الماسة بأمن الدولة، أو بوجود احتمال اعتداء على منظومة معلوماتية يهدد النظام العام أو الدفاع الوطني أو مؤسسات

الدولة أو اقتصادها الوطني، و يطلق على المراقبة الالكترونية للاتصالات لما يكون غرضها وقائي " بالتنصت الأمني المسبق لاتخاذ التدابير و الاحتياطات الضرورية" [1].

كما قد يكون الغاية من المراقبة الالكترونية للاتصالات هو التحري و الحصول على أدلة إثبات تقتضيها عمليتي التحري أو التحقيق.

هذا وتكلف مديرية المراقبة الوقائية و اليقظة الالكترونية بتنفيذ عمليات المراقبة الوقائية للاتصالات الالكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال بناء على رخصة مكتوبة من السلطة القضائية و تحت مراقبتها طبقا للتشريع الساري المفعول [2]، حيث توضع وحدة مراقبة مزودة بالوسائل و التجهيزات التقنية الضرورية المتكونة من مستخدمين تقنيين يعملون تحت إدارة ومراقبة قاض يساعده ضابط واحد من الشرطة القضائية أو أكثر ينتمي للهيئة [3].

ثالثا: ضوابط المراقبة الالكترونية

بالرغم من أنّ المراقبة الالكترونية للاتصالات تُشكل في حقيقة الأمر مساسا بالحق في الخصوصية، إلاّ أنّ حتمية التصدي للجريمة و بخاصة الجريمة المعلوماتية الّتي تفرض طبيعتها اللّجوء إلى المراقبة الالكترونية، فإنّ المشرع الجزائري قيّد اللّجوء إلى هذه الأخيرة بجملة من الضوابط و القيود والّتي تُعد تجسيدا فعليا لحماية حق الفرد في خصوصياتهم و احتراما لحياتهم الخاصة.

نجمل هذه الضوابط في النقاط الآتية:

1- أن يكون إجراء المراقبة الالكترونية للاتصالات من بين الحالات المنصوص عليها قانونا أو كان اللّجوء إليها ضروريا لسير التحريات و التحقيقات القضائية [4]؛

2- الحصول على إذن مكتوب من السلطة القضائية المختصة[5]؛

3- أن يعهد تنفيذ عملية المراقبة الالكترونية للاتصالات إلى مديرية المراقبة الوقائية و اليقظة الالكترونية

1. نزيه نعيم شلالا، دعاوى التنصت على الغير، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2010، ص 65.
2. المادة 11 من المرسوم الرئاسي رقم 261/15 المحدد لتشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.
3. المادة 22 من المرسوم رقم 261/15 المرجع السابق.
4. المادة 4 من القانون رقم 04/09 المرجع السابق.
5. المادة 4 فقرة خامسة من القانون رقم 04/09 المرجع السابق.

أو إلى مديريات جهوية [1] ؛

4- أداء المستخدمين والتقنيين المنتمين المكلفين بإجراء المراقبة الالكترونية للاتصالات لليمين قبل تنصيبهم أمام المجلس القضائي[2]؛

5- التزام المكلفين بعملية المراقبة بالسر المهني وواجب التحفظ [3]؛

6- تسجيل وتسليم الاتصالات الالكترونية المسجلة إلى السلطات القضائية و إلى مصالح الشرطة القضائية المختصة [4]؛

7- استعمال المعطيات المتحصل عليها من المراقبة الالكترونية في الحدود المقررة قانونا إمّا لضرورة التحريات أو التحقيقات القضائية [5]؛

8- المتابعة الجزائية للمستخدمين المكلفين بإجراء المراقبة سواء كانوا مستخدمين تقنيين أو ضباط شرطة في حال استخدام المعطيات المتحصل عليها في غير الأغراض المقررة لها قانونا[6].

