وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي – تبسة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مكملة لنيل شهادة ماستر (ل.م.د) في الحقوق

تخصص: قانون جنائي وعلوم جنائية

الحق في الخصوصية الرقمية في مواجهة مقتضيات التحقيق الجنائي

إعداد الطالب:

– سلطاني عبد الرؤوف

إشراف الأستاذ:

– جبيري ياسين

أعضاء لجنة المناقشة:

اللقب والاسم	الرتبة العلمية	الجامعة	الصفة
خذيري عفاف	أستاذ محاظر أ	جامعة العربي التبسي	رئيسا
جبيري ياسين	أستاذ محاظر أ	جامعة العربي التبسي	مشرفا ومقررا
شارني نوال	أستاذ محاظر ب	جامعة العربي التبسي	عضوا مناقشا

السنة الجامعية:

2023 – 2022

الكلية لا تتحمل مسؤولية ما يرد في هذه المذكرة من آراء

قال الله تعالى:

﴿يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ ۖ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا ۚ أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ ۚ وَاتَّقُوا اللَّهَ ۚ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ﴾

سورة الحجرات الآية 12.

الشكر والعرفان:

اول الكلام الحمد لله الملك العلام ذا المن والجود والاحسان نحمده حمدا كثيرا يليق بجلال وجهه و عظيم سلطانه

اما بعد نتوجه بعظيم القدر و الامتنان لكل اساتذة الكلية كل بإسمه ومكانته لكل ما قدموه لنا طيلة هذه المسيرة

ونتوجه بأحر عبارات الشكر والعرفان للأستاذ الذي اكرمنا بعطائه ولم يبخل علينا بما يملك مما آتاه الله به من بحر العلم للاستاذ الفاضل جبيري ياسين

وبعد أتقدم بجزيل الاحترام للوجوه التي انارت يوم مناقشتي ويوم فرحي للأساتذة الأكارم الذين كانوا خير عون وسند في إتمام هذا العمل من العبد الفقير لله.

الإهداء

الى من افاضوا عليا من جودهم وإحسانهم الى من كانوا مصدر وجودي في هذه الحياة

الى من أبصر بنور محياهم الى من لا حياة إلا معهم ولا رضاء إلا برضاءهم كيف لا

وقد قرنت مرضات الله بمرضاتهم الى الوالدين الكريمين حفظهما المولى بحفظه

واجلهما بستره ورزقهما الجنة بلا حساب

الى اخوتي وأملي في الحياة الى إسلام الحبيب و ولسيم سندي ورفقتي التي لا أظل معهما

ولا أحمل هما وهما في كتفي

الى قرة العين ولؤلؤة الفؤاد الى رفيقة الدرب وشقيقة الروح الى أختي الوحيدة

الى كل من حمل لقب العائلة الى عائلة سلطاني كل بإسمه ولهم منا التحية

الى أصدقائي وأحبتي وكل فرد كان لنا معينا و مشجعا ولو بكلمة صغيرة

أهدي ثمرة جهد السنين وسهر الليالي

قائمة المختصرات

دط:دون طبعة

دب ن: دون بلد النشر

ق إ ج : قانون الاجراءات الجزائية

ط: طبعة

ص: صفحة

دس ن: دون سنة النشر

المقدمـة

تمهيد:

لقد تطورت قضية حقوق الإنسان في العقود الأخيرة، وتوسعت رقعة الاهتمام بها وتزايدت الأصوات ليس عن تقنينها وإكسابها الشرعية الدستورية فحسب، بل عن طلب الوسائل القانونية والشرعية لضمان تطبيقها، وقبلها ثم جاءت الرسالات السماوية مؤكدة على ذلك وموضحة له في الكثير من مصادرها، حيث نصت الشريعة الإسلامية على حرمة المساكن ومنع دخولها دون إذن وحضر كافة أنشطة التجسس حماية لأحاديث الأفراد وسترا لعيوبهم، قال الله تعالى: ﴿**يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ ۖ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا ۚ أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ ۚ وَاتَّقُوا اللَّهَ ۚ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ**﴾ (الحجرات 12.

وقد كفلت القوانين حق الأفراد أو المجموعات أو المؤسسات في أن يحددوا لأنفسهم مدى وصول المعلومات المرتبطة بحياتهم الخاصة للآخرين وبأن يضبط عملية حصر المعلومات الشخصية ومعاملتها آليا، واستخدامها في صنع القرار الخاص أو المؤثر في حياتهم، وذلك لربط ولادة مفهوم الحق في الخصوصية المعلوماتية بمخاطر تقنية المعلومات المحيطة بمسألة حماية بنوك المعلومات وعمليات المعالجة الآلية للبيانات الشخصية، كما أن الحق في خصوصية المعلومات الشخصية يتوقف على فكرة الاعتداء عليها إلكترونيا من قبل الآخر، واستخدامها وفقا لأغراض خارجة عن القانون بدون علم أو إرادة صاحبها.

الأهمية:

في ظل ازدياد تطور التكنولوجيا الحديثة ازدات مخاطرها على الحق في الحياة الخاصة وأضحى الفرد مقيدا في تعاملاته من خلال رصد البيانات الشخصية وتخزينها ومعالجتها بواسطة مختلف الوسائط المعلوماتية كتقنيات المراقبة أو التجسس والقرصنة والمساس بالمعطيات الخاصة بالأفراد وهي جميعها تمثل تهديدا مباشرا على حياتهم الخاصة وحرياتهم الفردية بصورتها المستحدثة والمتمثلة في بنك المعلومات لا سيما إذا استغلت لغايات خارجة عن إرادة أصحابها ودون علمهم، والقانون الجزائري قد قرر هذا الحق من خلال اكثر من مادة أهمها المادة 39 من الدستور التي تنص على: (لا يجوز انتهاك حرمة حياة المواطن وحرمة شرفه ويحميها القانون.

حيث أن التحقيق الجزائي هو اتخاذ جميع الإجراءات والوسائل المشروعة التي تؤدي إلى كشف الحقيقة وغموضها، والدعوى الجزائية تمر قبل أن توضع أمام القضاء للفصل فيها بمرحلة التحقيق الابتدائي وهي مرحلة جمع الأدلة والتصرف فيها وتهدف إلى اتخاذ الإجراءات اللازمة لكشف الجريمة ومرتكبيها بالتثبت من وقوعها والبحث عن فاعليها وجمع العناصر اللازمة لأن تكون أساساً لبدء النيابة العامة نظرها في أمر الدعوى، حيث أن لكل شخص الحق في الخصوصية بوجه عام يكفلها له القانون ويحميها من أي تعديات ومن بينها الخصوصية الرقمية التي سلط المشرع الجزائري عليها الضوء من خلال حمايتها من الانتهاكات بمجموعة من الإجراءات التقليدية والمستحدثة.

الأهداف:

تهدف هذه الدراسة في الأساس إلى تبيان الإجراءات التي تعد انتهاكا للخصوصية الرقمية فيكون هذا الاعتداء أو الانتهاك أما عن طريق إجراءات خاصة بالبيانات وعن طريق الإجراءات الإلكترونية والمتمثلة في التجسس والتسلل الإلكتروني.

وكذلك مظاهر حماية الحق في الخصوصية الرقمية في ظل قانون الإجراءات الجزائري كالمعاينة وضبط الأدلة والاستجواب وإجراءات خاصة أو مستحدثة متمثلة في الخبرة والشهادة.

الدوافع:

وما دفعنا لاختيار هذا الموضوع هو تسليط الضوء على الوسائل الجديدة التي لجأ إليها المشرع الجزائري لمكافحة الانتهاكات التي تقع على الخصوصية الرقمية والإجراءات التقليدية والمستحدثة ذلك أن الحق في الخصوصية الرقمية يتعرض إلى العديد من الانتهاكات تنصب على البيانات الشخصية كإفشائها ومعالجتها دون ترخيص كما تنصب أيضا على الحاسبات الآلية والبريد، وتطورها في التشريع الجزائري ومدى ملائمة هذه الإجراءات مع الحق في الخصوصية.

الدراسات السابقة:

ومن بين الدراسات السابقة التي ناقشت هذا الموضوع:

- صغير يوسف، "الجريمة المرتكبة عبر الأنترنت"، مذكرة ماجيستر، لجامعة مولود معمري تيزي وزو.

حيث تناول جزئية من موضوع الدراسة بعنوان الخبرة في الفصل الثاني المبحث الأول

بالإضافة إلى الفصل الأول بعنوان الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت أي أن دراسته تتمثل في جزئية هامة في موضوع بحثي.

- ثابت دنيا زاد، "مراقبة الإتصالات والحق في حرمة الحياة الخاصة في القانون الجزائري" مجلة العلوم الإجتماعية والإنسانية لجامعة تبسة.

حيث تناولت جزئية من موضوع الدراسة وهي المراقبة وضوابطها وقمنا بالاستعانة بها في المبحث الأول للدراسة بعنوان الإجراءات التقليدية في التحقيق الإبتدائي لانها نقطة هامة في موضوع البحث.حيث اختلفنا عنها بإضافة حالات اللجوء للمراقبة.

الصعوبات:

ومن بين الصعوبات التي واجهتنا في إعداد هذه المذكرة:

- صعوبة ضبط الموضوع في خطة شاملة.
- تشعب وعلاقاته بمواضيع أخرى مما لا يسمح لنا بذكرها كلها لاتباعنا المنهجية المعتمدة في إنجاز المذكرة
- صعوبة جمع المعلومات وعدم توفرها

الإشكالية:

هل كفل المشرع الجزائري الحق في الخصوصية الرقمية أثناء إجراءات التحقيق التمهيدي الابتدائي؟ وماهي الضمانات التي تحمي حق الخصوصية أثناء إجراءات التحقيق؟ وهل تم استحداث وسائل جديدة لمكافحة الانتهاكات التي تقع على الخصوصية الرقمية ؟

المنهج المتبع:

يتمثل منهج الدراسة في المنهج الوصفي واعتمدته في تعريف وشرح المصطلحات القانونية والمنهج التحليلي المنصب على تفكيك وشرح النصوص القانونية التي جسدت الآليات التي اتخذها المشرع الجزائري وسيلة لحماية الحق في الخصوصية.

التصريح بالخطة:

قصد الإجابة على هذه الإشكالية وتحليلها واستقصاء مضمونها قسمت الخطة على النحو الآتي:

مبحث تمهيدي تناولنا فيه المصطلحات الخاصة بالموضوع في مطلبين الخصوصية الرقمية ومحلها ومبرراتها من خلال المطلب الأول والتحقيق الجنائي من خلال المطلب الثاني، وفصل أول تناولنا فيه الحق في الخصوصية الرقمية في مواجهة مقتضيات التحقيق التمهيدي في مبحثين: مضاهر حماية الحق في الخصوصية الرقمية في ضل قانون الاجرائات الجزائري في المبحث الأول، الاجرائات التي تعد انتهاكا للخصوصية الرقمية في التحقيق التمهيدي المبحث الثاني

أما الفصل الثاني تناولنا فيه الحق في الخصوصية الرقمية في مواجهة مقتضيات التحقيق الابتدائي في مبحثين المبحث الأول: الإجراءات التقليدي. وفي المبحث الثاني: الإجراءات المستحدثة.

المبحث التمهيدي

مبحث تمهيدي

سيتم في هذا المدخل دراسة بعض المصطلحات الخاصة بموضوع البحث والمتمثلة في؛ الخصوصية الرقمية ومحلها ومبرراتها من خلال المبحث الأول والتحقيق الجنائي من خلال المبحث الثاني كما يلي:

المطلب الأول: الخصوصية الرقمية

ستتم الدراسة في هذا المبحث من خلال التعرف على الخصوصية الرقمية وكذلك محل هاته الخصوصية ومبرراتها من خلال الفروع الآتية:

الفرع الأول: تعريف الحق في الخصوصية

ينعقد شبه إجماع بين الفقه والتشريع على عدم إيجاد تعريف جامع مانع للحق في الخصوصية وهذا يترجم من خلال التعدد التعريفي لهذا المفهوم في إطار النظام القانوني الواحد، ولعل هذه الصعوبة في توحيد المفهوم يرجع إلى طبيعة الحق التي تكتسب صفة المرونة وعدم التحديد والضبط في إطار محدد وتختلف باختلاف المجتمعات الإنسانية والحقب الزمنية عبر العصور.

أولا–الحق في الخصوصية في وجهه التقليدي

وبهذا فقد ذهب العديد من الفقه لإيجاد تعريف الحق في الخصوصية كل وفق توجهاته ومنطلقات الفكرية على اعتبار أن المكونات المنطقية للخصوصية تتسم باضطرادها المستمر في كل حقبة زمنية فعلى سبيل المثال قد بدأت بلورة مفهوم الخصوصية سابقا في إطار المراسلات التقليدية الورقية ومن ثم بدأت الفكرة تتطور إلى حين وصولها إلى الحياة في العالم الرقمي وهنا يتشكل الفرق في جوهر مفهوم الخصوصية.

فوفقا للفقيه «Edward Bloustein» أن الخصوصية هي الحق في حماية الحياة الشخصية للأفراد وضمان عدم الاعتداء عليها واستقلالها[1].

[1] عبد الله عبد الكريم، جرائم المعلوماتية والأنترنت –الجرائم الإلكترونية– دون طبعة، منشورات الحلبي الحقوقية، بيروت، 2007، ص36.

أما وفقا للفقيه « Gavison Ruth» فلقد بني مفهوم الحق في الخصوصية وفقا لـ 3 عناصر السرية والعزلة والتخفي بحيث اعتبر أنه الحق في الحماية ضد التدخل في الحياة الخاصة وشؤون عائلتهم بوسائل مادية مباشرة أو عن طريق نشر المعلومات».

كما يرجع الفقيه هشام محمد فريد رستم قيام مفهوم الحق في الخصوصية بتوافر وجهين أحدهما مادي وقوامه عدم إقحام الشخص في خصوصيات الآخرين، والثاني إعلامي مقتضاه ألا تكون الشؤون الخاصة بالفرد محلا للحق في الإعلام بالنسبة للآخرين مما يستتبع معه عدم استغلال الآخرين لتلك المعلومات بالنشر أو التشهير.[1]

ثانيا-الحق في الخصوصية في العالم الرقمي

وهنا يسند أغلب الفقه والتشريعات فكرة الحق في الخصوصية إلى النطاق الحديث الذي تتناول فيه، والتي يتشكل مفهومها في حق الأفراد أو المجموعات أو المؤسسات أن يحددوا لأنفسهم مدى وصول المعلومات المرتبطة بحياتهم الخاصة للآخرين وبأن يضبط عملية حصر المعلومات الشخصية ومعاملتها آليا، واستخدامها في صنع القرار الخاص أو المؤثر في حياتهم.[2]

وبهذا دل التعريف إلى مفهوم الاستحداث في التعاملات بين الأفراد من خلال معالجة المعلومات الخاصة بهم إلكترونيا وضمان تلك الخصوصية التي تنبع من حصر فكرة الاطلاع على البيانات الشخصية وعدم التطاول عليها من قبل الآخر.

ولقد اتجه غالبية الفقه إلى ربط ولادة مفهوم الحق في الخصوصية المعلوماتية بمخاطر تقنية المعلومات المحيطة بمسألة حماية بنوك المعلومات وعمليات المعالجة الآلية للبيانات الشخصية وبهذا فقد عرفها الفقيه الأمريكي «ويستن Alan Westin» في كتابه المعنون

[1] محمد هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، دون طبعة، مكتبة الآلات الحديثة، مصر، سنة 1992، ص176.

[2] حسام الدين الأهوائي، الحق في احترام الحياة الخاصة، الحق في الخصوصية، دراسة مقارنة، طبعة ثانية، دار النهضة العربية، 2002، ص132.

«**الخصوصية والحرية**» فوفقا له فإن خصوصية المعلومات تعني حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للآخرين.

في حين جاء تعريف الفقيه ميلر في كتابه «الاعتداء على الخصوصية» أكثر عمقا إذ عرفها بأنها قدرة الأفراد على التحكم في سرية المعلومات المتعلقة بهم.[1]

وبهذا فقد نجد أن الحق في خصوصية المعلومات الشخصية يتوقف على فكرة الاعتداء عليها إلكترونيا من قبل الآخر، واستخدامها وفقا لأغراض خارجة عن القانون بدون علم أو إرادة صاحبها.

وبالارتكاز على منحى الخصوصية في وجهها المستحدث نجد التعريف الصادر عن مركز دراسات البيانات المجتمعية والذي أرجع الحق في الخصوصية إلى إمكانية الفرد بالتصرف بشكل قانوني دونما وجود عائق يحول هذا التصرف[2] وبهذا فإن المعنى العميق لمفهوم الخصوصية يتجلى في تبني تلك الرخصة في حرية التصرف وضمان عم التدخل أو التطفل من الغير تحت أي ظرف وهنا نستشف تلك الإضافة التي جاء بها هذا التعريف من خلال تسييج الخصوصية ضد أي خروق تصدر من الأفراد أو حتى من الدولة في إطار ما يعرف بالمراقبة الإلكترونية.[3]

ثالثا-المفهوم التشريعي للحق في الخصوصية

بداية إن مفهوم الخصوصية قد بني في مختلف التشريعات المقارنة تحت إطار ضمان الحد الأدنى في حق الفرد بعدم التدخل أو المساس بالحياة الشخصية أو الأسرية أو خرق لسرية المعاملات أو الحقائق التي تحيط بحياته، وأما الدستور الجزائري قد قرر هذا الحق من خلال نص المادة 39 التي تنص على: «لا يجوز انتهاك حرمة حياة المواطن وحرمة شرفه ويحميها القانون».

---

[1] محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإليكترونية، طبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، سنة 2014، ص 272.

[2] السيد عتيق، جرائم الانترنت، دون طبعة، دار النهضة العربية، مصر، 2002، ص 61.

[3] عبد الفتاح حجازي، الحماية الجنائية المعلوماتية للحكومة الإلكترونية، دون طبعة، دار الكتب القانونية، مصر، 2007، ص33.

أما عن نص المادة 39 فلقد كان النص واضحا مباشرا في تكريس الحماية لحق الخصوصية أما عن نص المادة 40 فقد كانت الإشارة ضمنية تكفل خصوصية الأفراد بعدم خرق حقهم في أن يكونوا آمنين على أنفسهم ضد أي تعسف في التفتيش أو الاحتجاز أو اقتحام المساكن غير مبني على أسس قانونية وهو مظهر من مظاهر الحماية للحياة الخاصة.

وهو نفس الموقف الذي تبناه المشرع الإماراتي من خلال الباب الثالث في المواد 25-44 من الدستور الاتحادي.

الفرع الثاني: محل الخصوصية الرقمية

يتمثل في البيانات الشخصية في:

أولا- تعريف البيانات الشخصية

البيان يجد مرادفه في اللغة الإنجليزية Data وفي اللغة الفرنسية Donnée، ويقصد به من الناحية الفنية، كل تمثيل يمكن أن تخزن فيه المعلومة، يمكن أن يكون نصا أو جدولا أو رسما بيانيا، كما يمكن أن يكون منديلا أو لونا أو إشارة أو أية رموز أخرى، تكون ذات دلالة ومعنى لدى معالج المعلومة[1].

وتقوم مختلف الأنظمة المعلوماتية اليوم في أدائها على تمثيل البيانات تمثيلا رقميا، باستعمال الرقمين 1 و0 فقط .

ومن الناحية القانونية- وغير بعيد عن هذا المعنى-فقد أورد المشرع الجزائري تعريفا للبيانات الرقمية ،حيث عبر عنها بـ "المعطيات المعلوماتية" وعرفها بأنها:" أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها [2].

---

[1] أنظر: كيث دفلين، الإنسان والمعرفة في عصر المعلومات، ترجمة: شادن اليافي، الطبعة الأولى، مكتبة العبيكان، السعودية، سنة2001.

[2] القانون رقم 18-10 المؤرخ في 00 شعبان عام 0021 الموافق ل 5 أوت3118 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية للجمهورية الجزائرية/ العدد 02.

أما البيانات الشخصية فلم يورد لها تعريفا خاصا بها. وهي بحسب اللجنة الوطنية للمعلوماتية والحريات، كل معلومة تتعلق بشخص طبيعي معروف الهوية أو ممكن التعرف على هويته بصفة مباشرة أو غير مباشرة بالرجوع إلى رقم تعريفي أو إلى واحد أو مجموعة من العناصر التي تخصه..."، أو كما تعرفها اتفاقية 108[1]" كل معلومة تتعلق بتحديد هوية الفرد، أو بفرد محدد.

ثانيا- نواع البيانات الشخصية

من خلال التعريفات السابقة يتضح أن البيانات الشخصية تنقسم إلى نوعين أساسيين هما: البيانات المحددة للهوية والبيانات الخاصة.

1- لبيانات الشخصية المحددة للهوية

بالنظر إلى الوسائل والتقنيات المعلوماتية المتعلقة بتحديد هوية الأشخاص، نجد أن البيانات المحددة للهوية تنقسم إلى نوعين من البيانات. يتمثل النوع الأول في الحروف والأرقام والرموز. والتي تتمثل أهمها في كلمات المرور التي تسمح أو تمنع المستخدم من الولوج إلى الحاسوب الشخصي أو قاعدة البيانات أين يعمل أو الولوج إلى البريد الإلكتروني أو البيانات التي يقتضيها إتمام معاملة من معاملات التجارة الإلكترونية. أو تسجيل الدخول إلى منتدى أو حساب شخصي على موقع إلكتروني. فيما يتمثل النوع الثاني في القياسات الحيوية، على غرار بصمة الإصبع، بصمة القزحية، البصمة الصوتية ،بصمة أبعاد الكف، خط اليد (التوقيع، بصمة الوجه... إلخ[2].