الفرع الرابع: الضبط الالكتروني

الضبط الالكتروني أو حجز المعطيات المعلوماتية يأتي هذا الإجراء بعد عملية التفتيش الالكتروني، وإن كان ضبط الأشياء المادية المتعلقة بالجريمة المعلوماتية كأجهزة الحاسوب و ملحقاته لا يطرح أي صعوبة أو إشكالية على خلاف حجز المعلومات و البيانات المخزنة في ذاكرة الحاسوب "بنك المعلومات" أو "الأموال المعنوية"[7].

أولا: تعريف الضبط الالكتروني

يُعرّف الضبط بأنّه: "وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها"[8]، أمّا الضبط الإلكتروني فيُعرّف بأنّه: "وضع اليد على الدعائم المادية المخزنة فيها البيانات الإلكترونية أو المعلومات الّتي تتصل بالجريمة المعلوماتية الّتي وقعت وتفيد في كشف الحقيقة

1. المادة 11 من المرسوم الرئاسي رقم 261/15 المرجع السابق.
2. المادة 28 من المرسوم الرئاسي رقم 261/15 المرجع السابق.
3. المادة 27 من المرسوم الرئاسي رقم 261/15 المرجع نفسه.
4. المادة 25 من المرسوم الرئاسي رقم 261/15، المرجع نفسه.
5. المادة 9 من القانون رقم 04/09 المرجع السابق.
6. المادة 26 من المرسوم الرئاسي رقم 261/15 المرجع السابق.
7. زبيحة زيدان، المرجع السابق، ص 148.
8. علي عدنان الفيل، المرجع السابق، ص 54.

عنها وعن مرتكبيها"، كما يعني أيضا: "استخدام البرامج الهامة من أجل الولوج للبيانات المراد ضبطها إلى جانب وضع اليد على تلك الدعائم المادية" [1].

برأينا يمكن تعريف الضبط الإلكتروني بأنّه: "نسخ البيانات المعلوماتية المتواجدة في الفضاء الإلكتروني أو في الدعائم الممغنطة ووضعها في دعائم تخزين بغية كشف الحقيقة حول الجريمة المعلوماتية".

ثانيا: مدى قابلية البيانات المعلوماتية للضبط

أثارت فكرة ضبط المكونات المنطقية للحاسب الآلي أي البيانات الإلكترونية جدلا كبيرا وسط فقهاء القانون الجنائي وهذا باعتبار فكرة الضبط تقوم على أساس وضع اليد على شيء مادي ملموس، على إثر هذا ظهر اتجاهين فقهيين حول مدى إمكانية حجز البيانات المعلوماتية.

1-الاتجاه الأول: عدم قابلية البيانات الإلكترونية للضبط

يذهب هذا الاتجاه إلى استحالة حجز البيانات المعلوماتية المتواجدة في الفضاء الرقمي، مرّد هذا يرجع إلى انتفاء كيان مادي لهذه البيانات ولا مجال لحجزها إلاّ بعد نقلها عن طريق نسخها بالتصوير الفوتوغرافي أو عن طريق دعامة كالشرائط الممغنطة [2].

2- الاتجاه الثاني: قابلية البيانات الإلكترونية للضبط

على خلاف الاتجاه الأول يأخذ هذا الاتجاه بفكرة قابلية البيانات الإلكترونية للحجز، باعتبار هذه الأخيرة مجرد ذبذبات إلكترونية أو موجات كهرومغناطيسية قابلة للتسجيل و التخزين و الحفظ على وسائط مادية وبالتالي يمكن نقلها و إعادة إنتاجها [3].

3- موقف المشرع الجزائري من قابلية البيانات الإلكتروني للضبط

بالرجوع إلى القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها نجد المشرع الجزائري قد أجاز ضبط البيانات الإلكترونية أي حجزها عن طريق النسخ وهذا بحسب المادة 6 من القانون رقم 09-04 بنصها:" عندما تكتشف السلطة الّتي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و أنّه ليس من الضروري حجز كلّ المنظومة ، يتم نسخ المعطيات محل البحث وكذا المعطيات

1. فهد عبد الله العبيد العازمي، المرجع السابق، ص 271.
2. فهد عبد الله العبيد العازمي، المرجع السابق، ص 278.
3. علي عدنان الفيل، المرجع السابق، ص 58.

اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحراز..."؛ تجدر الإشارة إلى أنّه في حال استحالة حجز البيانات المعلوماتية عن طريق نسخ المعطيات الإلكترونية أو في حال تعذر إعادة تشكيل هذه المعطيات نص المشرع الجزائري على حجز هذه المعطيات عن طريق منع الوصول إليها من خلال استعمال تقنيات مناسبة أو بوضع الترتيبات التقنية اللازمة لمنع الاطلاع عليها[1].

ثالثا: الصعوبات الّتي تواجه ضبط البيانات الإلكترونية

تواجه عملية حجز البيانات المعلوماتية صعوبات ترجع للأسباب الآتية:

1-وجود أدلة رقمية متصلة بنظام معلوماتي لدولة أخرى ما يستدعي تعاون دولي لإضفاء المشروعية على عملية الضبط؛

2-ضخامة الشبكة المعلوماتية الّتي تحتوي على البيانات الإلكترونية محل الضبط كالبحث في نظام معلوماتي تابع لشركة متعددة الجنسيات؛

3-مساس الضبط الإلكتروني بحرمة الحياة المعلوماتية الخاصة ممّا يتطلب مراعاة كافية للضمانات اللازمة لحماية هذا الحق؛

4-وجود أحزمة أمنية مفروضة من قبل مستخدم النظام حول البيانات المعلوماتية كتشفير الدخول للنظام؛

5-اللّجوء إلى عزل النظام المعلوماتي بالكامل لمدة زمنية قد تطول ما يؤدي إلى إلحاق أضرار بالجهة المستخدمة للنظام[2].

المطلب الثاني: الدليل الرقمي كوسيلة إثبات في الجريمة المعلوماتية

نظرا لخصوصية الجريمة المعلوماتية يبقى الدليل الرقمي الوسيلة الكافية في إثبات هذا النوع من الجرائم، كما لا يخص الدليل الرقمي هذا النوع من الجرائم بل يمكن الاستعانة به في باقي أنواع الجرائم باعتبار التطور التكنولوجي أصبح وسيلة في ارتكاب العديد من الجرائم.

الفرع الأول: مفهوم الدليل الرقمي

تعددت التعريفات الاصطلاحية للدليل الرقمي و إن كانت في مجملها تجتمع في نقطة محددة تتعلق بالبيئة الالكترونية لهذا الدليل الحديث، مع تميزه بجملة من الخصائص.

1. المادة 7 و8 من القانون 09-04، المرجع السابق.
2. سعيداني نعيم، المرجع السابق، ص 162.

أولا: تعريف الدليل الرقمي

الدليل الرقمي:" هو الدليل المأخوذ من أجهزة الكمبيوتر في شكل موجات ونبضات مغناطيسية أو كهربائية يمكن تجميعها و تحليلها بواسطة برامج تطبيقات و تكنولوجيات خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الرسوم من أجل اعتماده أمام أجهزة تطبيق القانون" [1].

كما يُعرّف بأنّه:" الدليل الّذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة أو هو تلك المعلومات الّتي يقبلها المنطق و العقل و يعتمدها العلم و يتم الحصول عليها بإجراءات قانونية و علمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال و يمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء له علاقة بجريمة ما أو المجني عليه" [2]، برأينا يمكن تعريف الدليل الرقمي بأنّه ذلك الدليل الّذي يتضمن بيانات إلكترونية مخزنة بالحاسب الآلي و لها وجود في الوسط الافتراضي و الّتي من خلالها يتم الكشف عن الجريمة أو إثبات العلاقة بين حدوث الجريمة وفاعلها.