2-البيانات الشخصية الخاصة

يتعلق هذا النوع من البيانات بالحياة الخاصة للأفراد وتشمل كل البيانات التي من شأنها الكشف عن الأصل العرقي أو الآراء السياسية أو المعتقدات الدينية أو غيرها، وكذلك

---

[1] المادة الثانية من الاتفاقية حول حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية)108، المجلس الأوربي ستراسبورغ 1981.

[2] منصور بن محمد الغامدي، البيانات الحيوية، البصمة الصوتية، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، 2005، ص 16.

البيانات الشخصية المتعلقة بالصحة أو الحياة الجنسية، أو السوابق العدلية لمخزنة لدى المؤسسات العامة والخاصة في شكل قواعد بيانات، أو في خوادم الشبكات المعلوماتية و تعتبر قواعد البيانات لمختلف المنظمات مصدرا هاما لهذا النوع من البيانات، كذلك المواد الإعلامية المنشورة على صفحات شبكات التواصل الاجتماعي، والبيانات التي تقوم وكالات التحقيق والاستخبارات بتقصيها وجمعها.

الفرع الثالث: مبررات الحق في الخصوصية الرقمية

إن مبررات حماية الحق في الخصوصية الرقمية كثيرة ومتعددة، يمكن إجمالها فيما يلي:

أولا-اتساع شبكة الانترنت:

لقد أثبت الواقع أن أهم التقنيات التي تتحكم في مجموع التعاملات الإلكترونية تعتمد على شبكة الانترنت وهذه الأخيرة ليست بمنأى عن ولوج أي متطفل أو معتدي يستغل شتى الاتصالات التي تترك أثر حتى دون علم مستخدم الشبكة، فتدفق المعلومات والاتصالات عبر الحدود دون أي اعتبار لحدود جغرافية أو سياسية، بحيث يعمل الأف ارد على تبادل المعطيات الخاصة بهم لجهات مختلفة داخلية وخارجية، وهو ما يثير مخاطر إساءة استخدام هذه البيانات خاصة في الدول التي لا تتوفر فيها الحماية القانونية للبيانات الشخصية[1].

ثانيا-الطبيعة الخاصة لقنوات التعامل الإلكتروني:

إن الطبيعة الافتراضية لقنوات التعامل الإلكتروني التي تفتقد إلى المادية تجعل من الشخص وهو بصدد استخدام شبكة الإنترنت يتوقع قدرا من الخفية في نشاطاته أكثر مما هو عليه الحال في العالم الواقعي، بينما الواقع يثبت عكس ذلك على اعتبار أن التعاملات الإلكترونية تترك آثارا ودلالات على شكل سجلات رقمية حول الموقع الم ازر والأمور التي

[1] جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي دون طبعة، دار النهضة العربية، مصر، سنة 2000، ص40.

بحث عنها والمواد التي قام بتنزيلها والوسائل التي أرسلها والخدمات والبضائع التي قام بشرائها، مما يجعله عرضة للقرصنة ثم الاستغلال غير المشروع لها[1].

ثالثا- فقدان المركزية وآليات السيطرة في قنوات التعامل الإلكتروني

يكتسب حق الخصوصية في إطار العالم الرقمي نوعا من التميز إذ أن إقرار قانون فعال يكرس من وجود استراتيجية ملائمة لحماية حق الأفراد بعيدا عن العالم الرقمي قد يكون نوعا من السهولة بحيث يمكن للدولة وضع رقابة على الاعتداءات المختلفة، إلا أن الأمر لن يكون بذات السهولة إذا ما تعلق الأمر بحماية حق الخصوصية المعلوماتية لأن لها ارتباط مباشر بعالم افت ارضي شاسع يرتبط بشبكة الانترنت اللامتناهية الحدود، وهنا يحتدم الصراع على السيطرة على الانترنت من خلال الصعوبة في التحكم في مركزية أسماء النطاقات وعناوين المواقع وغيرها، وهو ما يوسع من دائرة اختراق حق الأفراد ويصعب من الحماية ضد أي انتهاكات لخصوصياتهما[2].

[1] عمر محمد أبو بكر، الجرائم الناشئة عن استخدام الانترنت-الأحكام الموضوعية والجوانب الإجرائية، دون طبعة دار النهضة العربية مصر، سنة20004، ص 398

[2] أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي دون طبعة، دار النهضة العربية، مصر، سنة 2000، ص359.

المطلب الثاني: التحقيق الجنائي

ستتم في هذا المبحث دراسة التحقيق الجنائي والفرق بينه وبين التحقيق التقليدي من خلال المطالب الآتية:

الفرع الأول: تعريف التحقيق الجنائي

التحقيق بمعناها العام "اتخاذ جميع الإجراءات والوسائل المشروعة التي تؤدي إلى كشف الحقيقة وغموضها. فإذا صادف الإنسان حادث ما فإن الطبيعة البشرية تدفعه إلى البحث عن سبب الحادث ومن الذي ارتكبه وكيفية ووقت وقوعه والظروف التي أحاطت به، ثم يخرج الإنسان من كل هذا البحث والتقصي إلى النتيجة التي يراها صواباً في نظره. وكذلك الحال في مجال التحقيق الجنائي فإذا تلقى المحقق بلاغاً أو وقعت جريمة تحركت أجهزة التحقيق سعياً وارء كشف الحقيقة، بمباشرة الإجراءات التي تؤدي إلى اكتشاف الجريمة ومعرفة فاعليها من أجل تقديمهم إلى المحكمة المختصة من أجل معاقبتهم[1] فعرف على أنه: "المرحلة الأولى من م ارحل سير الدعوى الجنائية وينصرف إلى مجموعة من الإجراءات المشروعه يلجأ إليها المحقق قبل المحاكمة في سبيل كشف غموض الجريمة من حيث معرفة فاعلها وسبب ارتكابها ومكان وزمن ارتكابها"، كما عرفه بعض آخر بأنه: "مجموعة من الإجراءات التي تباشرها سلطات التحقيق بالشكل المحدد قانوناً رغبة لتمحيص الأدلة والكشف عن الحقيقة قبل مرحلة المحاكمة"[2].

فتعددت التعريفات الفقهية للتحقيق الجنائي إلا أنها وعلى الرغم من تعددها لا تخرج من مدلول كونها مجموعة من الإجراءات القضائية التي تمارسها سلطات التحقيق بالشكل المحدد قانوناً بغية التنقيب عن الأدلة في الجريمة المرتكبة وتجميعها ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة أو الأمر بألا وجه لإقامة الدعو ى. فالغاية من التحقيق الجنائي الوصول إلى الحقيقة عن طريق جمع الأدلة من خلال الاستماع إلى الشهود

---

[1] خالد محمد عجاج، القاضي علي دايح جريان، "أصول التحقيق الجنائي"، دون طبعة، دار التعليم الجامعي، الإسكندرية، 2018، ص10.

[2] مأمون محمد سلامة، "الإجراءات الجنائية في التشريع المصري"، الجزء الأول، دون طبعة، دار النهضة العربية، القاهرة، 2008، ص641.

والاستعانة بالخب ارء والاعت ارف ومن جهة أخرى تقدير كل ذلك لاتخاذ الق ارر الصحيح إما بالإحالة إلى المحكمة أو عدم السير في الدعوى فالقاعده انه لا يمكن بناء الاتهام دون ان يكون هناك منطق للتحقيق يضمن حق الفرد في مرحلة ما قبل المحاكمة وهذا يبين العلاقة ما بين مرحلة جمع الاستدلالات ومرحلة التحقيق الابتدائي فالهدف لكل منهما هو محاولة كشف الحقيقة-.

ويتضح من ذلك أن الدعوى الجنائية تمر قبل أن توضع أمام القضاء للفصل فيها بمرحلة التحقيق الابتدائي وهي مرحلة جمع الأدلة والتصرف فيها وإن كانت محكمة النقض و قد قضت بان الدعوى الجنائية لا تكون قد بدأت باي إجراء تقوم به سلطات الاستدلال ولو في حالة التلبس بالجريمة، ومن ثم لا تعد إجراءات الاستدلالات من إجراءات التحقيق إلا أن إجراءات الاستدلالات تصاحب إجراءات التحقيق في العادة وتهدف إلى اتخاذ الإجراءات اللازمة لكشف الجريمة ومرتكبيها بالتثبت من وقوعها والبحث عن فاعليها وجمع العناصر اللازمة لأن تكون أساساً لبدء النيابة العامة نظرها في أمر الدعوى مما يعني أن التحقيق له معنيان يقصد بها إجراءات التحقيق التي تقوم بمباشرتها سلطة التحقيق مضافاً إليها إجراءات جمع الاستدلالات التي يقوم به مأموري الضبط القضائي بما فيهم النيابة العامة اذا لم تكن لها سلطة التحقيق والمعنى الآخر يقصد به ما يقوم به قاضي التحقيق أو النيابة العامة في الأحوال التي يباشر فيها التحقيق.

أما تعريف التحقيق الجنائي في الجرائم الإلكترونية فانه "عمل قانوني يقوم به مأمور الضبط القضائي المختص لضبط الجريمة الإلكترونية من فاعل لها ودليل إلكتروني لتقديمهم إلى سلطات التحقيق القضائي المتخصصة في هذا النوع من الجرائم لإقامة العدل[1]

وهناك من عرفه:"بأنه البحث في مستودع السر للمتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه أو الاطلاع على حمل منحه القانون حماية خاصة باعتباره

[1] مصطفي محمد موسي، "التحقيق الجنائي في الجرائم الإلكترونية"، الطبعه الأولى، مطابع الشرطه، القاهره، 2009، ص 169.

مستودع السر بصاحبه فيمكن أن يكون المحل جهاز الكمبيوتر أو أنظمته أو الانترنت للاستدلال بها على صدق نسبة الفعل إلى شخص معين أو كذبه"[1].

ويمكن تعريف التحقيق الجنائي الإلكتروني على أنه" الإجراءات التي يقوم بها مأموري الضبط القضائي أو المحققين عبر العالم الافتراضي لضبط الجريمة الإلكترونية والتثبت من أدلتها ومعرفة فاعلها تمهيداً لإحالتهم للمحاكمة".

الفرع الثاني: التمييز بين التحقيق الجنائي والتحقيق التقليدي

1- التحقيق في الجرائم الإلكترونية يتميز بتطور المفاهيم المستخدمة فيه فأصبح هنالك مصطلحات جديدة تعد أكثر قرباً وملائمة من البيئة الافتراضية والتقنية الذي تباشر فيه إجراءات التحقيق فمثلاً استخدام مصطلح الولوج بدلاً من مصطلح التفتيش واستخدام مصطلح النسخ بدلاً من مصطلح الضبط وهذه المصطلحات تتلائم مع البيئة الافتراضية عنها في الجريمة التقليدية".

2- يعد التحقيق في الجرائم الإلكترونية له ذاتية خاصة ومستقله مستمدة من الطبيعة الخاصة والمميزة للجريمة الإلكترونية عن الجريمة التقليدية فالتحقيق بها لا يعد استثناء على التحقق في العالم المادي فاكثر المساحات الافتراضية التي تنمو فيها الجريمة الإلكترونية هي بيئة شبكات الانترنت وقواعد البيانات والبريد الإلكتروني والنقود الإلكترونية والتجارة الإلكترونية والأسهم والسندات والأنظمة الأمنية الحساسة ونشر الفيروسات والإرهاب الإلكتروني.

3- غالباً ما يتخذ الدليل في الجرائم الإلكترونية شكلاً مغايرا للشكل التقليدي للدليل فالجريمة التي ترتكب بواسطة الكمبيوتر تنشأ في الخفاء وينصب الاعتداء فيها على معطيات الكمبيوتر فالتعامل مع مسرح الجريمة الإلكترونية والتحفظ على الدليل يجعلها تتميز

[1] محمد صلاح محمد عبد المنعم، "الجرائم الإلكترونية وتحدياتها – دراسة مقارنة"، رسالة دكتواره، كلية الحقوق، جامعة المنصورة، 2005، ص234.

بالتحقيق عنها في الجرائم التقليدية[1]، وبالتالي يصعب على المحقق التقليدي أن يفهم حدودها الإجرامية وما تخلفه من آثار غير مرئية.

4- التحقيق في الجرائم الإلكترونية يختلف عن التحقيق في الجرائم التقليدية إذ يصعب توضيحها لهيئة المحكمة ويسهل زرع الشك في وجدانها ويرجع ذلك إلى صعوبة إد ارك المفاهيم التي يشملها موضوع التحقيق والبحث محل الادعاء سيما عدم وجود سلطات تحقيق ومحاكمة متخصصة للتحقيق والفصل في الجريمة الإلكترونية. فاذا كان التحقيق يعتمد على ذكاء.

[1] خالد عياد الحلبي، إجراءات البحث والتحقيق في جرائم الكومبيوتر والإنترانت، دون طبعة، دار الثقافة للنشر والتوزيع، الردن، 2011، ص143.

الفصل الأول:

الحق في الخصوصية الرقمية في مواجهة مقتضيات التحقيق التمهيدي

المبحث الأول: مظاهر حماية الحق في الخصوصية الرقمية في ضل قانون الإجراءات الجزائري

المبحث الثاني: الإجراءات التي تعد انتهاكا للخصوصية الرقمية في التحقيق التمهيدي

لكل شخص حق في الخصوصية بوجه عام يكفلها له القانون ويحميها من أي تعديات ومن بين هاته الخصوصية ظهرت لنا ما يعرف بالخصوصية الرقمية التي سلط عليها المشرع الجزائري الضوء من خلال حماياتها من الانتهاكات سواء بالطرق التقليدية أو طرق مستحدثة.

وبالحديث عن الانتهاكات لابد من معرفة معنى الانتهاك وهو اختراق أو التعدي فانتهاك الخصوصية الرقمية يعني اختراقها أو التعدي عليها ونجد فيها إجراءات خاصة بالبيانات والمتمثلة في الإفشاء غير المشروع لها أو في معالجتها دون ترخيص وهناك إجراءات إلكترونية والمتمثلة في التجسس والتسلل الإلكتروني.

ولحماية هاته الخصوصية من الانتهاكات أورد المشرع الجزائري حماية لها، إما عن طريق الإجراءات التقليدية والمتمثلة في الانتقال والمعاينة وضبط الأدلة وكذلك الاستجواب أو عن طريق إجراءات مستحدثة والمتمثلة في الخبراء والشهادة وللتعرف اكثر على هذا الموضوع قمنا بتقسيم هذا الفصل إلى:

-المبحث الأول: مظاهر حماية الحق في الخصوصية الرقمية في ظل قانون الإجراءات الجزائري

-المبحث الثاني: الإجراءات التي تعد انتهاكا للخصوصية الرقمية في التحقيق التمهيدي

المبحث الأول: مظاهر حماية الحق في الخصوصية الرقمية في ظل قانون الإجراءات الجزائري

يسعى المشرع الجزائري إلى تحقيق العدالة والأمن وذلك من خلال النصوص القانونية التي يجرم من خلالها الانتهاكات ويضع عقوبات لمرتكبيها ففي الانتهاكات التي تقع على الحق في الخصوصية الرقمية فإن المشرع الجزائري سلط الضوء عليها من خلال حمايتها وفق قانون الإجراءات الجزائري وهذه الإجراءات منها ما هو تقليدي كالمعاينة وضبط الأدلة والاستجواب وإجراءات خاصة أو مستحدثة متمثلة في الخبرة والشهادة ولدراسة هذه الإجراءات اكثر لابد من تقسيم هذا المبحث إلى مطلبين لتتم فيهما الدراسة على النحو التالي

المطلب الأول: الإجراءات التقليدية

قبل استحداث إجراءات لحماية الخصوصية كان المشرع الجزائري يلجأ إلى الإجراءات التقليدية من اجل حماية الحق في الخصوصية الرقمية وذلك في ظل قانون الإجراءات ومن بين هاته الإجراءات التي يلجأ إليها المشرع هي المعاينة وضبط الأدلة والاستجواب وهو ما ستتم دراسته من خلال هذا المطلب وفق تقسيمه إلى فرعين وستتم الدراسة على النحو الاتي

الفرع الأول: المعاينة

المعاينة التقنية هي المكان الذي ارتكبت فيه الجريمة، الوعاء الأساسي الذي يحتوي على اخطر الأدلة الجنائية التي يخلفها الجاني وراءه في أعقاب اقترافه الجريمة، وفي لحظة يكون فيها اضطرابه العصبي والذهني قد بلغ قمة الانفعال بصورة لا تتيح المراجعة الدقيقة لأعماله وإزالة الأثار التي يخلفها في مكان الحادث (المجرم مهما كانت دقته سوف يترك وراءه ما قد يشير إلى شخصيته [1]ولذلك كان من الواجب على ضباط الشرطة القضائية الانتقال إلى ذلك المكان لمعاينة وإثبات الأثار المادية للجريمة والمحافظة عليها وإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة، وكذا أخطار النيابة فورا بانتقاله، لكي تنتقل بدورها إلى محل الجريمة في حالة الجناية الملتبس بها ويقصد بالمعاينة رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة، وهي تقتضي

[1] نبيلة هبة هروال. الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات. دون طبعة، دار الفكر الجامعي. الإسكندرية: 2013 ص212

في ذلك سرعة الانتقال إلى محل تلك الواقعة حيث يقوم ضابط الشرطة القضائية بجمع الدلائل والقرائن التي يستدل بها عن الجريمة والتثبيت المباشر لحالة الأشخاص والأشياء والأماكن ذات الصلة بالحادث، وهي المرحلة الأولى للاستدلال حول ملابسات أية جريمة ونظرا لاختلاف الجريمة المعلوماتية كثيرا عن الجرائم التقليدية نظرا لكون مسرحها الإجرامي قد يتعدى حدود الدولة فان المعاينة التقنية تتم باتباع مجموعة من الإجراءات الخاصة التي سنوردها فيما بعد.[1]

وتظهر أهمية المعاينة في أنها تنقل لجهات التحقيق والمحاكمة صورة مجملة لموقع الجريمة بكل ما يحتويه هذا الموقع من تفصيلات سواء تعلقت هذه التفصيلات بمكانه أو وصفه من الداخل أو الأثار الموجودة به، والتي تنقلها بالجريمة وإجمالا كل ما يمكن جهات الشرطة والقضاء من وضع تصور لكيفية وقوع الجريمة واستخلاص بعض الأدلة من المادة التي تم جمعها[2].

وحتى تحقق المعاينة ثمارها وتفي بأغراضها المشهودة، نجد أن بعض التشريعات قد قررت جزاءات جنائية على كل من يقوم بإجراء أي تغيير على حالة الأماكن التي فيها الجريمة أو ينزع أي شيء منها[3] أو يحدث تعديلا في مكان وقوع الجريمة قبل قيام سلطة التحقيق أو الاستدلالات بإجراء المعاينة الأولى أيا كان مرتكبها

وقد نصت المادة 42 من قانون الإجراءات الجزائية الجزائري على المعاينة بشكل عام كإجراء يتم في مرحلة جمع الاستدلالات وهو مخول لجهاز الضبطية القضائية سواء في الحالة العادية أو حالات التلبس، ويترتب على تغيير أو تعديل يطرأ على مكان وقوع الجريمة الجزاءات المنصوص عليها في المادة 43 قانون إ.ج.ج. وحتي يكون التفتيش في بيئة إلكترونية لابد ان يتم علي مستويين تتمثل في تفتيش المكونات المادية للحاسب الآلي والتي

---

[1] عبد العال الديري ومحمد صادق إسماعيل .الجرائم الإلكترونية، ط10.المركز القومي للإصدارات القانونية: القاهرة 2012.ص 264

[2] نبيلة هبة هروال. الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات. مرجع سابق، ص216

[3] عبد الفتاح بيومي حجازي. مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، ط1. دار الفكر الجامعي. الإسكندرية، 2006، ص160.

تمثل مسرح الجريمة التقليدي وأيضا تفتيش المكونات المعنوية للحاسوب والتي تمثل مسرح الجريمة الافتراضي

أولا- مدى صلاحية مسرح الجريمة المعلوماتية للمعاينة

إذا كانت المعاينة في الجرائم التقليدية تتم في مسرح الجريمة العادي فان الجريمة المعلوماتية تتم المعاينة فيها على مستويين.

1-المسرح التقليدي

المسرح التقليدي هو المسرح الذي يقع عادة خارج بيئة الحاسوب ويتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة وهو قريب من مسرح الجريمة التقليدية، ومن أمثلة هذه الجرائم تلك الواقعة على أشرطة الحاسب F.D ، والكابلات الخاصة به وشاشة العرض الملحق به ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسب الآلي ذات الطابع المادي المحسوس (الملموس).[1]

وليس هناك صعوبة مادية لتقرير صلاحية مسرح الجريمة الذي يضم هذه المكونات لمعاينته من قبل ضباط الشرطة القضائية والتحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة ونسبها إلى شخص معين، وكذلك وضع الأختام في الأماكن التي تمت المعاينة فيها، وضبط كل الأدوات والوسائل التي استخدمت في ارتكاب الجريمة مع وجوب إخطار النيابة العامة بذلك

وفي هذه الحالة تتميز المعاينة بالسهولة. باعتبار أنها تتم على عناصر ملموسة كانت محلا للجريمة أو تخلفت عنها.

2/ المسرح الافتراضي

والمسرح الافتراضي يقع عادة داخل البيئة الإلكترونية ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الأقراص الصلبة الموجودة بداخله وفي مقدمة هذه الجرائم الواقعة على برامج الحاسب الآلي أو بياناته أو تتم بواسطتها، وكذلك الجرائم التي تتم

[1] المادة 30/24 القانون رقم 20/51 المؤرخ في 230يوليو 2015 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، الجريدة الرسمية العدد04.

بطريق الانترنت ومنها جرائم التزوير المعلوماتي والتخريب[1] وتتميز المعاينة في العالم الافتراضي بالصعوبة تتمثل في:

– ندرة الأثار المادية التي تتخلف عن الجرائم التي تقع على أدوات المعلومات.

– الأعداد الهائلة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية وحتى يمكن لضابط الشرطة القضائية القيام بالمعاينة في العالم الافتراضي لابد عليه أن ينتقل إلى العالم الافتراضي لمعاينة من مكتبه أو اللجوء إلى مقهى الأنترنت أو إلى الخبراء وغيرها من الأماكن التي تساعده في إظهار الحقيقة.

وللمعاينة في جرائم الانترنت والحاسوب (المعلوماتية) أشكال مختلفة تختلف بحسب نوعية الجريمة المرتكبة على ان هناك طرقا عامة تتوافق مع طبيعة الاتصال بالأنترنت أو الوسيلة التي تستخدم مثلا: وسيلة تصوير شاشة الحاسوب impression de captures d'écran والتي تكون بواسطة آلة تصوير تقليدية أو عن طريق استخدام برمجة حاسوب متخصصة في اخذ صورة لما يظهر على الشاشة وهذا ما يصطلح عليه تجميد مخرجات الشاشة frozen وغيرها[2]

ثانيا– إجراءات المعاينة التقنية

لابد على الضابط الشرطة القضائية اتباع بعض القواعد والارشادات الفنية عند معاينة مسرح الجريمة المعلوماتية، تتمثل هذه الإجراءات في:

– عند العثور على حاسبات الية أو أجهزة أخرى داخل مسرح الجريمة يجب عدم العبث بها ،تدوين الحالة التي هي عليها إذا كانت منطفئة أو في حالة تشغيل موصولة بالكهرباء أو بجهاز لاحق اخر، كما ينبغي ترقيم لواحقها بشكل متسلسل

– يجب تحرير الأوراق المطبوعة على الحاسب الآلي والتي عثر عليها في مسرح الجريمة ووضعها في أكياس حسب حالتها، ويمكن إعادة الطباعة إذا كان الجهاز في حالة تشغيل

---

[1] عبد الفتاح بيومي حجازي. مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت..مرجع سابق. ص162/164

[2] نبيلة هبة هروال. الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات. مرجع سابق. ص218.

وتحرير الأوراق التي تمت طباعتها. بالإضافة إلى تفقد الجهاز وتسجيل ما إذا كانت هناك برامج تم استخدامها لحظة دخول مسرح الجريمة عند العثور على دعائم التخزين (أسطوانات، أقراص، حوامل مغناطيسية يجب ترقيمها وتسجيل الحالة التي هي عليها والمكان الذي وجدت فيها (داخل الحاسب الآلي أو خارجه)[1].

عند الانتهاء من الترقيم يجب تصوير ودمج الأجهزة وملحقاتها في الحالة التي هي عليها يجب تحرير جميع العينات التي عثر عليها من أجهزة ودعائم داخل أكياس خاصة (بلاستيكية أو ورقية كما ينبغي حمايتها من الكسر وتأثير العوامل الجوية وإبعادها عن أي مجال مغناطيسي لتفادي فقدان المعلومات وإرسالها إلى المخبر لإجراء الخبرة تقتضي القاعدة العامة بأن تكون هناك استعانة بالخبراء في المسائل العلمية والتقنية التي تحتاج إلى خبرة خاصة كخبرة الطبيب الشرعي لمعرفة سبب الوفاة فالخبرة في الجريمة المعلوماتية لها أهمية بالغة للتطور السريع والمتلاحق في مجال صناعة الحاسبات والبرمجيات شبكات الاتصال ما قد يصعب على المحقق لا تتبعها واستيعابها[2].

يحتاج خبراء الأدلة الجنائية الرقمية لتأدية أعمالهم التقنية إلى الأدلة الرقمية واكتشاف المعلومات التي يحتويها كل دليل ومن هذه الأجهزة والأنظمة والبرمجيات ما يلي:

- أجهزة بقدرة عالية على التحليل وتخزين المعطيات
- نسخ من مختلف أنظمة التشغيل المستعملة أدى الأفراد والمؤسسات.
- نسخ من برامج حذف وكسر كلمات المرور لمختلف الحاسبات، برامج نسخ الأقراص المدمجة والمحمولة، برامج الضغط وفك الضغط، برامج التشفير وفك التشفير، برامج حماية الأنظمة الشبكات من اختراق برامج كشف الشبكة المخفية من الأقراص الصلبة، برامج استعادة الملفات المحذوفة وبرامج البحث عن الانترنت.

---

[1] وهي اهم إجراء من إجراءات المعاينة من اجل ضبط الدليل الرقمي وايضا كافة الأدلة التي تساعد في الكشف عن المجرم.

[2] ويقصد بها بعث جميع الأدلة التي تم ضبطها في مجال الجريمة المعلوماتية إلى خبراء تقنيين من اجل فحصها وكشف الغموض والقبض علي مرتكبيها .

– ومن أجل التحقيق في الجرائم المعلوماتية يمكن للخبراء اللجوء إلى بعض التقنيات منها: تحديد عناوين IPوعناوين البريد الإلكتروني[1] المستعملة في ارتكاب الجريمة، استخدام تقنيات التخفي عن طريق نظام البروكسيproxy[2] ، استخدام برامج التتبع، تسمح هذه الأخيرة بالتعرف على الأشخاص المشتبه فيهم وتحديد أماكن تواجدهم. كما يتبع المحقق في تحقيقه مناهج وطرق تحري لإثبات وقوع الجريمة وتحديد شخصية مرتكبها منها: افتقار الأثر في الجريمة المعلوماتية كون المجرم غالبا ما يعمد إلى محو أثاره ، يجب على المحقق الاطلاع على مختلف الأنظمة المعلوماتية ومكوناتها من شبكات وتطبيقا وخدمات، كما يجب على المحقق الاطلاع على العمليات التي يقوم بها النظام المعلوماتي المراد التحقيق فيه كقاعدة البيانات، وكيفية عمل الحاسوب ، وخطة تأمينها ، ويمكن الاستعانة بالذكاء الاصطناعي[3] لحصر الحقائق والاحتمالات والأسباب والفرضيات ومن ثم استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها الحاسب الآلي وفق برامج صممت خصيصا لهذا الغرض، حيث أثبتت تقنيات الحاسب الآلي نجاحها في جمع الأدلة الجنائية وتحليل القرائن، وإن من أعمال قاضي التحقيق الانتقال إلى أماكن وقوع الجريمة للمعاينة وضبط ما قد يعثر عليه من آثار وسماع ما قد يجده من شهود في عين المكان قبل أن يقع التأثير عليهم من المتهم أو من أطراف أخرى وهو ما قرره المشرع الجزائري في المادة 97 ق.إ.ج.ج.[4]

وتتم المعاينة في الجريمة المعلوماتية المرتكبة عبر الإنترنت كأي جريمة أخرى عن طريق الانتقال إلى محل الواقعة الإجرامية إلا أن الانتقال هناك لا يكون إلى العالم المادي وإنما إلى العالم الافتراضي أو عالم الفضاء الإلكتروني[5].

---

[1] هو وسيلة للتواصل بين الأشخاص حيث يرسل شخص ما رسالة إلى شخص آخر عن طريق خط تلفوني.

[2] هو باختصار نوع من أنواع الfirewall حيث انه ينظم الحركة بين الشبكة المحلية كشبكة الجامعة وبين شبكة الانترنت حتي يمكن الاتصال بالمواقع الممنوعة

[3] هو سلوك وخصائص معينة تتسم بها البرامج الحاسوبية تجعلها تحاكي القدرات الذهنية البشرية وأنماط عملها.

[4] انظر المادة 97 ق.إ.ج.ج، السابق ذكره

[5] عبد العالي الديري. محمد صادق إسماعيل. الجرائم الإلكترونية . مرجع سابق. ص264.

وحتى تكون المعاينة صحيحة لابد على قاضي التحقيق أن ينتقل إلى مكان وقوع الجريمة بصحبة كاتبه بعد إخطار وكيل الجمهورية المختص إقليميا بجميع الإجراءات اللازمة.

وحتى يستطيع قاضي التحقيق أن ينتقل إلى عالم الفضاء الإلكتروني لمعاينته، عدة طرق تتمثل في:

- الانتقال إلى العالم الافتراضي من المكتب بالمحكمة من خلال الكمبيوتر الخاص به.
- اللجوء إلى مقهى الإنترنت.
- يجوز له اللجوء إلى مقر عمل مزود خدمة الإنترنت server internet provider. الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة.

كما يستطيع قاضي التحقيق أيضا الانتقال إلى العالم الافتراضي للمعاينة من خلال مقر مكتب الخبير التقني المختص.[1]

وبالتالي يتضح مما سبق أن هناك عوائق ومشكلة أمام القاضي التحقيق من خلال الانتقال إلى العالم الافتراضي، حيث يلزم أن يكون هذا الانتقال بالسرعة الكافية التي تمنع زوال آثار الجريمة.[2]

ثالثا: الخطوات الواجب إتباعها قبل الانتقال إلى مسرح الجريمة المعلوماتية:

يجب على المحقق الجنائي (قاضي التحقيق قبل الانتقال إلى معاينة مسرح الجريمة المعلوماتي إتباع الخطوات التالية:

- توفير معلومات مسبقة عن مكان الجريمة، ومالك المكان، نوع وعدة أجهزة الكمبيوتر.
- الحصول على الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل.

---

[1] خالد ممدوح إبراهيم. فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2008، ص158/156.

[2] خالد عياد الحلبي. إجراءات البحث والتحقيق في جرائم الكمبيوتر والانترنت، المرجع السابق ص155.

– قطع التيار الكهربائي عن موقع المعاينة لشل فعالية الجاني من القيام بأي فعل من شأنه التأثير على أو محو آثار الجريمة.

– إعداد فريق بحث من المختصين والفنيين.[1]

رابعا–شروط صحة معاينة مسرح الجريمة

حتى تعطى المعاينة ثمارها للكشف عن الغموض والتوصل إلى الجاني لابد أن يراعي قاضي التحقيق ما يلي:

1/ سرعة الانتقال إلى مكان الجريمة:

فور تلقي المحقق أو قاضي التحقيق البلاغ عن وقوع الجريمة من الجرائم المعلوماتية والتأكد من صحة الواقعة، عليه ان ينتقل إلى مكانها، وذلك ضمانا لعدم التغيير شكل مسرح الجريمة عن الوضع والحالة التي تركها الجاني عليه، والحصول على شهادة الشهود.[2]

2/ السيطرة على مكان وقوع الجريمة:

بمجرد وصول قاضي التحقيق البلاغ عن مكان وقوع الجريمة من أجل معاينتها لابد من أن يتبع مجموعة من الإجراءات التالية:

– منع تواجد أحد بداخل مسرح الجريمة حتى لا يؤثر ذلك على الآثار والأدلة التي تم العثور عليها في المسرح.

– التأكد من عدم لمس أية آثار أو أدوات بداخل مسرح الجريمة.

– التحفظ على كل ما له علاقة بالحادث من أشياء وأشخاص.

– إخطار الخبراء لرفع الآثار والبصمات[3].

---

[1] نبيلة هبة هروال. الجوانب الإجرائية لجرائم الإنترنت. مرجع سابق. ص54.

[2] علي عبد القادر القهوجي. الحماية الجنائية لبرامج الحاسب الآلي. ط.1 دار الجامعة الجديدة للطباعة والنشر: بيروت، 1999. ص58.

[3] خالد ممدوح إبراهيم. فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق ص 159.

الفرع الثاني ضبط الأدلة والاستجواب

أولا-ضبط الأدلة

يعتبر ضبط الأشياء المتعلقة بالجريمة هو الأثر المباشر للتفتيش، ولذلك نجد أن التشريعات الإجرائية تجمع عادة بين أحكام الضبط والتفتيش في موضع واحد لكن ليس معنى ذلك أن الضبط هو التفتيش، إذ قد يكون نتيجة معاينة وغيرها هو ما سنتناوله:

1- مفهوم ضبط الأدلة الإلكترونية:

هو وضع اليد على شيء يتصل بالجريمة ويفيد في كشف الحقيقة عنها وعن مرتكبيها وهو يرد إلا على الأشياء المادية[1] وبالتالي الصعوبة في ضبط أدلة الجريمة الواقعة على المكونات المادية للكمبيوتر بالبصمات مثلا، وإنما تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس وكذا المكونات المعنوية للحاسوب[2] وفي هذا الإطار اختلفت التشريعات الإجرائية والاتجاهات الفقهية حول مسألة ضبط الأشياء المعنوية والكيانات المنطقية التي لا تصلح بطبيعتها محلا لوضع اليد، وانقسم ذلك إلى اتجاهين[3]وهما

الاتجاه الأول: يرى أصحاب هذا الاتجاه انه يمكن تصور إجراء ضبط على الكيانات المعنوية للحاسب الآلي لانتقاء الكيان المادي عنها، وبالتالي عدم صلاحيتها، ومن بين التشريعات التي أخذت بهذا الاتجاه التشريع الألماني

الاتجاه الثاني: يرى أصحاب هذا الاتجاه أن المعطيات المخزنة التي تصلح أن تكون محلا للضبط المنصوص عليه في النصوص التقليدية.

غير أن المشرع الجزائري تدخل بموجب القانون 40/90 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال حيث قررها آليات خاصة منها:

- حجز المعطيات المعلوماتية عندما تكتشف السلطة التي تباشر في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وانه ليس من

---

[1] نبيلة هبة هروال. الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات. مرجع سابق ص246.

[2] خالد ممدوح إبراهيم. فن التحقيق الجنائي في الجرائم الإلكترونية. مرجع سابق. ص284

[3] خالد عياد الحلي. إجراءات البحث والتحقيق في جرائم الكمبيوتر والانترنت. مرجع سابق ص169.

الضروري حجز كل منظومة، يتم نسخ المعطيات محل البحث على دعامة تخزين إلكترونية تكون قابلة للحجز[1].

– حجز هذه المعطيات عن طريق منع الوصول إليها، ويتم ذلك عادة عن طريق الترميز أو بتقييد الدخول إلى تلك المنظومة، أو عن طريق أية وسيلة إلكترونية[2].

– حجز المعطيات ذات المحتوى الجرمي للمجرم[3].

وتقع تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به في قانون العقوبات وقانون الإجراءات الجزائية الجزائري؛ لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون إلا في الحدود الضرورية للتحريات والتحقيقات القضائية[4].

2- أنواع الأدلة الإلكترونية:

من بين الأشياء أو الأدلة التي تضبط وتحتفظ بها في الجرائم المتعلقة بالجريمة المعلوماتية[5] والتي لها قيمة في إثبات تلك الجريمة وتنسبها إلى المتهم:

أ-الورق: على الرغم من ان الكمبيوتر قلل من استخدام أو حجم الأوراق أو الملفات التقليدية حيث يتم حفظ المعلومات لأغراض المراجعة أو التأكد من الشكل العام. للمستند أو الرسالة، وبالتالي فهي تعتبر من الأدلة التي ينبغي الاهتمام بها[6].

ب-ضبط جهاز الكمبيوتر وملحقاته: أي أن وجوده وضبطه امر مهم جد للقول بأن الجريمة الواقعة هي جريمة معلوماتية أو أنها مرتبطة بالمكان أو الشخص الحائز على الجهاز[7] ولأجهزة الكمبيوتر أشكال وأنواع مختلفة الأمر الذي يتطلب على ضباط الشرطة

---

[1] انظر المادة 60 من القانون 40/90 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

[2] انظر المادة 70 من القانون 04/90.

[3] انظر المادة 80 من القانون 04/90.

[4] انظر المادة 90 من القانون 04/90.

[5] محمود إبراهيم غازي. الحماية الجنائية للصوصية والتجارة الإلكترونية. طبعة أولى. مكتبة الوفاء القانونية. الإسكندرية: 2013 ص 702.

[6] خالد ممدوح إبراهيم. فن التحقيق الجنائي في الجرائم الإلكترونية. مرجع سابق ص 274.

[7] خالد عياد الحلبي. إجراءات البحث والتحقيق في جرائم الحاسوب والانترنت. مرجع سابق ص 176.

القضائية المعرفة الكافية التي تؤهله للتعامل معه ومواصفاته بسرعة فائقة اما بنفسه أو بواسطة خبير.

ج-البرمجيات:software إذا كان الدليل الرقمي ينشأ باستخدام برنامج خاص فإن ضبط الأقراص الخاصة بالتثبيت وتنصيب هذا البرنامج امر في غاية الأهمية عند فحص الدليل.

د-وسائل التخزين المتحركة: كالأقراص المدمجة "أقراص الليزر، والاقراص المرئية والأشرطة المغناطيسية وغيرها".[1]

هـ-المودم:modem : وهي الوسيلة التي تمكن أجهزة الكمبيوتر من الاتصال ببعضها البعض عبر خطوط الهاتف.[2]

ثانيا-الاستجواب

الاستجواب هو مناقشة المتهم بالتهم والوقائع المنسوبة إليه ومواجهته بالأدلة القائمة ضده والمتهم حر في الإجابة عن الأسئلة الموجهة عليه ولا يعد امتناعه قرينة ضده، وهو وسيلة تمحيص للتهم أو لنفيها عنه فهو طريق من طرق تقصي الحقيقة ومصدر من مصادر الإثبات وليس وسيلة إثبات.[3]

إذ اعتبر الاستجواب ذو طبيعة مزدوجة فهو أداة اتهام ووسيلة دفاع في آن واحد بحيث يسمح للمتهم أن يحاط بالتهم والوقائع المنسوبة إليه وبكل ما يوجد بالملف من أدلة التي تساعد على كشف براءته.

ويختلف الاستجواب عن السؤال وأن الثاني لا يتطلب مناقشة المتهم في هويته، ومدى خطورته، إعمالا بالمواد.

---

[1] محمود إبراهيم غازي. الحماية الجنائية للخصوصية والتجارة الإلكترونية. مرجع نفسه، ص715.

[2] نهلا عبد القادر المومني .الجرائم المعلوماتية.، ط20.دار الثقافة للنشر والتوزيع، عمان .2010، ص 42.

[3] أحسن بوسقيعة. التحقيق القضائي. ط7، دار هومة للنشر والتوزيع. الجزائر، 2009، ص45.

استجواب المتهم في الموضوع: أي مواجهة قاضي التحقيق المتهم بالتهم المنسوبة إليه ومناقشته فيها مناقشة تفصيلية ومواجهته بالأدلة القاطعة ضده ولابد أن يكون الاستجواب بحضور المحامي طبقا لنص المادة 110/75 ق.إ.ج.ج 101، 102 ق.إ.ج.ج .

الاستجواب الإجمالي للمتهم: يكون في مسائلة جنائية (جنايات وهو إجراء وجوبي إذ تعلق التحقيق بقضية ذات طابع جنائي، يهدف إلى تخليص الوقائع وإبراز الأدلة التي سبق جمعها[1].

1- القواعد التي يلتزم بها المحقق في الاستجواب

يعتبر الاستجواب إجراء من الإجراءات العامة في التحقيق لأن نجاح المحقق في إسناد الواقعة إلى الجاني واعترافه بارتكابها.

وحتى يكون الاستجواب صحيحا لابد أن يتضمن مجموعة من الإجراءات وهو ما سنتناوله بالتفصيل في مالي:[2]

أ- القواعد التي يلتزم بها المحقق قبل إجراء الاستجواب: قبل أن يقوم المحقق بإجراء الاستجواب والمواجهة عليه أن يستعد لها وذلك بإتباع القواعد العامة التالية:

الإلمام الكامل بفهم أقوال الشهود وسائر المتهمين أن يحدد النقاط الجوهرية التي سيتم إيضاحها من المتهم.

فهم فحوى التقارير الفنية التي وضعها الخبراء عن نتائج عملهم في الآثار المستخلصة.

وضع خطة لنفسه يسير عليها في استجواب المتهم.[3]

ب/ القواعد التي يلتزم بها المحقق الجنائي عند البدء في الاستجواب: على المحقق عند البدء في الاستجواب أن يراعي اتخاذ وإتباع القواعد التالية:

- إذا أعلن المتهم عن محاميه لابد من دعوة المحامي لحضور الاستجواب.

---

[1] محمد حزيط مذكرات في قانون الإجراءات الجزائية الجزائري . الطبعة02، دار هومة: الجزائر، 2010ص103/102.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية. مرجع سابق. ص .240

[3] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق. ص 243.

- تفتيش المتهم.

- عدم إكراه المتهم على الاعتراف بأي شكل من أشكال التعذيب.

المطلب الثاني: الإجراءات المستحدث

مع تطور الجرائم وتطور الزمان كان لا بد على المشرع الجزائري من مواكبتهما وذلك من اجل حماية الحق في الخصوصية الرقمية عن طريق الوسائل المستحدثة من اجل ردع مرتكبي هاته الانتهاكات ومن بين هاته الإجراءات المستحدثة نجد الخبرة والشهادة ولمعرفة هاته الإجراءات اكثر لابد من تسليط الضوء عليها من خلال تقسيم هذا المطلب إلى فرعين كالاتي:

الفرع الأول: الخبرة

الخبرة هي إجراء يستهدف استخدام قدرات شخص الفنية أو العلمية والتي لا تتوافر لدى رجال القضاء من أجل الكشف عن دليل أو قرنية يفيد في معرفة الحقيقة بشأن وقوع الجريمة ونسبتها إلى المتهم أو تحديد ملامح شخصيته الإجرامية [1]ولهذا فان للخبرة التقنية في مجال الجريمة المعلوماتية أهمية بالغة حيث أنه لا يستطيع التعامل مع هذه الجريمة إلا شخص ذو دراية وخبرة في مجال الشبكات.