ثانيا: خصائص الدليل الرقمي

يتميّز الدليل الرقمي بمجموعة من الخصائص تميّزه عن باقي الأدلة الجنائية تتمثل هذه الأخيرة في ما يلي:

1- الدليل الرقمي دليل علمي و تقني:

يتكوّن الدليل الرقمي في أساسه من مجموعة من البيانات و المعلومات ذات صبغة الكترونية غير ملموسة يتم إدراكها بواسطة أجهزة و معدات و أدوات الحاسبات الآلية و الاستعانة بنظم برامجية حاسبية[3]، هذا ما يجعل من الدليل الرقمي من الأدلة العلمية و التقنية الحديثة ؛ نظرا لبيئته التقنية في المجال الافتراضي كما أنّه و باعتبار الدليل الرقمي عبارة عن نبضات رقمية ذات طبيعة ديناميكية تتميز

1. نور الهدى محمودي، "حجية الدليل الرقمي في إثبات الجريمة المعلوماتية"، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة 1، العدد الحادي عشر، جوان 2017، ص 911.
2. أشرف قنديل عبد القادر، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2015، ص 123-124.
3. عائشة بن قارة، المرجع السابق، ص 62.

بالسرعة الفائقة المتعدية لحدود الزمان و المكان[1] ، كلّ هذا يجعل الدليل الرقمي دليل يعتمد على التقنيات بالدرجة الأولى.

2- الدليل الرقمي ذو طبيعة متطورة:

لا اختلاف عي اعتبار الدليل الرقمي دليل متطور بطبيعته، فهو يمتاز بتطور تلقائي تبعا لتطور البيئة الرقمية الّتي تعتمد أساسا على التجدد [2]، ويرجع هذا إلى تطور الثورة التكنولوجية خاصة في مجال الاتصالات و أجهزة التواصل.

3- صعوبة إتلاف الدليل الرقمي:

قد يتعرض الدليل الرقمي إلى عملية إتلاف سواء بصفة كلية أو جزئية وهذا من خلال عملية المحو، غير أنّه و بالرغم من هذا فإنّ إتلافه لا يمنع من إعادة استرجاع محتوى الدليل الرقمي من ذاكرة الحاسب الآلي أو بالاستعانة بنسخ منه [3].

الفرع الثاني: تقسيمات الدليل الرقمي

لم يتطرق أغلب فقهاء القانون الجنائي إلى دراسة شاملة و دقيقة للأدلة الجنائية الرقمية نظرا لحداثة هذا النوع من الأدلة و بيئته الّتي تمتاز بالتطور المستمر، و بالرغم من ذلك نشير إلى محاولة فقهية قسمت الدليل الرقمي إلى أربع تقسيمات هي:

أولا: الأدلة الرقمية الخاصة بأجهزة الحاسب الآلي وشبكاتها، تعتبر هذه الأخيرة مستخرجات برامج الحاسب الآلي.

ثانيا: الأدلة الرقمية الخاصة بالإنترنت.

ثالثا: الأدلة الرقمية الخاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

ثالثا: الأدلة الرقمية الخاصة بالشبكة العالمية للمعلومات [4].

1. أشرف قنديل عبد القادر، المرجع السابق، ص 126.
2. إدريس خوجة لخضر، "الإثبات بالأدلة الجنائية الرقمية على ضوء التشريع الجزائري"، مجلة آفاق للدراسات القانونية المقارنة، جامعة سعيدة الطاهر مولاي، جوان 2017، ص 157.
3. محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، دار الحامد للنشر و التوزيع، الأردن، 2014، ص 236.
4. عائشة بن قارة، المرجع السابق، ص 71.

الخاتمة:

ختاما لموضوع البحث في خصوصية التحقيق في الجريمة المعلوماتية يتضح أنّ طبيعة الجريمة المعلوماتية تفرض نمطا تحقيقي مغايرا عن التحقيق الجنائي المعتاد في الجرائم العادية ، فتختلف بذلك الوسائل ويكون وجود خبير في الإعلام الآلي في عملية التحقيق الجنائي لما له من كفاءة ودراية بعالم المعلوماتية في الفضاء الإلكتروني .هذا من جهة ومن جهة أخرى ؛ما يبرر اللّجوء إلى إجراءات تحقيقية خاصة في هذا النوع من الجرائم هو طبيعة الدليل في إثبات قيام الجريمة ونسبها لفاعل محدد وهنا تكون الأدلة الرقمية الدليل المناسب لذلك.