ونظرا لأن الجريمة المعلوماتية لها خصوصيتها فأن الخبير المعلوماتي لابد أن توافر لديهم المقدرة الفنية والإمكانيات العلمية والفنية في المسألة موضوع الخبرة ولا يكفي في ذلك حصول الخبير على شهادة علمية بل يجب مراعاة الخبرة العملية لأنها هي التي تحقق الكفاءة الفنية من اجل كشف الغموض عن الجريمة أو تجميع ادلتها والتحفظ عليها ومساعدة المحقق في إيجاد جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق[2].

[1] أحمد شوقي الشلقاني. مبادئ الإجراءات الجزائية في التشريع الجزائري. الجزء الثاني، الطبعة الخامسة، ديوان المطبوعات الجامعية الجزائر، دون سنة نشر، ص259.

[2] عبد الفتاح بيومي حجازي. مبادئ الإجراءات الجزائية في جرائم الكمبيوتر والانترنت –مرجع سابق ص137

أولا- مهام الخبير

- تركيب الحاسب الآلي وطرازه ونوعه ونظام تشغيله والأنظمة الفرعية التي يستخدمها.

- بيئة الحاسوب أو الشبكة من حيث طبيعتها [1] تركيزها أو توزيعها، نمط ووسائل الاتصال.

- المكان المحتمل لأدلة الإثبات وشكلها وهيئتها.

- الأثار الاقتصادية والمالية المترتبة على التحقيق في الجريمة المعلوماتية[2].

- كيفية عزل النظام المعلوماتي عند الحاجة دون إتلاف الأدلة أو الأجهزة أو تدميرها.

- إمكانية نقل أدلة إلى أوعية دون أخرى والأوعية المادية كالأوراق على أن تكون مطابقة لما هو مسجل على الحاسب الآلي أو النظام أو الشبكة.

ثانيا- ضوابط الخبرة

تخضع الخبرة لمجموعة من الضوابط القانونية والفنية.

1- الضوابط القانونية

وتنحصر في تلك الضوابط القانونية المنصوص عليها في قانون الإجراءات الجزائية كاختيار الخبراء واجبات والتزامات الخبير (الحلف اليمين، وخضوعه للرقابة القضائية.[3]

- القيام بمهامه بنفسه واستجابته لطلبات الخصوم.
- إيداعه التقارير خلال المدة المحددة[4].

2- الضوابط الفنية:

---

[1] عبد الفتاح بيومي حجازي. الإثبات في الجرائم الكمبيوتر والانترنت. دون طبعة، دار الكتب القانونية مصر، 2008، ص187.

[2] صغير يوسف، الجريمة المرتكبة عبر الانترنت. مذكرة لنيل شهادة الماجيستير في القانون، جامعة مولود معمري، تيزي وزو، 2013 ص90

[3] انظر المواد 144، 145، 143، 148، 153 قانون الإجراءات الجزائية الجزائري.

[4] المادة 5 فقرة اخيرة من القانون 40/90 المؤرخ في 41 شعبان 1430 الموافق لـ 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

– تشمل خطوات اشتقاق الدليل الإلكتروني والتي تتمثل في خطوات ما قبل التشغيل والفحص وخطوات التشغيل و تحديد مدن الترابط بين الدليل المادي والإلكتروني ومرحلة تدوين النتائج وإعداد التقارير وتتمثل هذه الضوابط في:

– جمع مجموعة من الأدلة الرقمية وتحصيلها من خوادم المواقع ومن جهاز المعتدي بعد التوصل إلى تحديد النتائج.

– تحليل رقمي لمعرفة كيفية إعداد الأدلة الرقمية ونسبتها وتحديد عناصر حركتها، ثم التوصل في النهاية إلى معرفة بروتوكول الانترنت IP للحاسوب الذي صدرت منه الرسائل والهجمات الإلكترونية

ويرى بعض المتخصصين أن عمل الخبير ألمعلوماتي في اشتقاق وتجميع الأدلة الرقمية يتم عبر 30 مراحل:

المرحلة الأولى تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة من خلال تتبع الحاسبات الخادمة التي دخل فيها المجرم المعلوماتي[1]

المرحلة الثانية: مرحلة المراقبة ويتم بطرق مختلفة، كبرامج مراقبة يمكن تحميلها للبحث عن المشتبه فيه وتسجيل بيانات الدخول وخروج الموقع.

المرحلة الثالثة: فحص النظام ألمعلوماتي المشتبه فيه بعد ضبطه من طرف السلطات المختصة بمكوناته المادية والمعنوية لاشتقاق الدليل وتقديمه للعدالة[2]

الفرع الثاني: الشهادة

إن سماع شاهد بمعرفة ضباط الشرطة القضائية يدخل في عداد ما يسمى سلطته في الحصول على الإيضاحات والهدف من ذلك أن يجمع كل ما يمكن جمعه من المعلومات عن الجريمة ومرتكبيها[3].

أولا: تعريف الشاهد المعلوماتي:

---

[1] خالد ممدوح إبراهيم. فن التحقيق الجنائي في الجرائم الإلكترونية. المرجع السابق، ص280/300.

[2] سعيداني نعيم. آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. مذكرة لنيل شهادة الماجيستير علوم جنائية. جامعة الحاج لخضر – باتنة. 2013/2012 ص171.

[3] خالد ممدوح إبراهيم. فن التحقيق الجنائي في الجريمة المعلوماتية. مرجع نفسه ص257.

الشاهد في الجريمة المعلوماتية هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي، والذي لديه خبرة جوهرية لازمة للدخول إلى نظام المعالجة الآلية للمعطيات

متى كانت مصلحة التحقيق تتطلب التنقيب عن المعلومات داخله ولذلك يطلق على الشخص اسم الشاهد المعلوماتي تمييزا عن الشاهد التقليدي.

ثانيا: من هو الشاهد المعلوماتي؟

ينحصر الشاهد المعلوماتي في عدة طوائف وفئات وهم:

أ/ مشغلو الحاسب الآلي: عامل تشغيل الحاسب الآلي وهو ذلك الشخص المسؤول عن تشغيل الجهاز والمعدات المتصلة به[1] ولابد أن يكون لديه خبرة كبيرة في استخدام الحاسب الآلي ومكوناته عن طريق استخدام هذه البيانات وكيفية إدخال البيانات ثم استخراجها ونقلها ومعالجتها كما يجب أن تكون له خبرة واسعة في الكتابة السريعة عن طريق لوحة مفاتيح الحاسب الآلي[2].

ب/ خبراء البرمجة: أو خطوط البرامج وهم الأشخاص المتخصصين وكتابة أوامر البرامج وهم فئتين:

الأولى: مخططو برامج التطبيقات

الثانية: مخططو برامج النظم

ج/ المحللون: هو الشخص الذي يحلل الخطوات، ويقوم بتجميع البيانات الخاصة بنظام معين ،ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقة الوظيفة بينها.

د/ وهم المسؤولين عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكونات وشبكات الاتصال المتعلقة به[3].

---

[1] عبد الفتاح بيومي حجازي. مبادئ الإجراءات جنائية في جرائم الكومبيوتر والإنترانت مرجع سابق، ص339 –340.

[2] عبد الفتاح بيومي حجازي. الإثبات في جرائم الكمبيوتر والانترنت. مرجع سابق ص18.

[3] هلالي عبد الله، التزام الشاهد في الجريمة المعلوماتية. دون طبعة، دار النهضة العربية، القاهرة، 2006. ص42/32.

هـ/ مديرو النظم؛ وهم الذين توكل لهم أعمال الإدارة في النظم المعلوماتية.[1]

ثالثا: التزامات الشاهد في الجريمة المعلوماتية

يلتزم الشاهد في الجريمة المعلوماتية متى كان على معلومات جوهرية تفيد سير التحقيق بأن يعلم بها جهات التحقيق القضائي والا تعرض للعقوبات المقررة للامتناع عن الشهادة[2]

وترتكز الشهادة على ما يلي:

– طبع الملفات البيانات المخزنة في ذاكرة الحاسب الآلي أو حاملات البيانات الثانوية على أن يقوم بطبعها وتسليمها إلى المحقق طالما أن المصلحة العامة اقتضت ذلك.

– الإفصاح عن كلمات المرور السرية

– الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة حيث يجب على الشاهد الكشف عن مفاتيح الشفرات المدونة[1]

رابعا: شروط الشاهد بالإعلام عن الجريمة المعلوماتية

تتلخص هذه الشروط في:

– أن يكون يصد جريمة معلوماتية وقعت بالفعل سواء كانت جنحة أو جناية

– أن يكون الشاهد المعلوماتي على علم ومعرفة بالمعلومات الجوهرية المتصلة بالنظام المعلوماتي محل الواقعة.

– أن تقتضي مصلحة التحقيق الحصول على هذه المعلومات الجوهرية[3].

– معرفة بيئة الحاسوب من حيث طبيعتها وتركيزها ووسائل ونمط الاتصال

– المكان المحتمل لأدلة الإثبات وشكلها لأثار الاقتصادية والمالية المترتبة علي التحقيق في الجريمة المعلوماتية[1]

---

[1] عبد الفتاح بيومي حجازي. الإثبات في جرائم الكمبيوتر والانترنت. مرجع سابق ص 28.

[2] انظر قانون ق.أ.ج المواد 58 59 وما يليها.

[3] عبد الفتاح بيومي حجازي . مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت. مرجع سابق ص 350/345

مصطلح الشهادة الإلكترونية يطلق على نوع من الشهادة التي لا يكون فيها الشاهد حاضرا فقد تتم مثلا عن طريق وسائل إلكترونية أو رقمية من خلال شبكة الإنترنت.[2]

وقد أعطى قانون الإجراءات الجزائية لقاضي التحقيق الحرية في تحديد الأشخاص الذين يرى فائدة من سماع شهادتهم، سواء كان هؤلاء الأشخاص قد ورد ذكرهم في البلاغ عن الجريمة أو الشكوى منها، أو أي شخص آخر، وذلك تطبيقا للمواد 60، 88، 97، 110، ق.إ.ج.ج[3]

أما بالنسبة لجميع الحكام وضوابط والأشخاص الذين يراد سماعهم في مجال الجريمة الإلكترونية فقد تطرقنا إليها في المبحث الأول من هذا الفصل الاختلاف فقط في الجهة أو السلطة المختصة بسماع الشهود في المبحث الأول من هذا الفصل هي الضبطية القضائية أما المبحث الثاني قاضي التحقيق.

---

[1] عبد الفتاح بيومي حجازي الإثبات في جرائم الكمبيوتر والانترنت. مرجع نفسه، ص 188

[2] عبد العالي الديري. محمد صادق اسماعيل. الجرائم الإلكترونية. مرجع سابق. ص313.

[3] أنظر المواد 60، 88، 97، 110، ق.إ.ج.ج

المبحث الثاني: الإجراءات التي تعد انتهاكا للخصوصية الرقمية في التحقيق التمهيدي

الإجراءات تعني الأساليب والطرق التي تعد انتهاكا أي اعتداء واختراقا للخصوصية الرقمية والتي تقع بطبيعة الحال على محل الخصوصية الرقمية والمتمثل في البيانات الشخصية فيكون هذا الاعتداء أو الانتهاك إما عن طريق إجراءات خاصة بالبيانات والتي ستتم دراستها من خلال المطلب الأول والمتمثلة في إفشاء غير المشروع للبيانات ومعالجة البيانات دون ترخيص وعن طريق الإجراءات الإلكترونية والتي ستتم دراستها من خلال المطلب الثاني والمتمثلة في التجسس والتسلل الإلكتروني وتتم هاته الدراسة وفق ما يلي

المطلب الأول: إجراءات خاصة بالبيانات

تتمثل إجراءات الانتهاك الخاصة بالبيانات المتعلقة بالخصوصية الرقمية إما في الإفشاء غير المشروع لهاته البيانات وإما في معالجتها ولمعرفة معنى ذلك وكيف تتم هاته الانتهاكات لابد من تقسيم المطلب الاتي إلى فرعين حيث سنسلط الضوء في الفرع الأول على الإفشاء غير المشروع للبيانات وسندرس في الفرع الثاني معالجة البيانات دون ترخيص وذلك وفق ما يلي:

الفرع الأول: جريمة التخزين والإفشاء غير المشروع للبيانات الشخصية

إن الحماية الجزائية لحرمة الحياة الخاصة في عصر تقنية المعلومات الحديثة شهدت تطورا في نطاقها ومشتملاتها، ومن ثم اصبح من الضروري توفير الحماية الجنائية لحرمة الحياة الخاصة من صور الاعتداء التي تمس البيانات الشخصية للأفراد،[1] وبهذا الصدد لابد من تحديد ماهية المعلومات والبيانات التي تعرض خصوصية الأفراد للانتهاك وذلك في نطاق مجتمع المعلومات الإلكترونية، إذ يجري التمييز بين المعلومات المجهولة التي لا تدل ولا يستدل منها على شخص من تعلقت به، إذ أن المجهول لا خصوصية له، وبين

[1] محمد احمد الحمادي، تشريعات مكافحة جرائم تقنية المعلومات بدولة الإمارات، بحث مقدم لندوة جرائم تقنية المعلومات بوازرة الداخلية ومؤتمر جرائم تقنية المعلومات بجامعة الشارقة، 2006، ص46.

المعلومات التي تسمح بالتصرف على شخص من تتعلق به،[1] وهذه المعلومات قد تكون معلومات موضوعية لا تعكس أراء شخصية مثل "الاسم، الموطن، الحالة المدنية ،الوظيفة، العقوبات التي تعرض لها الشخص"، فهي من مميزات الشخصية وقد تكون المعلومة ذاتية تحمل أريا ذاتيا عن الغير والمعلومات الموضوعية والذاتية في الغالب تتعلق بالحياة العامة للأفراد غير أن المعلومات الاسمية المخزنة في بنوك المعلومات هي التي تمس حرمة الحياة الخاصة للأفراد.

وتعرف البيانات الاسمية بأنها "البيانات الشخصية التي تتعلق بحرمة الحياة الخاصة للمرء كالبيانات الخاصة بحالته الصحية والمالية والوظيفية والمهنية والعائلية عندما تكون هذه البيانات محلا للمعالجة الإلكترونية، وتبرز خطورة وسائل تقنية المعلومات الحديثة على حرمة الحياة الخاصة عند جمع وتخزين البيانات الاسمية وتشغيلها وعند استخراج هذه المعلومات من ذاكرة النظام وإيصالها إلى الغير أيا كان هيئة حكومية أو غير حكومية أم شخصا طبيعيا، ومن ثم تقع جريمة التخزين غير المشروع للبيانات الشخصية، متى تم ذلك دون رضاء صاحبها أو لاستخدامها لأغراض غير المخصصة لها"[2].

وتتحقق هذه الجريمة على أري في الفقه الجنائي حتى وان كانت الحكومات هي من قامت بأفعال التخزين للبيانات الشخصية ما دامت هذه الأفعال قد حصلت دون سند في القانون أو في غير الحالات التي يصرح بها القانون أو دون امر قضائي، ألا أن التخزين يعد مشروعا متى تم وفقا للقانون أو انه من مقتضيات الصالح العام كما هو الحال في الدول التي تطبق أعمال الحكومات الإلكترونية بموجب قوانين نافذة[3]

وفيما يتعلق بصفة عدم المشروعية التي تلحق أفعال الجمع والتخزين، فقد يكون مصدرها أساليب الحصول على البيانات أو مضمون وطبيعة هذه البيانات.

---

[1] أنظر: محمد احمد الحمادي، تشريعات مكافحة جرائم تقنية المعلومات بدولة الإمارات، بحث مقدم لندوة جرائم تقنية المعلومات بوازرة الداخلية ومؤتمر جرائم تقنية المعلومات بجامعة الشارقة، 2006، ص46.

[2] نائل عبد الرحمن صالح، واقع جرائم الحاسوب في التشريع الجزائي الأردني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنيت المنعقد في كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2000، ص10.

[3] احمد عوض بلال، قاعدة استبعاد الأدلة المتحصل عليها بطرق غير مشروعة، ط1، دار النهضة العربية، 2010، ص92

وأما أركان جريمة التخزين غير المشروع فأن الركن الأول هو محل أو موضوع الجريمة والذي يتمثل بالبيانات الشخصية، أما الركن المادي لها فيتمثل بالحفظ أو التخزين للبيانات الشخصية على نحو غير مشروع إما بانتهاج احدى الوسائل أو الطرق غير المشروعة ذات الطبيعة التقنية، أو معالجة بيانات يحظر القانون معالجتها، أو لأي سبب من أسباب عدم المشروعية سندا للنص القانوني المجرم لهذا السلوك

أما فيما يتعلق بالركن المعنوي للجريمة فأنه يتخذ صورة القصد الجنائي الذي يقوم على عنصري العلم والإرادة، إذ يجب أن يعلم الجاني بالطبيعة الشخصية لهذه البيانات وبعدم مشروعية تخزينها، وان تتجه إرادته إلى حفظها أو تخزينها خلافا لأحكام القانون[1]

وبخصوص جريمة إفشاء البيانات الشخصية، فأن موضوع هذه الجريمة كغيرها من جرائم الاعتداء على البيانات الشخصية، هو البيانات الشخصية المعالجة في الأنظمة الرقمية، أما الركن المادي فيقوم بإفشاء هذه البيانات أو نقلها إلى الغير أو إخباره بها، أما الركن المعنوي فأنه يتخذ صورتين القصد والخطأ غير العمدي، إذ من الممكن إفشاء البيانات الشخصية نتيجة الإهمال وعدم اتخاذ الحيطة الكافية، ومن ثم فأن هذه الجريمة قد تقع عمدا بتوافر القصد الجنائي بعنصرية العلم والإرادة أو أنها تقع خطأ بإهمال أو عدم انتباه أو عدم احتياط أو بأي صورة أخرى من صور الخطأ[2]

تنص المادة 394 مكرر2 [3]في فقرتها الثانية على المعاقبة بالحبس من شهرين إلى ثلاث سنوات وبغرامة من، 1000000 دج إلى 5000000 دج كل من يقوم عمدا وبطريق الغش ب: حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم.

---

[1] بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دون طبعة، منشوارت الحلبي الحقوقية، بيروت ، 2009.

[2] عاقب المشرع الجنائي الفرنسي في قانون العقوبات الفرنسي الجديد في نص المادة) 226-18(كل شخص جمع المعلومات الاسمية بطريقة التدليس أو الخديعة أو أي طريق غير مشروع.

[3] قانون 23/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات. الجريدة الرسمية. الجمهورية الجزائرية. العدد84

وعلى غرار المادة السابقة فإن المشرع أطلق لفظ "المعطيات"، دون أن يخص المعطيات الشخصية بعبارة خاصة. لكن هذا لا يمنع من إمكانية سحب النص وتطبيقه لحماية البيانات الشخصية باعتبارها صنفا من البيانات. هذا إذا ما أخذنا بعين الاعتبار أن الولوج أو البقاء غير المصرح بهما في النظام المعلوماتي هو جريمة من الجرائم المنصوص عليها في هذا القسم، أي القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات. والتي يمكن أن ترتكب بهدف حيازة بيانات شخصية أو إفشائها أو نشرها أو التصرف فيها بأي شكل آخر. كما أن هذه الجرائم شكلية وتعتبر تامة متى حصل الفعل ولا يشترط توافر قصد خاص مهما كان الباعث والغرض من حيازتها أو إفشائها أو نشرها أو استعمالها بأي شكل آخر .

الفرع الثاني: جريمة المعالجة الإلكترونية للبيانات الشخصية دون ترخيص وتجاوز الغاية من المعالجة الإلكترونية

نبحث أولا جريمة المعالجة الإلكترونية للبيانات الشخصية دون ترخيص ثم سنتناول بالبحث جريمة تجاوز الغاية من المعالجة.

أولا- جريمة المعالجة الإلكترونية للبيانات الشخصية.

تقع هذه الجريمة عند قيام شخص مسؤول عن معالجة البيانات الشخصية بمعالجتها في غير الأحوال المرخص بها قانونا ، وتقع كذلك في الأحوال التي تتم فيها معالجة البيانات بعد إلغاء الترخيص الممنوح بالمعالجة أو عند انتهاء مدته

ويتطلب لقيام هذه الجريمة توافر الركن المادي والركن المعنوي لها ويتمثل الركن المادي في المعالجة الإلكترونية للبيانات الاسمية دون التقيد بالإجراءات المقررة قانونا، وتقع الجريمة حتى وان توافر الخطأ في المعالجة الإلكترونية[1]

ومن ثم فأن الركن المعنوي للجريمة يمكن أن يتخذ صورة العمد أو الخطأ، إذ يتحقق العمد بتوافر القصد الجنائي العام وذلك بعلم الجاني بالصفة الاسمية أو الشخصية للبيانات وأن يتوافر لدية العلم أيضا بأن إجراء المعالجة الإلكترونية للبيانات يتم دون مراعاة

[1] انظر: مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، 2001، ص93.

الإجراءات المقررة قانونا ، وان تتجه إرادته لإجراء المعالجة الإلكترونية بأي صورة من صورها، أما صورة الخطأ، فأنها تقع بحصول المعالجة الإلكترونية بإهمال أو بأي صورة من صور الخطأ غير العمدي الأخرى.

ثانيا- جريمة تجاوز الغرض أو الغاية من المعالجة الإلكترونية.

تقع جريمة تجاوز الغرض أو الغاية من المعالجة الإلكترونية بتوافر الركن المادي والركن المعنوي لها، إذ يتوافر الركن المادي لهذه الجريمة بوقوع النشاط المادي المحقق للانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الشخصية، وي ارد بالغرض أو الغاية موضوع المعالجة الإلكترونية، الهدف الذي يتوخى القائم بالمعالجة الإلكترونية تحقيقه، وهو المبرر الوحيد لمعالجة البيانات الشخصية الإلكترونية وتفت رض هذه الجريمة الحصول على البيانات بصورة مشروعة[1].

ويعد النشاط المادي المكون للركن المادي لهذه الجريمة متحققا اذا استغل الجاني البيانات الشخصية في الكشف عن مصادر ثروة صاحب البيانات الشخصية أو معرفة مركزه المالي أو شأن له صله بحياته الخاصة

أما الركن المعنوي لهذه الجريمة فأنه يتخذ دائما صورة القصد الجنائي العام والذي يقوم بتوافر العلم والإرادة، إذ يجب أن يثبت علم الجاني بأن فعله يشكل انحرافا عن الغاية أو الغرض من المعالجة الإلكترونية للبيانات الشخصية، وان تتجه إرادته نحو ذلك، مع الأخذ بنظر الاعتبار انه لا عبره بالبواعث التي تدفع الجاني لارتكاب الجريمة أو الغاية التي يهدف إليها، سواء تمثلت بمنفعة للجاني أو دفع ضرر عنه أو تحقق مصلحة للغير[2]

المطلب الثاني: الإجراءات الإلكترونية

تعتبر الانتهاكات وفق الإجراءات الإلكترونية هي ثاني أنواع الانتهاكات التي تقع على الحق في الخصوصية الرقمية وتتمثل الإجراءات الإلكترونية في الاختراقات والاعتداءات التي تتم في المجال أو النطاق الإلكتروني والمتمثلة في التجسس الإلكتروني وهو ما ستتم

[1] يقصد بالمعالجة الإلكترونية للبيانات عملية إدخال البيانات أو تصنيفها أو توزيعها، أو دمجها مع بيانات أخرى أو تحليلها من أجل أن تعطي معلومة ذات دلالة خاصة أو القيام باسترجاع البيانات الشخصية.

[2] بولين انطونيوس أيوب، المرجع السابق، ص421.

دراسته من خلال الفرع الأول وكذلك الاختراق الإلكتروني وهو ما ستتم دراسته من خلال الفرع الثاني وستكون الدراسة على النحو الاتي:

الفرع الأول: التجسس الإلكتروني

لقد أثبتت التجربة الواقعية أن خطورة استخدام شبكة الانترنت تكمن أساسا في ضعف الوسائل المستخدمة في حماية انتقال البيانات عبر الشبكة، ضف إلى ذلك صعوبة الوصول إلى الأشخاص القائمين بالاعتداء وبهذا فقد ظهر التجسس الإلكتروني كأخطر صور الاعتداءات التي تحدث في إطار التعاملات الإلكترونية وهذا لارتباطه بشكل مباشر باغتصاب سرية المحادثات الشخصية وجل المراسلات والتعاملات التي تتم عبر شبكة الانترنت في كل المستويات.

ولقد عرف التجسس الإلكتروني في مجال المحادثات الشخصية بأنه: "عملية التنصت أو التقاط البيانات التي تنتقل بين جهازين عن بعد عبر شبكة الانترنت"، أو بترجمة الانبعاثات الكهرومغناطيسية الصادرة من الحاسب إلى بيانات وذلك باستخدام أي وسيلة من الوسائل التقنية. [1]

وما يجدر الإشارة إليه أن التجسس الإلكتروني الذي يصدر في سياق خارج عن القانون والممارس من طرف سلطات الدولة يعد من الأساليب المحرمة دوليا وداخليا لانتهاك حق الأفراد، وهذا في حالة ثبوت حصول فعل التجسس بدون إذن مسبق من المحكمة وهذا يدخل في إطار التعسف في استعمال حق الدولة في المساس بحقوق الأفراد تحت مظلة الأمن القومي أو العام.

أضف أن خطورة التجسس الإلكتروني أضحت تأخذ صورة أوسع مما كانت عليه سابقا خاصة في ظل العولمة والتقنيات الحديثة، بحيث لم تعد تقتصر على السلطات أو دوائر المخابرات بل قد أصبحت وسائل التجسس متاحة إلى الأفراد العاديين خاصة في

[1] يأتي هذا التعريف وفقا لما ورد في نص المادة 3 من اتفاقية بودابست لسنة 2001 المتعلقة بمكافحة الإجرام المعلوماتي.

الدول المتقدمة على عكس الدول العربية التي مازالت حركة تسويق أجهزة التجسس من الأمور المستصعبة والتي لا يمكن تداولها بشكل حر ويسير .[1]

ولقد اختلفت الوسائل المتبعة في إطار التجسس الإلكتروني وهذا تبعا لاختلاف ثقافة مستخدمي هذه الوسائل ومن أبرزها اتباع تقنية اعت ارض الاتصال الشبكي التي تقوم على الاعتماد على برامج لتنفيذها ، فيتم التدخل من قبل أحد الأشخاص الخارج عن الاتصالات الشبكية المقامة عبر الانترنت كتبادل النصوص أو الأحاديث الصوتية فيتم التقاط البيانات أو الصور أو التنصت على الأحاديث الصوتية واعت ارض المحادثات المقامة بالصوت والصورة عن طريق الكاميرات أثناء الاتصال .[2]

الفرع الثاني: اختراق الحاسبات الآلية والبريد الإلكتروني

أولا-اختراق الحاسبات الآلية

ذهب البعض من الفقه غلى تعريف جريمة الاختراق بأنها «عملية دخول غير مصرح بها إلى حاسب الآخر عن طريق استخدام برامج متطورة تحت تقنية وخبرة عاليين »[3]

كما ربط البعض الآخر فكرة الاختراق بالمعالجة غير المشروعة للبيانات فعرفه بأنه الولوج غير المصرح به قانونا إلى نظام معالجة البيانات باستخدام الحاسوب .[4]

وبهذا نجد أن عمليات الاختراق لا تقل خطورة عن النماذج السابقة على اعتبار أن الحاسب الشخصي أضحى يمثل أهم الوسائل المتاحة للاتصالات الحد يثة بين الأفراد وأضحى يعتمد عليه كليا كآلية للمراسلات والمعاملات التي تصدر في إطار التعاملات الإلكترونية وبهذا فإن فكرة اختراق الحاسب الشخصي تقوم على أساس الاعتداء على خصوصية وسرية المعاملات وتسخيرها واستغلالها في شتى الأغراض غير المشروعة التي

---

[1] نديم عبده، أمن الكمبيوتر، الفيروسات والقرصنة المعلوماتية وانعكاساتها على الأمن القومي، الطبعة الأولى، دار الفكر للأبحاث والدراسات، بيروت، 1991، ص 86.

[2] محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، الطبعة الأولى، دار النهضة العربية، مصر، 2016، ص 101.

[3] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، الاحكام الموضوعية والجوانب الاجرائية، دون طبعة، دار النهضة العربية، مصر، 2004ص 331

[4] خالد ممدوح إبراهيم، الجرائم المعلوماتية، دون طبعة، دار الفكر الجامعي، مصر، سنة 2004، ص 242 .

تلحق بالفرد عدة خسائر على المستوى المادي والمعنوي ، وهذا ما عبر عنه في السنوات الأخيرة من خلال ما يعرف بالاختراق الأسود أو «مخترقتي القبعة السوداء» وهي مجموعة من المجرمين الإلكترونيين الذين اعتمدوا أسلوب اختراق الحاسبات الشخصية للأفراد بالدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة وتعديل وتحريف وإتلاف البيانات بغرض الاستفادة المادية أو إحداث الضرر المعنوي للضحية، وقد تخل هذه التصرفات في غالب الأحيان في إطار العداءات الشخصية أو السياسية أو الدينية أو القيام بتلك الأفعال لحساب جهات منافسة أو معادية.[1]

ثانيا- جريمة اختراق البريد الإلكتروني

يعتبر البريد الإلكتروني من أحد الوسائل الحديثة في إطار المعاملات الإلكترونية التي تقدمها شبكة الانترنت في تدخل في إطار تسهيل الاتصال الإلكتروني عن طريق تبادل الرسائل

الفوري، وبهذا يعد اختراق البريد الإلكتروني من أهم المخاطر التي تواجه حق الخصوصية وتعرض الفرد إلى انتهاك سرية المعاملات والمراسلات التي تدخل في شتى المجالات وبهذا فإن المقرر وفق القواعد العامة تكريس ضمانات لحماية سرية المراسلات في حدود وضوابط معينة بغض النظر عن الأساليب المستخدمة سواء كانت تقليدية أو حديثة.[2]

[1] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دون طبعة، دار النهضة العربية، مصر، سنة 1994، ص 56.

[2] عمر محمد أبو بكر يونس، المرجع السابق، ص 339

خلاصة الفصل

في الأخير نخلص إلى أن الحق في الخصوصية الرقمية يتعرض إلى العديد. من الانتهاكات تنصب على البيانات الشخصية كإفشائها ومعالجتها دون ترخيص كما تنصب أيضا على الحاسبات الآلية والبريد الإلكتروني ومهما كانت هاته الانتهاكات ومهما تميزت بالخطورة فأن المشرع الجزائري قام بوضع مجموعة من الإجراءات يكفلها قانون الإجراءات الجزائية الجزائري لردعها واختلفت هاته الإجراءات فكانت في بدايتها تقليدية منها المعاينة وضبط الأدلة والاستجواب لتتطور بعدها الجرائم وذلك يؤدي تلقائيا إلى تطور إجراءات الحماية لتواكب هاته الجرائم فتؤدي بدورها إلى ظهور سبل وإجراءات حديثة أو خاصة متمثلة في الخبرة والشهادة وبذلك أصبحت هاته الانتهاكات قليلة مقارنة بما كانت علبه وذلك بفضل أساليب وإجراءات الحماية التي تردع هاته الجرائم ومرتكبيها ليصبح العالم الرقمي والخصوصية الرقمية اكثر أمان واستقرارا مما كانت عليه.

الفصل الثاني:
الحق في الخصوصية الرقمية في مواجهة مقتضيات التحقيق الابتدائي

المبحث الأول: الإجراءات التقليدية في التحقيق الابتدائي

المبحث الثاني: الإجراءات المستحدثة في الحقيق الابتدائي

إجراءات التحقيق الابتدائي هي مجموعة من الأعمال التي تباشرها سلطة مختصة للتحقيق في مدى صحة الاتهام الموجه من طرف النيابة العامة بشان واقعة جنائية معروضة عليها وذلك بالبحث عن الأدلة المثبتة لذلك، والتحقيق مرحلة لاحقة لإجراءات جمع الاستدلال وتسبق مرحلة المحاكمة التي تقوم بها جهة الحكم، وعليه فإن التحقيق يهدف إلى تمهيد الطريق أمام قضاء الحكم باتخاذ جميع الإجراءات الضرورية للكشف عن الحقيقة.

يهدف التحقيق الابتدائي إلى الكشف عن الحقيقة للوصول إلى هذا الغرض يلجا المحقق إلى مجموعة إجراءات بعضها يهدف للحصول على الدليل، وتسمى إجراءات جمع الدليل كالتفتيش والمراقبة يمهد للدليل كالتسريب.

وسوف تقتصر دراستنا على هذه إجراءات التي يكون منها القاضي الجزائي اقتناعه تلقائيا بحكم العقل والمنطق، وهذا من اجل حماية الحق في الخصوصية وسوف تسلط دراستنا على الخصوصية في العالم الرقمي ولمعرفة اكثر على هاته الإجراءات لا بد من دراستها من خلال هذا الفصل وسيتم. ذلك بتقسيمه إلى مبحثين كالاتي

- المبحث الأول: الإجراءات التقليدية في التحقيق الابتدائي
- المبحث الثاني: الإجراءات المستحدثة في التحقيق الابتدائي

المبحث الأول: الإجراءات التقليدية

كلما تطورت التكنولوجيا تطورت معها الجرائم لذلك وجد المشرع الجزائري نفسه مطالب بوضع إجراءات خاصة لحماية الحقوق من الانتهاكات ومن بين هاته الحقوق الحق في الخصوصية الرقمية فالمشرع الجزائري افردها بإجراءات لحمايتها تختلف من التحقيق التمهيدي إلى التحقيق الابتدائي فسلط الضوء على الإجراءات التي تجعل الحق في الخصوصية الرقمية في مواجهة مقتضيات التحقيق الابتدائي فمنها ما هو تقليدي اي إجراءات تقليدية كالتفتيش والاعتراض والمراقبة وهو ما سندسه في هذا المبحث من خلال تقسيم المبحث الاتي إلى مطلبين تتم الدراسة من خلالهما كما يلي

المطلب الأول: التفتيش

يعتبر التفتيش هو أول إجراء تقليدي الذي يباشر أثناء التحقيق الابتدائي وذلك من اجل جمع الأدلة التي تثبت انتهاك الخصوصية الرقمية وذلك من اجل حمايتها وفق إجراء التفتيش ولمعرفة هذا الإجراء وضوابطه وإجراءاته لا بد من دراسته من خلال هذا المطلب وذلك بتقسيمه إلى فرعين وستتم الدراسة كالاتي

الفرع الأول: تعريف التفتيش

لقد تعددت التعريفات التي أضافها الفقه على التفتيش، إلى أنها تجتمع على أن التفتيش عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل وذلك من اجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات القانونية المقررة، وقد أحاط القانون التفتيش بضمانات عديدة لأنه قد يقتضي البحث في محل له حرمة خاصة. وإذا كان التفتيش للأشياء المادية بما فيها المكونات المادية للحاسوب لا يثير إشكالية،

أولا- مدى قابلية نظم الحاسوب للتفتيش

يتكون الحاسوب من مكونات مادية ومكونات معنوية، ولا تثار أدنى صعوبة إذا كان محل جرائم الحاسوب الآلي مكونات مادية حيث ينطبق بصددها القواعد التقليدية دون صعوبة، فالواقع أن ولوج المكونات المادية للحاسوب بأوعيتها المختلفة بحثا عن شيء

يتصل بجريمة معلوماتية قد وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها وأنه يدخل في نطاق التفتيش طالما تم وفقا للإجراءات القانونية المقررة، بمعنى أن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه وهل هو من الأماكن العامة أو الأماكن الخاصة إذ أن لصفة المكان أهمية خاصة في مجال التفتيش.

إذا كانت موجودة في مكان خاص كمسكن المتهم أو احد ملحقاته كان له حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش منزله وبنفس الضمانات المقررة قانونا في التشريعات المختلفة، وبالنسبة للاماكن العامة سواء كانت بطبيعتها كالطرق العامة والشوارع أو كانت بالتخصيص كالمقاهي والمطاعم والسيارات العامة فان الشخص إذا وجد في هذه الأماكن وهو يحمل مكونات مادية للحاسوب أو كان مسيطرا أو حائـزا لها فان التفتيش لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا الصدد.[1]

أما إذا كان محل جرائم الحاسوب الآلي مكونات غير مادية أي معنوية، كبرامج لحاسوب أو بياناته فقد ثار خلاف كبير في الفقه بين مؤيد ومعارض، حيث يذهب رأينا إذا كانت الغاية من التفتيش هو جمع الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم يمتد ليشمل البرامج والبيانات. وقد لجأ الفقه في العديد من الدول استنادا إلى عمومية نصوص التفتيش إلى التوسع في تفسيرها وذلك بمد حكمها إلى البرامج والبيانات المخزنة في أنظمة المعالجة الآلية للمعطيات، وابرز مثال لذلك الفقه الكندي عندما وسع من تفسير المادة487من قانون العقوبات الكندي التي تنص على إمكانية إصدار أمر قضائي لتفتيش أي شيء تتوافر بشأنه أسس أو مبررات معقولة تدعو للاعتقاد بأن الجريمة قد وقعت أو يشتبه فيل وقوعها أو أن هناك نية لاستخدامه في ارتكاب جريمة أو انه سيتيح دليلا على ارتكاب الجريمة. وهكذا فإن هذا النص يفسر على أنه يسمح بضبط وبتفتيش البيانات وبرامج الحاسب الآلي.[2]

---

[1] هلالي عبد. الله تفتيش نظام الحاسب الآلي، وضمانات متهم المعلومات، دراسة مقارنة ، الطبعة الأولى، دار النهضة العربية، مصر، ص74.

[2] كامل عفيفي، جرائم الكمبيوتر دون طبعة، منشورات الحلبي الحقوقية، لبنان، 2003، ص366.

وفي هذا المعنى نجد المادة251 من قانون الإجراءات الجزائية اليوناني تعطي سلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع وحماية الدليل، ويفسر الفقه اليوناني أن عبارة أي شيء تشمل تفتيش البرامج والبيانات المعالجة الإلكترونية.

وعلى النقيض يرى أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم المادي لا ينطبق على برامج وبيانات الحاسب الآلي غير محسوسة، ويقترح هذا الرأي في مواجهة هذا القصور التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة (مواد معالجة إلكترونية)، ولذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هي البحث عن الأدلة أو أي مادة معالجة بواسطة الحاسب الآلي.

والحقيقة أن الحاجة ماسة لتدخل تشريعي لتقرير الضوابط القانونية الكفيلة لتغلب على الصعوبات الإجرائية التي تثار عند تفتيش الأنظمة المعلوماتية، ففي الولايات المتحدة الأمريكية تم تعديل المادة34من قانون الإجراءات الجنائية الفيدرالية عام1970 لتنص على السماح بتفتيش أجهزة الكمبيوتر والكشف عن الوسائط الإلكترونية، كما نص المشرع الانجليزي في القسم الثاني من قانون إساءة استخدام الكمبيوتر الصادر عام1990 على تفتيش نظم الحاسب الآلي جرائم الولوج غير المصرح به على أنظمة الحاسب الآلي، والتعديل غير المرخص به في نظام الحاسب الآلي بدون إذن طالما كان هدف هذا الدخول ارتكاب أفعال غير مشروعة عن قصد، أما إذا كان الدخول مجرد دون نية لارتكاب أفعال غير مشروعة فإن التفتيش ممكن ولكن دون إذن قضائي.[1]

كما قرر المشرع الجزائري بموجب المادة45 من القانون رقم 22/06 المؤرخ في20 ديسمبر 2006، التفتيش في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقرر له بعض الضوابط والقواعد سنراها لاحقا.

زيادة على ذلك فإن المشرع في بعض الدول الأخرى لجأ إلى تقرير بعض القواعد القانونية بغية التغلب على الصعوبات التي قد تثار عند تفتيش الأنظمة المعلوماتية، وشاركه في ذلك الفقه، ومن تلك التشريعات التشريع الهولندي الذي أجاز في المادة25/أ منه للقائم

[1] كامل عفيفي، المرجع السابق، ص 367.

بالتفتيش سلطة تسجيل البيانات الموجودة في النهاية الطرفية التي يتصل بها النظام المعلوماتي دون التقيد بالحصول على إذن مسبق بذلك من قاضي التحقيق وهذا لتذليل الصعوبة الخاصة بوجود النهاية الطرفية للنظام المعلوماتي في منزل أخر غير منزل المتهم، كما أجاز بموجب المادة25منه إلزام غير المتهم كالشاهد والشخص القائم بالتشغيل القائم بتقديم كافة البيانات والمعلومات اللازمة لدخول نظام الحاسب الآلي والتعامل مع سلطة التحقيق في هذا الصدد، وأيضا اتجه المشرع الجزائري بموجب القانون السالف الذكر إلى وضع ضوابط للتفتيش في الجرائم المعلوماتية.[1]

الفرع الثاني: ضوابط تفتيش

إذا كان الوصول إلى الحقيقة يمثل الغاية من الإجراءات، بيد أن تحقيق تلك الغاية لا يكون بأي ثمن، ففي كل الحالات فإن الغاية لا تبرر الوسيلة، فالبحث عن الحقيقة القضائية لا ينبغي أن يكون طليقا من كل قيد، بل إن ذلك يخضع لضوابط معينة، ومن هذا المنطلق يجب أن يخضع التفتيش لضوابط يمكن تقسيمها إلى ضوابط موضوعية وضوابط شكلية:

أولا- الضوابط الموضوعية

تنحصر هذه الضوابط فيما يلي:

1- وقوع جريمة معلوماتية:

والجريمة المعلوماتية هي كما سبق القول كل فعل غير مشروع يكون الحاسوب الآلي وسيلته أو محله وذلك لتحقيق أغراض غير مشروعة، وهناك العديد من التشريعات التي حرصت على استحداث نص خاص للجريمة المعلوماتية كما هو الحال بالنسبة لإنجلترا التي أصدرت قانون إساءة استخدام الكمبيوتر في 29يونيو1990، وفي فرنسا صدر قانون رقم19/88في 5يناير1988 وهو خاص بالغش المعلوماتي الذي تم تعديله مع صدور القانون العقوبات الفرنسي الجديد الذي بدأ العمل به اعتبارا من أول مارس 1994.

2- اتهام شخص أو أشخاص معينين بارتكاب الجريمة المعلوماتية أو المشاركة فيها:

[1] هلالي عبد الله، تفتيش نظام الحاسب الآلي، المرجع السابق، ص75.

فينبغي أن يتوفر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية، سواء بصفته فاعلا أو شريكا، بحيث أنه إذا لم تتوافر هذه الدلائل كان على قاضي التحقيق أن يصدر أمر بأن لا وجه للمتابعة، وهذا ما تؤكده المادة 163من قانون الإجراءات الجزائية الجزائري[1] والمادة177من قانون الإجراءات الجزائية الفرنسي.