بالنسبة للنتائج المستخلصة في موضوع البحث تتمثل في:

- طبيعة الجريمة المعلوماتية من حيث امتدادها عبر الحدود الوطنية وصعوبة اكتشافها في بعض الحالات ، بالإضافة إلى سرعة تنفيذها وصعوبة إثباتها يحتم إتباع إجراءات تحقيقية خاصة؛
- التحقيق الجنائي المعلوماتي مجموعة من الإجراءات القانونية المتكاملة تهدف للتنقيب و البحث عن الأدلة الرقمية لإثبات الجريمة المعلوماتية و الوصول إلى مرتكبيها؛
- التحقيق الجنائي المعلوماتي يعتمد على التخطيط الاستراتيجي المسبق و التخطيط التكتيكي مع تحديد لخطة عمل مسبقة؛
- محل التحقيق الجنائي المعلوماتي هو المعلومات و البيانات المتواجدة بالبيئة الإلكترونية؛
- يواجه التحقيق الجنائي المعلوماتي صعوبات قد ترجع إلى الجريمة المعلوماتية أو إلى الجهات المتضررة أو إلى جهات التحقيق؛
- الدليل الرقمي وسيلة أمثل لإثبات الجريمة المعلوماتية ومعرفة مرتكبها؛
- المعاينة الإلكترونية ؛ التفتيش الإلكتروني ، المراقبة الإلكترونية و الضبط الإلكتروني إجراءات تحقيقية للحصول على الدليل الرقمي.

بالنسبة للاقتراحات:

- الأخذ بنظام تخصص القضاة الجنائيين في الجريمة المعلوماتية على المستوى العلمي المعرفي و العملي؛
- ضرورة إعداد برنامج تكويني خاص ومعمق في الإعلام الآلي للطلبة القضاة من أجل التسهيل في المشروع المهني مستقبلا؛

- تنظيم دورات توعوية لفائدة مختلف فئات المجتمع و بالأخص فئة الأحداث حول مخاطر الجريمة المعلوماتية؛
- حث المواطنين على التبليغ عن الجريمة المعلوماتية؛
- إبرام اتفاقيات تعاون داخلية بين القضاء ومهندسو الإعلام الآلي من أجل إثراء المعرفة الفكرية في ميدان المعلوماتية.

قائمة المراجع:

أولا: الكتب

1. البشرى محمد الأمين، التحقيق في الجرائم المستحدثة، دار الحامد للنشر و التوزيع، الأردن، .2014
2. الديبري عبد العالي، صادق إسماعيل محمد، الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، القاهرة، 2012.
3. الشوابكة محمد أمين، جرائم الحاسوب و الإنترنت الجريمة المعلوماتية، الطبعة الثالثة، دار الثقافة للنشر و التوزيع، عمان الأردن، 2009.
4. العزمي فهد عبد الله العبيد، الإجراءات الجنائية المعلوماتية ، دار الجامعة الجديدة، الإسكندرية، 2016.
5. المومني نهلا عبد القادر ، الجرائم المعلوماتية، دار الثقافة للنشر و التوزيع ، الأردن، 2008 .
6. بوسقيعة أحسن، الوجيز في القانون الجزائي العام، الطبعة 14، دار هومة للطبع و النشر، الجزائر، 2014.
7. بيومي الحجازي عبد الفتاح ، الجريمة في عصر العولمة، دار الفكر الجامعي، الإسكندرية، 2008.
8. توبة عبد الحكيم رشيد، جرائم تكنولوجيا المعلومات، دار المستقبل للنشر و التوزيع، الأردن، 2008.
9. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2010.
10. زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011.
11. شومان نصر، التكنولوجيا الجرمية الحديثة و أهميتها في الإثبات الجنائي، بدون مكان نشر،2011.
12. عدنان الفيل علي، إجراءات التحري وجمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، دار الكتب والوثائق القومية، العراق، 2012.