وفي مجال المعلوماتية يمكن القول أن تعبير الدلائل الكافية يقصد به مجموعة المظاهر والدلائل التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة وكذلك على خبرة القائم بالتفتيش والتي تنسب الجريمة المعلوماتية إلى شخص معين سواء بصفته فاعلا أو شريكا.[2]

3-توافر قرائن على وجود أشياء لدى المتهم المعلوماتي أو غيره تفيد في كشف الحقيقة:

فلا يكفي مجرد وقوع جناية أو جنحة بل يجب أن تتوافر قرائن قوية على وجود أشياء تفيد كشف الحقيقة، ويستوي أن تكون هذه الأشياء المعلوماتية موجودة في حيازة الشخص أو في منزله.

وهكذا فإن التفتيش لا يجري إلا إذا توافرت لذا المحقق أسباب كافية على أنه يوجد في المكان أو لدى الشخص المراد تفتيشه أدوات استعملت في الجريمة المعلوماتية أو أشياء المتحصلة منها أو أية أشياء أخرى أو مستندات إلكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم المعلوماتي أو غيره.

4-جراء التفتيش لنظم الحاسوب الآلي من قبل سلطة مختصة بالتحقيق:

يجب أن يقوم بتفتيش نظم الحاسوب الآلي سلطة مختصة بالتحقيق، وقد جعل المشرع المصري الاختصاص بالتفتيش كإجراء التحقيق في الجرائم التقليدية للنيابة العامة بصفة أصلية ولقاضي التحقيق في حالات خاصة وذلك على خلاف التشريع الفرنسي والجزائري

---

[1] تنص المادة 163 من قانون الإجراءات الجزائية الجزائري على ما يلي:" إذا رأى قاضي التحقيق أن الوقائع لا تكون جنحة أو جناية أو مخالفة أو أنه لا توجد دلائل كافية ضد المتهم أو أن مقترف الجريمة ما يزال مجهولا، أصدر أمر بألا وجه لمتابعة المتهم.

[2] أمال قارة، المرجع السابق، ص59.

الذين أناطا الاختصاص الأصيل بقاضي التحقيق، أما النيابة العامة فلا تختص بالتفتيش إلا في حالات معينة كالتلبس، أما انجلترا فإن معظم الإجراءات الجنائية منوطة بالشرطة القضائية ما عدا بعض الجرائم التي تناط بالمدعي العام.[1]

ثانيا-الضوابط الشكلية

بالإضافة إلى الضمانات الموضوعية لتفتيش نظم الحاسب الآلي، توجد ضمانات شكلية يجب مراعاتها عند ممارسة هذا الإجراء صونا للحريات الفردية من التعسف أو الانحراف من استخدام السلطة وهي كالتالي:

1- الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش الخاص بنظم الحاسوب الآلي:

والهدف من ذلك ضمان الاطمئنان إلى سلامة الإجراء وصحة الضبط، وقد استوجب المشرع الجزائري في المادة 1/45أن يتم التفتيش في حضور صاحب المسكن الذي يجري فيه التفتيش وكذلك المشرع الفرنسي استوجب في الفقرة الأولى من المادة57من قانون الإجراءات الجنائية حضور صاحب المسكن الذي يجري فيه التفتيش وعدم حضوره يترتب عليه البطلان للتفتيش.

غير أن المشرع الجزائري بموجب المادة45 من القانون رقم22/06المؤرخ في 20 ديسمبر2006، استثنى إجراء الحضور لبعض الأشخاص، إذا تعلق الأمر بالتفتيش في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، لكنه أوجب الحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات، لكن إذا تعلق التفتيش بمسكن موقوف صاحبه للنظر أو محبوس في مكان أخر أوجب المشرع بموجب المادة 47 حضور شاهدين مسخرين أو بحضور ممثل يعينه صاحب المسكن محل التفتيش.

2- محضر تفتيش نظم الحاسب الآلي:

فإن التفتيش من أعمال التحقيق فينبغي تحرير محضر به يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة، ولم يتطلب القانون شكلا خاصا في محضر التفتيش،

[1] هلالي عبد الله. تفتيش نظام الحاسب الآلي، المرجع السابق، ص76.

وبالتالي فإنه لا يشترط لصحته سواء ما تستوجب القواعد العامة في المحاضر عموما والتي تقضي بأن يكون المحضر مكتوب باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره وأن يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها.[1]

3-الميقات الزمني لإجراء تفتيش نظم الحاسوب الآلي:

حرصا على عدم التضييق من نطاق الاعتداء على الحرية الفردية وحرمة المسكن حرصت التشريعات الإجرائية على حضر القيام بتفتيش المنازل وما في حكمها في وقت معين، فالقانون الفرنسي ينص في المادة 59 من قانون الإجراءات الجزائية على أن التفتيش لا يمكن أن يبدأ قبل الساعة السادسة صباحا وبعد التاسعة مساءا، ولقد أخذت بعض التشريعات العربية بمبدأ عدم جواز تفتيش المنازل ليلا كقانون التونسي والجزائري، أما بالنسبة لتشريعات الدول الانجلسكسونية كالقانون الإنجليزي والأمريكي فإنها لا تقيد التفتيش بوقت معين.

لكن المشرع الجزائري بموجب المادة47 من قانون الإجراءات الجزائية الجزائري قرر إجراء التفتيش والمعاينة والحجز في كل ساعة من ساعات الليل والنهار أو الليل وفي كل محل سكني وغير سكني، بناء على إذن مسبق من وكيل الجمهورية المختص، إلا أنه أوجب الحفاظ على السر المهني.

د-أن يتم التفتيش بناء على إذن مكتوب: إذا نصت المادة 44 من قانون الإجراءات الجزائية الجزائري على ضرورة أن يكون التفتيش بناء على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا إذن قبل الدخول إلى المكان والشروع في تفتيش نظم الحاسوب الآلي.

إن التفتيش لنظم الحاسوب الآلي يتطلب مذكرة قضائية تجيز تفتيش أنظمة الكمبيوتر، فإجراء التفتيش دون تلك المذكرة مسالة تثير الكثير من المعارضة خاصة في ظل ما يتقرر

[1] هلالي عبد الله تفتيش نظام الحاسب الآلي، مرجع سابق، ص77.

من قواعد تحمي الخصوصية وتحمي حقوق الأفراد. ويجب أن تكون المذكرة واضحة في تحديد النظام محل التفتيش.[1]

ثالثا-الضبط في مجال الجريمة المعلوماتية

منح المشرع في المادة 63[2] صلاحية القيام بالتحقيقات الابتدائية لأعوان الضبطية القضائية بشرط أن تكون تحت رقابة ضباط الشرطة القضائية.

1- فيما يخص التوقيف للنظر

إن التحقيق الابتدائي في الجرائم الخطيرة المذكورة في المادة16 من قانون الإجراءات الجزائية أصبح عسيرا وصعبا، خاصة وأن مرتكبي هذه الجرائم أصبحوا يستعملون أساليب متعددة، وحديثة ومعقدة.

وأصبحت مدة الوضع تحت النظر لا تتماشى ومتطلبات التحقيق الأولي، مما جعل المشرع الجزائري يعدلها بالمادة51 والتي نصت على انه: "**يمكن تمديد أجال التوقيف للنظر بإذن مكتوب من وكيل الجمهورية المختص:**

- مرة واحدة عندما يتعلق الأمر بجرائم الاعتداء على أنظمة المعالجة الآلية للمعـــطيات."

نلاحظ أن المشرع ربط تجديد مدة التوقيف للنظر بطبيعة الجريمة موضوع التحري واشترط أن يكون تمديد المدة بإذن مكتوب من وكيل الجمهورية وأثناء التحقيق الابتدائي كثيرا ما يقوم ضباط الشرطة القضائية باستدعاء أشخاص لإجراء التحقيق، إلا أنهم لا يمتثلون للاستدعاءات الواردة إليهم مما يقلص من فعالية وسرعة التحقيق لذا استوجب الترخيص لرجال الضبطية القضائية استعمال القوة لإحضارهم.

---

[1] أمال قارة، الحماية الجزائية للمعلومات في التشريع الجزائري الطبعة الأولى، دار هومة للنشر والطباعة، الجزائر، 2006، ص62.

[2] تنص المادة 63 من الأمر 155/66 المؤرخ في 18صفر 1836 الموافق ل8يونيو 1966 المتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم، الجريدة الرسمية العدد 47 على ما يلي: "يقوم ضباط الشرطة القضائية وتحت رقابتهم أعوان الشرطة القضائية بالتحقيقات الابتدائية بمجرد علمهم بوقوع الجريمة إما بناء على تعليمات وكيل الجمهورية وإما من تلقاء نفسه"

2- استعمال القوة لإحضار الأشخاص

جاء بالمادة 65الفقرة الأولى[1]أنه يجوز لضباط الشرطة القضائية بعد الحصول على إذن مسبق من وكيل الجمهورية المختص أن يستخدم القوة العمومية لإحضار الأشخاص الذين لم يستجيبوا لاستدعاء للمثول.

هذه المادة تتيح استعمال القوة لإحضار الأشخاص أمام الضبطية القضائية لأخذ أقوالهم بشرط أن يكون إحضارهم بترخيص من وكيل الجمهورية المختص، ولا يمكن إبقاؤهم في حالة التوقيف إلا للمدة اللازمة لأخذ أقوالهم بشرط أن يكون قد تم استدعائهم مرتين على الأقل ولم يمتثلوا.

حتى يحقق التفتيش غايته في جمع الأدلة الإجرامية لا بد من وسيلة التقاط تلك الأدلة وهذه الوسيلة هي الضبط والضبط في معظم الأحيان يكون هو غرض التفتيش وإن لم يكن هو السبب الأوحد له فقد يأتي الضبط لأسباب أخرى غير التفتيش مثل المعاينة.

ويقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها وهو من حيث الطبيعة القانونية من إجراءات الاستدلال أو التحقيق، وتتحدد طبيعته بحسب الطريقة التي تم فيها وضع اليد على الشيء المضبوط، فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضى الأمر تجريده من حيازته كان الضبط بمثابة إجراء تحقيق أما إذا كان الاستيلاء عليها دون الاعتداء على حيازة قائمة فإنه يكون بمثابة استدلال.[2]

وإذا كانت الجرائم الواقعة على المكونات المادية للحاسوب الآلي لا يثير صعوبة للتقرير بصلاحية هذه الجرائم لضبط أدلتها، ذلك أن الضبط لا يرد بحسب الأصل إلا على أشياء مادية، إلا أن الأمر بالنسبة للجرائم الواقعة على المكونات المعنوية للحاسوب الآلي، يثير مشاكل بالنسبة لضبط أدلتها. وقد اختلف الفقهاء بين مؤيد ومعارض. ونجد المشرع

---

[1] تنص الماد 1/65من قانون الإجراءات الجزائية الجزائري على ما يلي: "إذا دعت مقتضيات التحقيق الابتدائي ضابط الشرطة القضائية إلى أن يوقف للنظر شخصا مدة تزيد عن 48 ساعة فإنه يتعين عليه أن يقدم ذلك الشخص قبل انقضاء هذا الأجل إلى وكيل الجمهورية"

[2] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مرجع السابق، ص162.

الجزائري قد أجاز بموجب المادة 47الضبط أو الحجز في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في محل سكني أو غير سكني، وفي ساعة من ساعات النهار أو الليل بإذن مسبق من وكيل الجمهورية.

ومن اجل ضبط أدلة الجريمة فإن المشرع الجزائري بموجب مواد65 مكرر إلى 65 مكرر 10 أجاز اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، إذا اقتضت ذلك ضرورة التحقيق الابتدائي بإذن من قاضي التحقيق لمدة أربعة أشهر قابلة للتجديد، وتنفذ العمليات المأذون بها تحت مراقبة مباشرة لقاضي التحقيق، وتتم العمليات المحددة دون المساس بالسر المهني المنصوص عليه في المادة45.

ويبقى أن نتساءل عما إذ يجوز لضباط الشرطة القضائية الاطلاع على محتويات الحاسوب الآلي التي يتم ضبطها.

أجاب القسم110من قانون الإجراءات الجنائية الألماني على هذا التساؤل بقوله إن سلطة الاطلاع على مطبوعات الحاسوب الآلي وحاملات البيانات الأخرى تقتصر على المدعي العام فقط ولا يكون ضباط الشرطة القضائية الحق في قراءة البيانات عن طريق تشغيل البرامج أو الوصول إلى ملفات البيانات المخزونة دون إذن الشخص الذي له حق نقل هذه البيانات لكل ما لهم هو مجرد فحص حاملات البيانات والبرامج دون استخدام أية مساعدات فنية.[1]

وإذا كان الأمر يبدو محسوما من الناحية النظرية في بعض التشريعات التي قالت بصلاحية البرامج ومعلومات وبيانات الحاسوب الآلي للضبط، إلا أن المسالة عند التطبيق تأخذ بعد أخر، إذ لا يمكن ضبط مكونات الحاسوب الآلي المعنوية بعد تفتيشها إلا إذا نقلت من صورتها المعنوية إلى صورتها المادية، فلا بد من حصرها وجمعها في حيز مادي، ويتم ذلك بإخراجها على الورق أو بأخذ تسجيل منها أو جمعها على أقراص مرنة أو ممغنطة.

إلا أن السؤال الذي يطرح نفسه، إلى أي حد يمكن اعتبار هذه المخرجات بصورتها المختلفة مستندات تصلح أن تكون أدلة إثبات مقبولة أمام القضاء؟

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترانت، مرجع السابق، ص163.

القاعدة في الدعاوى الجزائية هي جواز الإثبات بكافة طرق الإثبات القانونية ،والقيد على هذه القاعدة أن الدليل يتعين أن يكون من الأدلة التي يقبلها القانون، وبالتالي تظهر أهمية اعتراف القانون بالأدلة ذات الطبيعة الإلكترونية خاصة مع احتمال ظهور أنشطة إجرامية عديدة.

المطلب الثاني: المراقبة الإلكترونية

لم يكتفي المشرع الجزائري بالتفتيش كإجراء تقليدي بل تعداه إلى المراقبة ليواكب بعض الجرائم التي لا ينطبق عليها إجراء التفتيش ولمعرفة المرقبة اكثر وكيف تتم كلن لابد من دراستها وفق هذا المطلب من خلال تقسيمه إلى فرعين حيث يتضمن الفرع الأول تعريف المراقبة ويتضمن الفرع الثاني شروطها وسيتم ذلك وفق ما يلي:

الفرع الأول: تعريف المراقبة الإلكترونية:

المشرع الجزائري لم يتصدّ لضبط تعريف المراقبة الإلكترونية لا في مواد قانون الإجراءات الجزائية ولا في مواد القانون رقم 04/09 المتعلق بالقواعد الخاصّة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،[1] وإنّما ترك ذلك للفقه الذي اختلف هو الأخر في ضبط تعريف دقيق وموحّد لإجراء المراقبة الإلكترونية، حيث عرّفها بعض الفقه بأنّها إجراء يتعمّد فيه الإنصات والتسجيل ومحلها المحادثات الخاصّة سواء أكانت مباشرة أو غير مباشرة أي سواء كانت ممّا يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الاتصال السلكيّة واللاسلكية.[2]

أمّا البعض الأخر فقد عرّفها بأنّها: " إجراء تحقيق يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانوناً بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها ويتضمن من ناحية استراق السمع ومن ناحية أخرى حفاظه على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض "

---

[1] القانون رقم 04/09 المؤرخ في 10، اوت 2009 يتضمن القواعد الخاصّة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الصادر في الجريدة الرسمية للجمهورية الجزائرية، العدد 47، المؤرخ في 16اوت2009

[2] عوض محمد عوض، المبادئ العامّة في قانون الإجراءات الجنائيّة، دون طبعة، دار المطبوعات الجامعية، الإسكندرية، مصر، 1999ص400

كما تعرّف كذلك بأنها مراقبة شبكة الاتصالات أو هو العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع المعطيات والمعلومات عن المشتبه فيه سواء كان شخصاً أو مكاناً أو شيئاً حسب طبيعته، مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض أخر.[1]

كما نشير في هذا المقام إلى تصدّي بعض التشريعات لتعريف إجراء المراقبة الإلكترونية مثل التشريع الأمريكي الذي عرّفها في المادة04/2510 من قانون الاتصالات الفدارلي الأمريكي لسنة 1986 بأنّها: " عملية الاستماع لمحتويات أسلاك أو أي اتصالات شفو ية عن طريق استخدام جهاز إلكتروني أو أي جهاز أخر "، وطبقاً لقانون الاتصالات الإلكترونية الأمريكي لسنة 1986 أصبح التعريف المذكور يشمل الاتصالات الإلكترونية الأخرى.[2]

كما قامت لجنة خبراء البرلمان الأوروبي بمناسبة اجتماعها المنعقد بستراسبورغ في06اكتوبر 2006، لدراسة أساليب التحرّي التقنية وعلاقتها بالأفعال الإرهابية، بتعريف إجراء المراقبة الإلكترونية بأنها: " عملية مراقبة سرية المراسلات السلكية واللاسلكية وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو مشاركتهم في ارتكاب جريمة ".[3]

من خلال التعريفات السابقة يتضح لنا أنّ مفهوم المراقبة الإلكترونية يعني التنصّت ومن ناحية أخرى التسجيل، بالإضافة إلى إشارة تلك التعريفات إلى محل المراقبة الإلكترونية وهي الأحاديث الشخصية والمحادثات السلكية واللاسلكية فضلاً عن تبيان التعريفات السابقة ضرورة حصول التنصّت أو التسجيل خلسة دون علم صاحب الحديث وبواسطة إحدى الوسائل أو الأدوات العلمية الحديثة.[4] كما أكّدت أغلب التعريفات على ضرورة أن تتم عمليّة

---

[1] بوكر رشيدة، جرائم لاعتداء على نظم المعالجة الآلية للمعطيات في التشريع الجزائري والمقارن، الطبعة الأولى، منشوارت الحلبي الحقوقية، لبنان ، 2012، ص 370.

[2] ياسر الأمير فاروق، مراقبة الأحداث الخاصة في الإجراءات الجزائية الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، مصر، 2009، ص139.

[3] بوكر رشيدة، مرجع سابق، ص 442.

[4] أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 12-13، مذكرة مقدّمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، السنة الجامعية، 2013/2012، ص80.

المراقبة الإلكترونية من طرف جهات مختصّة وبإذن من الجهات القضائيّة ذات الصلة. المراقبة الإلكترونية في الغالب تنصب على المراسلات الإلكترونية مهما كان نوعها أو البرنامج الذي تمّت بواسطته، حيث يهتم القائمون بعمليّة المراقبة بإخضاع كل المراسلات الإلكترونية لعمليّة الاعتراض والمراقبة، في المراسلات تعتبر مصد اًر غنياً لتحصيل أدلة إثبات الجريمة المعلوماتيّة ومن بين أنواع المراسلات التي يتم مراقبتها في الوقت الحالي هي تلك التي تتم عبر البريد الإلكتروني وعبر برنامج الفيسبوك أو برنامج الماسنجر أو الفايبر والسكايب وغيرها العديد من برامج التواصل الإلكتروني، كون تلك البرامج من أكثر الوسائل الحديثة استخداماً للاتصال عبر الانترنت وتعتبر مجالاً خصباً للربط بين الأشخاص في مختلف أنحاء العالم بسرعة فائقة وبدون حواجز.[1]

كما أنّ اتفاقية مكافحة الجريمة المنظمة غير الوطنية المنعقدة في باليرمو الايطالية قد جاء فيها الدعوة إلى ممارسة المراقبة الإلكترونية بمختلف أنواعها باستثناء التسليم المراقبة وعمليّات التسرّب وبالتالي فإن لفظ مراقبة (يتضمّن الأساليب الجديدة للشرطة القضائية في التحقيقات باستخدام وسائل التكنولوجيا المعاصرة وهي: التنصت على البريد الإلكتروني الذي يحتوي الرسائل النصيّة وغيرها من البرامج الإلكترونية كأجهزة الاستماع وتحديد الأماكن وأجهزة الفيديو وتمدّد المراقبة لتشمل الاتصالات والتنقّلات أو أي تصرّف أخر مشبوه.[2]

كما يمكن للمراقِب الإلكتروني القيام بعمليّة المراقبة من خلال برنامج الفيديو وفتح كاميرا جهاز المراقَب دون علمه عندما لا يمكن استعمال الأساليب التقليديّة لذلك بسبب خصائص المكان الذي يوجد فيه الشخص المشتبه فيه وخاصّة عندما ينشط هذا الأخير في مناطق تشهد نسبة عاليّة من الإجرام.

كما أنّ أغلب أنظمة التواصل الإلكتروني حالياً والتي تكون محلاً للمراقبة الإلكترونية تعتمد نظام للتراسل باستخدام شبكات الحاسب والذي يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقمياً في صندوق خاص وشخصي للمستخدم ولا

---

[1] براهيمي جمال، التحقيق الجنائي في المراقبة الإلكترونية، أطروحة مقدّمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية جامعة مولود معمري تيزي وزو، السنة الجامعية 2017/2018ص 90

[2] مجراب الدوادي، الأساليب الخاصّة للبحث والتحرّي في الجريمة المنظّمة، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة الجزائر 10، بن يوسف بن خدّة، الجزائر، السنة الجامعية 2015/2016ص 203

يمكن الدخول إليه إلاّ عن طريق كلمة مرور،[1] كما تأخذ المراسلات الإلكترونية شكل محادثات فوريّة وهي نوع من المحادثات يتم عبر شبكة الانترنت وتبعاً لذلك تأخذ الاتصالات الإلكترونية شكل مراسلات مكتوبة أو محادثات شفويّة.[2]

وبسبب التطوّر التكنولوجي الهائل الذي تشهده البشريّة اليوم، فمن المتوقّع ظهور وسائل وأساليب جديدة لتبادل المراسلات وربط الاتصال بين الأفراد.