13. قنديل عبد القادر أشرف، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة، الإسكندرية 2015.
14. محدي عماد عبد الملك، جرائم الكمبيوتر و الإنترنت، دار المطبوعات الجامعية، القاهرة، 2011.
15. نزيه نعيم شلالا، دعاوى التنصت على الغير، منشورات الحلبي الحقوقية، لبنان، 2010.
16. هروال نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، دار الفكر الجامعي، الإسكندرية، 2006.

ثانيا: المقالات

1. السوداني حسن، "تكنولوجيا الإعلام الجديد و انتهاك حق الخصوصية"، مجلة دفاتر السياسة و القانون، كلية الحقوق و العلوم السياسية، جامعة ورقلة، الجزائر، العدد الحادي عشر، 2014.
2. خوجة لخضر إدريس، "الإثبات بالأدلة الجنائية الرقمية على ضوء التشريع الجزائري"، مجلة آفاق للدراسات القانونية المقارنة، جامعة سعيدة الطاهر مولاي، الجزائر، جوان 2017.
3. محمودي نور الهدى، "حجية الدليل الرقمي في إثبات الجريمة المعلوماتية"، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة 1، الجزائر، العدد الحادي عشر، جوان 2017.
4. نوفل علي عبد الله، "جريمة إنشاء موقع أو نشر معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات"، المجلة المصرية للدراسات القانونية و الاقتصادية، كلية الحقوق، مصر، العدد الثالث، جانفي 2015.

ثالثا: الرسائل

1. أحمد مسعود مريم، "آليات مكافحة جرائم تكنولوجيا الإعلام و الاتصال في ضوء القانون رقم 04/09"، رسالة الماجستير، قانون عام ، جامعة ورقلة، الجزائر، 2013.
2. براهيمي جمال، "التحقيق الجنائي في الجرائم الالكترونية"، رسالة دكتوراه، قانون جنائي، كلية الحقوق و العلوم السياسية، جامعة تيزي وزو، 2018.
3. سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير علوم جنائية، كلية الحقوق و العلوم السياسية الحاج لخضر جامعة باتنة، الجزائر، 2013/2012.
4. قارة آمال، الجريمة المعلوماتية، رسالة شهادة الماجستير، قانون جنائي، كلية الحقوق و العلوم السياسية، جامعة الجزائر، 2002.

رابعا: القوانين

1. القانون رقم 06-22 ، المعدل و المتمم للأمر رقم 66-155،المؤرخ في 18صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون الإجراءات الجزائية ،المؤرخ في 29 ذي القعدة عام 1427الموافق 20 ديسمبر سنة 2006، الجريدة الرسمية للجمهورية الجزائرية الديمقراطيّة الشعبيّة، العدد84، الصادر في 4 ذي الحجة عام 1427 الموافق 24 ديسمبر سنة 2006.
2. القانون رقم 09-04 ،المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، المؤرخ في 14 شعبان عام 1430 الموافق 5 أوت سنة 2009، الجريدة الرسمية للجزائرية الديمقراطيّة الشعبية، العدد 47، الصادر بتاريخ 25 شعبان عام 1430 الموافق 16 أوت سنة 2009.
3. المرسوم الرئاسي رقم 15-261 ، المحدد لتشكيلة و تنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، المؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015، الجريدة الرسمية للجمهورية الجزائرية الديمقراطيّة الشعبيّة، العدد.53
4. المرسوم التنفيذي رقم 06-348، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، المؤرخ في 12 رمضان عام 1427 الموافق 5 أكتوبر سنة 2006، الجريدة الرسمية للجمهورية الديمقراطيّة الشعبيّة، العدد 36.