الفرع الثاني: ضوابط المراقبة الإلكترونية

يعتبر إجراء الإلكترونية إجراء خطير جداً باعتباره ينتهك أهم الحقوق المكفولة دستورياً وهي سريّة المراسلات والاتصالات، حيث أحاطها المشرّع الجزائري بجملة من الاعتبارات والضوابط التي تسمح القيام به والحدود التي يمكن أن نقف عندها حتى لا نصطدم بمسألة حقوق الإنسان وحرّياته.

أولا–حالات اللجوء للمراقبة الإلكترونية

نصّت المادة 04 من القانون رقم 04/09 إلى الحالات التي إذا توّفرت يمكن فيها اللجوء إلى إجراء المراقبة الإلكترونية وهي كالتالي:

أ– الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم م الماسّة بأمن الدّولة، فهنا طبّق المشرع الجزائري مستوى من مستويات السياسة الجنائيّة وهو المستوى الوقائي على غرار المستويين التجريمي والعقابي.[3]

ب– في حالة توفّر معلومات عن احتمال اعتداء على منظومة معلوماتيّة على نحو يهدّد النظام العام أو الدفاع الوطني أو مؤسسات الدّولة أو الاقتصاد الوطني.

ج– لمقتضيات التحرّي والتحقيقات القضائيّة عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

---

[1] زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دون طبعة، دار الهدى، الجزائر، 2011 ص159

[2] ثابت دنيا زاد، مراقبة الاتصالات والحق في حرمة الحياة الخاصّة في القانون الجزائري، العدد السادس، مجلة العلوم الاجتماعية والإنسانية، جامعة تبسة ، 2012ص 207

[3] حاجة عبد العالي، قلات سمية، المكافحة الإجرائية لجرائم الإلكترونية " دراسة حالة الجزائر "، مجلة الفكر، العدد السادس عشر ، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، ديسمبر 2017ص238

د- في إطار تنفيذ طلبات المساعدة القضائيّة الدوليّة المتبادلة.[1]

باستقراء الحالات المذكورة في المادّة رقم 04 من القانون رقم 04/09، يتبيّن لنا أنّ المشرع حصر الحالات التي يمكن اللجوء فيها إلى عمليّة المراقبة الإلكترونية مثل اقتصارها على الجرائم التي تمس بالأمن الوطني وذلك لأنّه عندما يتعلق الأمر بالجرائم الإرهابيّة التي تطال المدنيين لا يمكن الحديث عن حقوق الإنسان وعن حق الشخص في الخصوصية لأنّ المصلحة العامة في خطر بالإضافة كذلك إلى حالات المساعدة القضائيّة، إلاّ أنّ إضافة الحالة الواردة في الفقرة " ج " من المادّة الرابعة سالفة الذكر والمتعلقة بإمكانية اللجوء في كل قضيّة مستعصية إلى المراقبة الإلكترونية صغيرة كانت أو كبيرة يؤدّي إلى تعميم استخدام الآلية دون حد.

ثانيا- ضوابط اللجوء للمراقبة

نظرا لخطورة إجراءات المراقبة الإلكترونية على حقوق وحريّات الأفراد فقد أورد المشرع العديد من الضمانات والإجراءات التي تعتبر بمثابة قيود ترد على السلطة التي تأمر بإجراء المراقبة وتحول دون تعسفها سواء كانت هي أو السلطات التي تتولى تنفيذها، وبقدر ما تكون هذه الأحكام القانونيّة محدّدة وواضحة بقدر ما تكون مباشرة المراقبة مقيّدة وفقاً للهدف منها، وعلى العكس من ذلك فإنّ عدم تحديد هذه الأحكام أو قصورها يفسح المجال لوجود سلطة تقديريّة واسعة في اللجوء إلى المراقبة تختلف ممارستها من سلطة إلى أخرى ممّا يمثّل خطرا كبيرا على حرمة الحياة الخاصّة.[2]

الغاية من تقرير تلك الأحكام القانونيّة هو خلق نوع من التوازن بين حق المجتمع في إقامة العدالة وكشف غموض الجرائم وضبط الجناة وبين حق الأشخاص في حرمة حياتهم الخاصّة فلا تستباح الحرمات ولا تهدر الحريّات.[3]

---

[1] المادة 04من القانون رقم 04/09، سابق الإشارة إليه.

[2] ركاب أمينة، اسالب التحري الخاصة في جرائم الفساد القانون الجزائري، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة ابو بكر بالقايد، تلمسان، 2015/2014ص 12.

[3] ياسر الأمير فاروق، مرجع سابق، ص 449

كما قيّد القانون اللجوء إلى عمليّة المراقبة الإلكترونية بشرط الحصول المسبق على إذن مكتوب ومسبب من الجهات القضائيّة المختصّة المتمثّلة في النائب العام لدى مجلس قضاء الجزائر، حيث يعتبر هو المختص بمنح الإذن لإجراء عملية المراقبة في الجرائم الماسّة بأحكام القانون رقم 09/04،[1] بينما في الأحكام العامّة المنصوص عليها في قانون الإجراءات الجزائية الجزائري فإنّ الإذن الذي يمنح لإجراء المراقبة الإلكترونية يكون من طرف وكيل الجمهوريّة أثناء مرحلة التحقيق الابتدائي أو قاضي التحقيق في مرحلة التحقيق القضائي والاّ كان الإجراء باطلاً وهو ما نصّت عليه المادة65 مكرّر5 من القانون رقم 66-155[2] من قانون الإجراءات الجزائية حتى الفقرة رقم 05 من المادّة رقم 04 الواردة في القانون رقم 04/09 المتضمّن القواعد الخاصّة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما، فقد نصّت على أنه: "**لا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب من السلطة القضائية المختصة**"، وبالتالي فهي تكون قد أحالت بطريقة غير مباشرة إلى القواعد العامّة التي جاء بها قانون الإجراءات الجزائية فيما يتعلق بمنح الإذن لممارسة إجراء الرقابة الإلكترونية على عكس الفقرة رقم 06 و07 من المادّة رقم 04 التي قيّدت الحصول على إذن إجراء المراقبة الإلكترونية فيما يخص الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسّة بأمن الدّولة من طرف النائب العام لدى مجلس قضاء الجزائر كما. هذا وقد حدّد المشرع الجزائري مدّة الإذن الممنوح لضابط الشرطة القضائيّة بستة أشهر قابلة للتجديد.[3] وتركها على مطلقها ولم يقيّدها بوقت محدّد أو بعدد المرات التي يجوز فيها تجديد المراقبة بها.[4] من خلال استقراء أحكام الفقرة السادسة من المادّة رقم 04 من القانون رقم 04/09، يظهر لنا جلياً أنّ مدّة ستة أشهر خاصّة فقط بالفقرة " أ " من المادة رقم04 والمتعلقة بالجرائم الإرهابية أو التخريب أو تلك الماسّة بأمن الدّولة بينما في بقيّة الحالات يتم الرجوع إلى أحكام المادّة65 مكرّر7 من قانون الإجراءات الجزائية

---

[1] الفقرة 6-7من المادّة رقم 04 من القانون رقم 04/09، سابق الإشارة إليه.

[2] الأمر رقم 155/66 المؤرخ في 21يونيو2005، لمتضمن قانون الإجراءات الجزائية المعدل والمتمم، الصادر في الجريدة الرسمية، العدد10 المؤرخ في25يونيو 2005

[3] الفقرة 06 من المادّة رقم 04 من القانون رقم 04/09 سابق الإشارة إليه.

[4] بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة وهرن، 2013/2012 ص124

ومع كل ذلك وجب على المشرع الجزائري أن يضبط بدقّة حجم مدّة الإذن التي تمنح لضباط الشرطة القضائيّة من أجل ممارسة إجراء المراقبة الإلكترونية، فالمشرع الفرنسي مثلاً والذي يُعتبر المشرع الجزائري متأثرا به كثيرا. وقد نصّ في المادّة05 من القانون رقم 646/91 المؤرخ في 10 جويلية1991 المتعلق بسريّة المخابرات الجارية بواسطة وسائل الاتصال الإلكترونية، على أنّ إجراء المراقبة الإلكترونية منحصر في مدّة أربعة أشهر وخوّل فقط لرئيس الوزراء تحديد عدد حالات المراقبة المسموح بها سنوياً وإبلاغها للجنة المكلفة بمراقبة التنصّت الأمني على المحادثات بهذا العدد.

كذلك اشترط المشرع الجزائري في منح الإذن لضباط الشرطة القضائيّة لممارسة إجراء الرقابة الإلكترونية أن يكونوا منتمين لتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها من أجل السماح له القيام بعملية المراقبة الإلكترونية بموجب إذن مكتوب صادر عن النائب العام لدى مجلس قضاء الجزائر.[1]

كما تكون الترتيبات التقنيّة الموضوعة والمنصوص عليها وفقاً لما أوردته بالذكر الفقرة " أ " من المادّة رقم 04 من القانون رقم 09/04 موجّهة حصرياً لتجميع وتسجيل معطيات ذات الصلة بالأفعال الإرهابيّة والتخريبيّة والاعتداءات على أمن الدّولة وبالوقاية منها ومكافحتها فقط دون غيرها من الحالات الأخرى التي أردتها المادّة 04 من نفس القانون المذكور.[2]

المشرع الجزائري من خلال الفقرة 07 من المادّة 04 من القانون رقم 04/09 خصّ المعطيات والمعلومات المتنصّت عليها عن طريق عمليّات مراقبة الاتصالات الإلكترونية المنصوص عليها في الفقرة " أ " لحماية موضوعيّة خاصّة وذلك يجعل عقوبتها نفس عقوبة جنحة المساس بالحياة الخاصّة للأشخاص وهو الفعل المنصوص عليه بموجب المادّة303 من القانون رقم 66-156 المتضمّن قانون العقوبات الجزائري المعدّل والمتمّم[3].

---

[1] الفقرة 6 من المادّة رقم 04 القانون رقم 04/09 سابق الإشارة إليه.

[2] بوخبزة عائشة، مرجع سابق، ص 141

[3] الأمر رقم 156/66 المؤرخ في 8 يونيو 1966المتضمن قانون العقوبات المعدل والمتمم، الصادر في الجريدة الرسمية للجمهورية الجزائرية، العدد48، المؤرخ في 10 يونيو1966.

المبحث الثاني: الإجراءات المستحدثة

لجأ المشرع الجزائري إلى استحداث وسائل جديدة لمكافحة انتهاكات التي تقع على الخصوصية الرقمية وكانت اهم هاته الوسائل هي التسرب ولكن ذلك لا يخلو ان إجراءات التحقيق سواء الابتدائي أو التمهيدي قد تكون باطلة فينتقل التحقيق هنا لدى غرفة الاتهام لتفصل في هذا البطلان وهو ما سنتعرف عليه من خلال دراستنا في هذا المبحث وتقسيمه إلى مطلبين الأول يضم التسرب والثاني التحقيق لدى غرفة الاتهام تتم الدراسة كما يلي

المطلب الأول: التسرب

يعتبر التسرب من اهم الإجراءات التي يعتمدها القاضي أثناء التحقيق الابتدائي لحماية الخصوصية الرقمية وتحكم هذا الإجراء مجموعة من الضوابط والإجراءات التي سندرسها من خلال هذا المطلب بتقسيمه إلى فرعين وستتم الدراسة كما يلي

الفرع الأول: تعريفه

التسرب لغة مشتق من الفعل تسرب تسربا أي دخل وانتقل خفية وهي الولوج والدخول بطريقة أو بأخرى إلى مكان أو جماعة .[1]

يعد التسرب أو الاختراق تقنية جديدة أدرجها المشرع في تعديل قانون الإجراءات الجزائية سنة 2006، عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 05، كما يجوز لوكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب من شروط محددة [2]

ويعتبر أسلوب التسرب أو الاختراق تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط الشرطة القضائية آخر مكلف بتنسيق عملية التسرب، بهدف مراقبة أشخاص مشتبه فيهم،

---

[1] سهيل حسيب سماحة، معجم اللغة العربية، الطبعة الأولى، مكتبة سمير، 1984، ص130.

[2] نجيمي جمال، إثبات الجريمة على ضوء الاجتهاد القضائي، دراسة مقارنة، دون طبعة، دار هومة للنشر والتوزيع والطباعة، 2011، ص451.

وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقة، ويقدم المتسرب نفسه على أنه فاعل أو شريك.[1]

أما فيما يخص التعريف القانوني للتسرب فقد تناوله المشرع الجزائري في المادة 65 مكرر 12 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 بقوله: "يقصد بالتسرب قيام ضباط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف." هذا ويلاحظ أن المشرع سمى هذه العملية بالتسرب في قانون الإجراءات الجزائية في حين استخدم مصطلح الاختراق في المادة 56 من القانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته ، وهما مسميان لمسمى واحد ولهما نفس المدلول.

من خلال التعريف السابق يتضح أن التسرب هو عبارة عن عملية ميدانية تستخدم أسلوب التحري لجمع الوقائع المادية والأدلة من داخل العملية الإجرامية وكذا الاحتكاك شخصيا بالمشتبه بهم والمتهمين وهذا ينطوي على خطورة بالغة تحتاج إلى دقة وتركيز وتخطيط سليم.

من ثم يمكن القول أن التسرب هو أكثر الوسائل تعقيدا وخطورة، لأنه يتطلب من ضابط الشرطة القضائية وأعوانه القيام بمناورات وتصرفات توحي بأن القائم بها مساهم في ارتكاب الجريمة مع بقية أفراد العصابة، لكنه في حقيقة الأمر يخدعهم ويتحايل عليهم فقط، حتى يطلع على أسرارهم من الداخل ويجمع ما يستطيع من أدلة إثبات، ويبلغ السلطات بذلك فتتمكن من ضبط المجرمين ووضع حد للجريمة.

إذن ترتكز عملية التسرب على ضرورة الحصول على صورة حقيقية على الوسط المراد استكشافه لمعرفة طبيعة سيره وأهدافه وكذا معرفة تاريخ هذه الجماعة وكيفية نشأتها واختصاصات كل فرد من عناصرها ،وأيضا الوسائل التي تعمل بها كوسائل النقل والاتصال وتحديد نقاط قوة وضعف هذه الجماعة، وبعد دراسة الوسط المستهدف يتم اختيار الأشخاص المناسبين لتولي مهمة التسرب.[2]

---

[1] حريزي ربيحة، إجراء جمع الأدلة ودورها في الكشف عن الجريمة، رسالة ماجستير، جامعة الجزائر، 2001ص59

[2] زوزو زوليخة، جرائم الصفقات العمومية، رسالة ماجستير، جامعة محمد خيضر، بسكرة، 2011ص72

الفرع الثاني: شروطه وإجراءاته

أولا-شروطه

اشترط المشرع في المادة 65 مكرر 11 من قانون الإجراءات الجزائية وجوب أن تقتضي ضرورات التحري أو التحقيق إجراء عملية التسرب، وبمفهوم المخالفة فإن وجود أدلة كافية تعزز الاشتباه أو تدعم الاتهام فإنه لا داعي للمخاطرة بإجراء عمليات تسرب وعليه فإن هذه الأخيرة تجرى عند الضرورة فقط المتمثلة في قلة أو صعوبة الحصول على أدلة وبراهين كافية لتحريك دعاوى عمومية.

كما اشترط المشرع في اللجوء إلى هذا الأسلوب ضرورة ارتكاب أنواع محددة من الجرائم التي تتسم بالخطورة والتعقيد، من ثم فإن الأمر بإجراء عمليات التسرب ليس مفتوحا لكل الجرائم بل هو خاص بمجموعة محددة من الجرائم المذكورة في المادة 65 مكرر 5 من قانون الإجراءات الجزائية، هذه الجرائم هي: جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، إذن فيما عدا هذه الأنواع المذكورة على سبيل الحصر لا يجوز استخدام هذا الأسلوب.

فما يلاحظ هنا أن المشرع الجزائري عدد هذه الجرائم على سبيل الحصر، وقد يرج ع هذا للخطورة الإجرامية لهذه الأفعال واثرها على السياسة العامة في الدولة واقتصادها، اما إذا كانت هذه الأعمال في غير هذه الجرائم فإجراؤها باطل.[1]

ثانيا-إجراءاته

هناك عدة إجراءات تطلبها المشرع لصحة عمليات التسرب، وهذا لإضفاء طابع الشرعية في الحصول على الدليل تطبيقا لمبدأ المشروعية الذي يمثل أساسا لكل إجراء صحيح، سواء من حيث الجهات صاحبة السلطة في الإذن بإجراء عمليات تسرب أو من حيث الجهات المختصة بمباشرة هذا الإجراء.

[1] محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة الرابعة، دار هومة للنشر والتوزيع والطباعة، الجزائر، 2009، ص134.

ضمانا لمشروعية الدليل المستمد من إجراء عملية التسرب اشترط المشرع ضرورة حصول المتسرب على إذن من وكيل الجمهورية المختص وأن تتم عملية التسرب تحت إشرافه ومراقبته فإن قرر قاضي التحقيق مباشرة هذا الإجراء وجب عليه أولا إخطار وكيل الجمهورية بذلك، ثم يقوم بمنح إذن مكتوب لضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، عل أن يتم ذكر هويته فيه.[1] كما يجب أن يكون الإذن مكتوبا ومسببا، حيث يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، ولا بد أن يحدد الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (04 أشهر.[2]

ويمكن أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية، غير أنه يجوز للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة، وتودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب.[3]

يجوز لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد وهذا ما تناولته المادة 65 مكرر 11 ، التي اشترطت ضرورة أن تتم العملية تحت رقابة قاضي يقدر هذه العملية ويراقبها خطوة بخطوة لتلافي حدوث تجاوزات للقانون، ويكون هذا الإذن القضائي مكتوبا ومسببا تحت طائلة البطلان طبقا لأحكام المادة 65 مكرر 15 ، وكما هو معلوم فإن بطلان الإذن يرتب بطلان كافة الإجراءات المتخذة بناء عليه، إذ يشترط أن يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية التي تـ تم العملية تحت مسؤوليته ويحرر بهذا الإذن مدة عملية التسرب والتي لا يمكن أن تتجاوز أربعة (04

---

[1] محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، الطبعة الثانية، دار هومة، الجزائر، 2009، ص155.

[2] المادة، 02، 03، 65 مكرر15 من الامر155/66قانون الإجراءات الجزائية، السابق ذكره.

[3] المادة04/65مكرر15القانون نفسه.

أشهر ويمكن تجديدها حسب مقتضيات التحري والتحقيق كما يجوز للقاضي الذي رخص بها ان يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة وتودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب .

يسمح القانون طبقا لأحكام المادة 65 مكرر 14 لضابط أو لعون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وان يرتكب عند الضرورة الأعمال التالية: اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو المستعملة في ارتكابها، واستعمال أو وضع تحت تصرف مرتكبي الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل والتخزين أو الإيداع أو الحفظ أو الاتصال.

هناك من الفقهاء من يرى في هذه الأعمال خروجا عن مبدأ نزاهة ومشروعية الدليل الجنائي للوصول لغاية أسمى هي ضرورة حماية المجتمع عندما تعجز الأساليب التقليدية للتحري والتحقيق عن مواجهة بعض الجرائم.[1]

يحرر ضابط الشرطة القضائية المكلف بالتنسيق تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي قد تعرض للخطر أمن الضابط العون المتسرب، وكذا الأشخاص المسخرين لهذا الغرض وهذا ما تناولته المادة 65 مكرر 13.

إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في رخصة التسرب وفي حالة عدم تمديديها يمكن للعون المتسرب مواصلة المهمة للوقت الضروري الباقي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا على أن يتجاوز ذلك مدة أربعة 04 أشهر وإذا انقضت مدة أربعة أشهر دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه يجب إخبار القاضي المرخص الذي يستطيع ان يرخص بتمديدها لمدة أربعة أشهر أخرى على الأكثر، للإشارة فإنه يجوز سماع ضابط الشرطة القضائية الذي تجري العملية تحت مسؤوليته دون سواه لوضعه شاهد عن العملية ، كما يرتب القانون عقوبات جزائية على كل من يكشف هوية ضابط أو أعوان الشرطة القضائية الذين باشروا

[1] المادة65مكرر 11من الامر 155/66 قانون الإجراءات الجزائية. سابق ذكره.

عملية التسرب تحت هوية مستعارة في أي مرحلة من مراح ل الإجراءات (المادة 65 مكرر16[1].

أما عن الجهات المخولة بإجراء عمليات تسرب فهم ضباط الشرطة القضائية المذكورون في المادة 15 من قانون الإجراءات الجزائية،[2] ويستثنى من هؤلاء لاعتبارات ميدانية الولاة ورؤساء المجالس الشعبية البلدية بالإضافة إلى مساعدي ضباط الشرطة القضائية وهم الأعوان الذين جاء ذكرهم في المادة 19 من نفس القانون، فالأعوان يمارسون مهامهم تحت مسؤولية ضباط الشرطة القضائية المكلفين بتنسيق العملية وتصدر باسمهم.

كما أضافت المادة 65 مكرر 13 مصطلح المسخرين ويقصد بهم كل الأشخاص من الجنسين يراه ضابط الشرطة القضائية القائم بتنسيق عملية التسرب مفيدا لإنجاز مهمته، وهذا دائما تحت رقابة القضاء.

المطلب الثاني: اعتراض المراسلات

سنتعرف في هذا المطلب عن عملية اعتراض المراسلات اضافة الى القيود الواردة على هاته العملية او الاجراء.

الفرع الأول: تعريفها

عرفها المشرع الجزائري في المادة 65[3] مكرر 5 من قانون الاجراءات الجزائية بأنها «اعتراض او تسجيل او نسخ المراسلات التي تتم عن طريق قنوات او وسائل الاتصال السلكية واللاسلكية، وهذه المراسلات عبارة عن بيانات قابلة للانتهاج والتوزيع، التخزين، الاستقبال والعرض، مع العلم ان هذا النص هو اعادة صياغة المادة100 من قانون الاجراءات الجزائية الفرنسي.

---

[1] انظر: المادة 16 من قانون العقوبات الجزائري المعدل بالقانون رقم 23/06 المؤرخ في 20 ديسمبر 2006.

[2] انظر: المادة 15 والمادة 19 من قانون الإجراءات الجزائية المعدل بالقانون رقم 22/06 المؤرخ في 22 ديسمبر 2006

[3] المادة 65 مكرر 5من قانون الاجراءات الجزائية السابق ذكره.

وبالرجوع الى نص هذه المادة نلاحظ ان المشرع الجزائري حدد المراسلات التي تصلح ان تكون محلا للاعتراض بتلك المراسلات التي تتم بواسطة وسائل اتصال سلكية ولاسلكية، دون ان يشير الى طبيعة هذه المراسلات، مما يفتح المجال لمختلف الرسائل المكتوبة، بغض النظر عن شكلها (كتابة، رموز، اشكال، صور) او الدعامة التي تنصب عليها(ورقية او رقمية)، او الوسيلة المستعملة في ارسالها سلكية كانت (كالفاكس، تلغرام) ، او لاسلكية(البريد الالكتروني، الهاتف النقال)، باستثناء الكتب والمجلات والرسائل والحوليات التب تعد مراسلات خاصة.

وبغض النظر عن طبيعة المراسلات السلكية واللاسلكية فعملية الاعتراض تتم بواسطة ترتيبات تقنية سرية يتم وضعها دون علم او موافقة المعنيين، وذلك لغرض التصنت وتثبيت وبث وتسجيل البيانات المرسلة او المحادثات التي اجراها المشتبه فيه بصفة خاصة او سرية في اماكن خاصة او عمومية، ومن ثما استعمالها كدليل لمواجهة المتهم. [1]

الفرع الثاني: القيود الواردة على عملية اعتراض المراسلات

اذا كان اسلوب اعتراض المراسلات السلكية واللاسلكية دون علم اصحابها قد اثبت جدارته في كشف واثبات الكثير من الجرائم الغامضة كتللك المتعلقة بالجرائم الإلكترونية، فهو في الوقت نفسه يمثل انتهاكا خطيرا لحرمة الحياة الخاصة للأفراد، واعتداء صارخا عل سرية مرسلاتهم واتصالاتهم التي كفلتها معظم الدساتير والتشريعات العقابية بالحماية. [2]

لذلك وجب احاطة هذا الاجراء بمجموعة من القيود حتى لا يعتبر انتهاكا للحياة الخاصة وتتمثل هاته القيود في

[1] ربيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دون طبعة، دار الهدى، الجزائر، 2011،ص157

[2] ربيحة زيدان، مرجع نفسه، ص159

1-الحصول على إذن السلطة القضائية المختصة: قيد القانون اللجوء الى عملية اعتراض المراسلات بشرط الحصول المسبق على اذن مكتوب ومسبب من الجهة القضائية المختصة المتمثلة عادة في وكيل الجمهورية اثناء مرحلة التحقيق الابتدائي،[1] او قاضي التحقيق في مرحلة التحقيق القضائي.

وحتى يكون الاذن صحيحا ومنتجا لأثره يجب ان يتضمن جملة من العناصر:

أ-طبيعة الجريمة التي تبرر الاجراء: وهي الجرائم المحددة على سبيل الحصر في المادة 65 مكرر 5 من قانون الاجراءات الجزائية والمادة 04 من القانون 09-04[2]

ب-التعريف بالعملية: يعني تحديد المراسلات والاتصالات المطلوب اعتراضها وتسجيلها، وتحديد الاماكن المقصودة، الى جانب تحديد المدة التي لا تتجاوز 4 اشهر قابلة للتجديد ضمن الشروط نفسها.

ولا يكفي الحصول على اذن مشمول بالعناصر المذكورة لإتمام عملية اعتراض المراسلات، انما لا بد ان تنفذ العملية تحت الرقابة المباشرة للسلطات التي اذنت بها.

2-تسبيب اللجوء الى اعتراض المراسلات: يقصد به المبرر الشرعي والضرورة الملحة التي تستدعي القيام بعملية اعتراض المراسلات، وتتحقق هذه الضرورة عندما يكون من الصعب الوصول الى نتيجة تهم مجريات التحقيق دون اللجوء الى هذه العملية. وقد اجاز المشرع ايضا كذلك تطويع هذه التقنية لغرض الوقاية من احتمال وقوع جرائم خطيرة تهدد كيان الدولة كما قررته المادة 04 من القانون 09-04

3-تحديد الجرائم محل الاعتراض: ان الاستعانة بعملية الاعتراض لغرض التحقيق لا يكون مسموح به في كافة الجرائم، انما مجال تطبيقها يتوقف عند نوع محدد فقط وهي:

[1] براهيمي جمال، مرجع سابق، ص94

[2] انظر المادتين 65 مكرر 5 من ق. إ. ج والمادة 04 من القانون 09-04

-جرائم المخدرات، الجريمة المنظمة العابرة للحدود، جرائم تبييض الاموال، الارهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد، والجرائم الماسة بالمعالجة الالية للمعطيات، جرائم الاعتداء على المنظومة المعلوماتية. [1]

4-سرية الاجراءات وكتمان السر المهني: ينبغي ان تنفذ عملية الاعتراض في سرية تامة ودون علم او رضا المشتبه فيه او صاخب الاماكن، مع مراعاة عدم المساس بالسر المهني المقرر بنص المادة 45 الفقرة 4 من ق. ا. ج. [2]

كما ينبغي التنبيه ان المشرع الجزائري لم يشر صراحة الى كيفية وضع الادلة المتحصل عليها من عملية اعتراض المراسلات في احراز مختومة.

المطلب الثالث: التحقيق لدى غرفة الاتهام

أثناء بطلان التحقيق سواء التمهيدي أو الابتدائي فأن غرفة الاتهام تتدخل وتباشر التحقيق وذلك بعد إخطارها ببطلان التحقيق فهي التي تفصل في هذا البطلان وللتعرف اكثر على هذا لابد من تقسيم المطلب الاتي إلى فرعين الأول إخطار غرفة الاتهام بالبطلان والثاني فصلها فيه

الفرع الأول: إخطار غرفة الاتهام بالبطلان

يتم اتصال غرفة الاتهام بملف الدعوى بعدة طرق نوضحها على النحو التالي:

أولا-عن طريق إرسال المستندات إلى النائب العام من قاضي التحقيق.

إذا تعلق التحقيق بجناية فإن التحقيق فبها وجوبي على درجتن وفقا لنص المادة 66 من ق. إ،ج، وهي الطريقة العادية لتوصل غرفة الاتهام بالدعوى، فعند انتهاء قاضي التحقيق من تحقيقه يصدر أمر إرسال مستندات القضية إلى نائب العام وذلك بقصد جدولتها

[1] انظر المادتين 65 مكرر5 و04 من القانون 09-04

[2] انظر المادة 45 الفقرة 4 من ق. ا. ج

بغرفة الاتهام، وهو ما نصت عليه المادة 166 من ق إ ج، ذلك لأن غرفة الاتهام جهة إحالة إلى محكمة الجنايات وهو الأمر الذي لا بملكه قاضي التحقيق مباشرة[1]

ثانيا-عن طريق الاستئناف.

الطريقة الثاني لتوصل غرفة الاتهام بالملفات، فهو بمناسبة استئناف أحد أطراف الخصومة الجزائية أي المتهم أو محاميه والطرف المدني أو محاميه، ووكيل الجمهورية أو النائب العام لأحد أوامر قاضي التحقيق التي يجوز لهم استئنافها طبقا لما هو منصوص عليه في المواد من 170 إلى 174 من ق.إ.ج.ج ، فترفع الدعوى أو ملف الاستئناف إلى غرفة الاتهام من قبل النائب العام الذي يتلقى الملف من وكيل الجمهورية لتفصل فيه حسب ما هو مخول لها قانونا بتأييد أمر قاضي التحقيق محل الاستئناف أو بإلغائه [2]

ثالثا- عن طريق النائب العام.

هناك حالة نادرة التطبيق تنص عليها المادة 180 من ق.إ.ج.ج ، إذا تبيّن للنائب العام أن القضية المطروحة أمام محكمة غير محكمة الجنايات لها وصف جنابية جازلة أن يأمر بإحالتها على غرفة الاتهام لتفصل في مسألة تكييفها شرط أن يكون ذلك قبل بداية المناقشة أمام المحكمة التي كانت مطروحة عليها القضية[3].

وهناك حالة ثانية إذا تبيّن للنائب العام من الأوراق التي يتلقاها بعد صدور قرار بألا وجه للمتابعة أن ثمة سبب لإعادة التحقيق لظهور أدلة جديدة، وقد نصت على ذلك المادة 181 من ق.إ.ج.ج .[4]

---

[1] عبد الرحمان خلفي ، الإجراءات الجزائية في التشريع الجزائري والمقارن، دون طبعة، دار بلقيس للنشر، الجزائر ، 2015، ص302.

[2] محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، مرجع سابق، ص257.

[3] مختار سيدهم ، (موجز اختصاص غرفة الاتهام)، مجلة المحكمة العليا، الغرفة الجنائية، العدد الثاني، الجزائر ، 2005، ص 60.

[4] محمد حزيط، مذكرات في قانون الإجراءات الجزائية، مرجع سابق، ص266.

رابعا- الأخطار مباشرة.

1- من المتهم:

إذا تعلق بتقديم طلب إفراج إلى قاضي التحقيق ولم يبت هذا الأخير في الطلب خلال 08 أيام من تاريخ إرسال الملف إلى وكيل الجمهورية وهو ما تنص عليه المادة 127 من ق إ ج ج ففي هذه الحالة يرفع الأمر مباشرة إلى غرفة الاتهام التي تفصل في الطلب خلال 30 يوم من تاريخ الطلب، كذلك يجوز للمتهم رفع الطلب مباشرة إلى غرفة الاتهام إذا تعلق الأمر بتقديم طلب رفع الرقابة القضائية إلى قاضي التحقيق وهذا الأخير لم يبت فيه خلال 15 يوم من تاريخ تقديم الطلب فيرفع الأمر مباشرة إلى غرفة الاتهام.

2- من وكيل الجمهورية وقاضي التحقيق:

في حالة قدم طلب إفراج للمتهم (مادة 2/127 ق.إ.ج.ج أو إذا طلب رفع الرقابة القضائية (المادة 125 مكرر2 وفي حالة ما إذا تبيّن أن أي إجراء من إجراءات التحقيق قد شابها عيب نتيجة البطلان (المادة 158.

ونفس الشيء ينطبق على قاضي التحقيق الذي يملك كذلك أن يطعن في أي أمر قام به هو شخصيا أمام غرفة الاتهام ويطالب إبطاله وهو ما تنص عليه المادة 1/158.[1]

الفرع الثاني: فصل غرفة الاتهام في التحقيق

أولا- الفصل في شكل الاستئناف.

إن الفصل في موضوع الاستئناف يتطلب التأكد من توافر الشروط المقررة قانونا، وهي الشروط الشكلية التي تتعلق بثبوت حق الطعن، فإذا توافرت هذه الشروط كان الاستئناف مقبولا، أما إذا كان الأمر المستأنف غير قابل للطعن أو كان ارفع الاستئناف غير ذي صفة أو كان طعنه قد وقع خارج الميعاد القانوني أو بشكل غير صحيح كان الاستئناف غير مقبول من الناحية الشكلية لعدم توافر أحد الشروط المتعلقة بآجال الاستئناف وبكيفية التقرير

[1] عبد الرحمان خلفي، مرجع سابق، ص303/302.

به وهذا ما أكده القرار الصادر من المحكمة العليا بتاريخ 27 نوفمبر 1984 تحت رقم 64/82.[1]

ثانيا: الفصل في موضوع الاستئناف.

بعد تصريح غرفة الاتهام بقبول الاستئناف شكلا تتطرق للموضوع فتصدر قرار إما بتأييد الأمر المستأنف وإما إلغائه.

1-تأييد الأمر المستأنف.

تصدر غرفة الاتهام قرارها بتأييد الأمر المستأنف إذا تبيّن لها أن قاضي التحقيق قد طبق القانون سليما فيما انتهى إليه وقد سبب أمره المستأنف تسبيبا كافيا، كالقرار الصادر عن غرفة الاتهام بتأييد أمر قاضي التحقيق بانتفاء وجه الدعوى. [2]

2- إلغاء الأمر المستأنف.

طبقا للمادة 2/192 من ق.إ.ج.ج فإنه إذا كان الاستئناف ضد أمر قضى في مسألة الحبس المؤقت، تنحصر صلاحية غرفة الاتهام في نظر هذه المسألة فقط دون التصدي لموضوع الدعوى، كأن تقضي بإلغاء أمر قاضي التحقيق الذي كان أمر برفض الإفراج عنه وتقضي من جديد بالإفراج عنه، أو تقضي بإلغاء أمر قاضي التحقيق الذي كان قد قضى برفض الإفراج عن المتهم وتقضي من جديدة باستمرار حبسه مؤقتا أما دون ذلك فيجوز لغرفة الاتهام أن تتصدى لموضوع الدعوى أو تُحال القضية إلى نفس القاضي المحقق أو إلى قاضي تحقيق آخر لمواصلة التحقيق ما لم يكن قرار الإلغاء قد أنهى التحقيق.[3]

الفرع الثالث: إجراءات التحقيق لقاضي الحكم

---

[1] سماتي الطيب، حماية حقوق ضحية الجريمة خلال الدعوى الجزائية، دون طبعة، مؤسسة البديع للنشر والخدمات الإعلامية، الجزائر، 2008ص207.

[2] محمد حزيط، مذكرات في قانون الإجراءات الجزائية، مرجع سابق، ص269.

[3] محمد حزيط، مرجع نفسه، ص270.

يسود المحاكمة الجنائية بوجه عام مبادئ الحضورية والشفوية والعلنية في المرافعات ، فيأمر الرئيس بتلاوة قرار الإحالة ،[1] ويستجوب المتهم ويتلقى تصريحاته ، ويجوز لاطراف الدعوى المتهم ومحاميه والمدعي المدني والمسؤول عن الحقوق المدنية ومحاميهما طرح الاسئلة على اطراف الدعوى وعلى الشهود والخبراء بواسطة الرئيس او بإذن منه ، في ما عدا النيابة العامة التي يجوز لها طرح الاسئلة مباشرة .

وتتميز الاجراءات في مرحلة المحاكمة بانها مرحلة تعرض فيها الادلة بنوعيها من ادلة الاثبات وادلة النفي ، فيقوم الرئيس بسؤال المتهم عن هويته ويستجوبه عن التهم المنسوبة اليه ويستمع للشهود بصفة انفرادية بعد ادائهم لليمين القانوني ويستمع لشهود الاثبات قبل شهود النفي ثم يستمع لتقارير الخبراء ان كان ثمة حاجة لذلك[2] .

وبعد عرض الادلة ومناقشتها في الجلسة العلنية يقوم المدعي المدني او محاميه بتقديم مرافعته و طلباته ثم تبدي النيابة العامة طلباتها ، ويقدم بعد ذلك المتهم ومحاميه اوجه دفاعهما مع تمكين كل من النيابة العامة والمدعي المدني من الرد على طلبات المتهم ، مع وجوب ان تكون الكلمة الاخيرة في جميع الاحوال للمتهم ومحاميه ثم يعلن الرئيس عن اختتام المرافعات فتنتهي مناقشة الادلة ، فلا تقبل بعد ذلك ادلة جديدة الا اذا اعلن الرئيس عن فتح المرافعات من جديد ، كما يمتنع عن تقديم مذكرات اثناء المداولات[3].

وبعد اعلان الرئيس عن اختتام المرافعات يتلو في قاعة الجلسات الاسئلة الموضوعية والتي ستطرح على هيئة المحكمة للاجابة عنها اثناء عملية المداولة ويشترط القانون وضع سؤال عن كل واقعة ينسب ارتكابها للمتهم بالصغة التالية :

هل المتهم مذنب بارتكاب هذه الواقعة ؟

ويعتبر الاخلال بالشروط الشكلية لورقة الاسئلة مبطلا للحكم الذي بني عليه ويجب ان تشمل على البيانات الجوهرية المقررة قانونا لصحتها وهي:

---

[1]) عبد الرحمان خلفي، الاجراءات الجزائية في التشريع الجزائري والمقارن ،ط3 ، دار بلقيس للنشر ، الجزائر ،2017، ص207.

[2]) عبد الرحمان خلفي، المرجع نفسه ، ص208.

[3]) عبد الرحمان خلفي ، المرجع نفسه ، ص208.

- الاسئلة والاجوبة عنها وفقا لاحكام المادتين 305 و309 الفقرة 2 أ ج .
- العقوبة المتداول بشأنها والمحكوم بها على المتهم .
- النصوص القانونية المطبقة عليها طبقا لاحكام المادة 314 الفقرة 9 أ ج [1].
- التوقيع عليها من الرئيس والمحلف الأول ، فان خلت بواحدة منها تعد لاغية ويكون الحكم الذي بني عليها باطلا .

[1]) عبد الرحمان خلفي ، المرجع السابق، ص 208.

خلاصة الفصل

في الأخير نستنتج أنه أثناء التحقيق الابتدائي قام المشرع بوضع مجموعة من الإجراءات منها ما هو تقليدي كان أهمه التفتيش والمراقبة ومع تطور التقنيات لجأ بدوره إلى تطوير الإجراءات واستحداثها فكان أهمها التسرب و اعتراض المراسلات وفي صورة ما إذا شاب هذا التحقيق عيب يصبح باطلا ويتم استئنافه.

أمام غرفة الاتهام عن طريق إخطاره بطرق متعددة وذلك للفصل في صحة أو غلط هذا الاستئناف فتقرر تأييد التحقيق أو إلغائه اما امام قاضي الحكم فيتبع كذالك اجرائات للتحقيق وبهذا يصبح المشرع سلط الضوء واستوفى كل الإجراءات لحماية الخصوصية الرقمية من أي انتهاكات.

خاتمة

خلاصة

كلما تطورت التكنولوجيا تطورت معها الجرائم لذلك وجد المشرع الجزائري نفسه مطالب بوضع إجراءات خاصة لحماية الحقوق من الانتهاكات ومن بين هاته الحقوق الحق في الخصوصية الرقمية فالمشرع الجزائري افردها بإجراءات لحمايتها تختلف من التحقيق التمهيدي إلى التحقيق الابتدائي فسلط الضوء على الإجراءات التي تجعل الحق في الخصوصية الرقمية في مواجهة مقتضيات التحقيق الابتدائي فمنها ما هو تقليدي أي إجراءات تقليدية كالتفتيش والاعتراض والمراقبة ولجأ المشرع الجزائري إلى استحداث وسائل جديدة لمكافحة انتهاكات التي تقع على الخصوصية الرقمية وكانت اهم هاته الوسائل هي التسرب ولكن ذلك لا يخلو من إجراءات التحقيق سواء الابتدائي أو التمهيدي قد تكون باطلة فينتقل التحقيق هنا لدى غرفة الاتهام لتفصل في هذا البطلان وهو ما تطرقنا إليه.

ويمكن القول أن الحق في الخصوصية الرقمية يتعرض إلى العديد. من الانتهاكات تنصب على البيانات الشخصية كإفشائها ومعالجتها دون ترخيص كما تنصب أيضا على الحاسبات الآلية والبريد الإلكتروني ومهما كانت هاته الانتهاكات ومهما تميزت بالخطورة فأن المشرع الجزائري قام بوضع مجموعة من الإجراءات يكفلها قانون الإجراءات الجزائية الجزائري لردعها واختلفت هاته الإجراءات فكانت في بدايتها تقليدية منها المعاينة وضبط الأدلة والاستجواب لتتطور بعدها الجرائم وذلك يؤدي تلقائيا إلى تطور إجراءات الحماية لتواكب هاته الجرائم فتؤدي بدورها إلى ظهور سبل وإجراءات حديثة أو خاصة متمثلة في الخبرة والشهادة وبذلك أصبحت هاته الانتهاكات.

النتائج:

وبناء على ما سبق تم التوصل إلى عدة نتائج أهمها:

حرص المشرع الجزائري على فرض الحماية المستحقة للحق في الخصوصية، من خلال دسترته ودسترة واجب الدولة في التكفل بحمايته، مع تسخير جميع تشريعاته المتعلقة بهذا الحق لتجسيد عدم جواز المساس بحرمته.

لم يعمل المشرع الجزائري بعدم جواز التدخل المطلق في خصوصيات الأفراد، لما يترتب عن ذلك من إمكانية التعارض بين المصلحة الشخصية والمصلحة العامة التي تقتضي حمايتها السماح للجهات المختصة بانتهاك حق الأفراد في الخصوصية في حالات محددة.

أثناء التحقيق الابتدائي قام المشرع بوضع مجموعة من الإجراءات منها ما هو تقليدي كان أهمها التفتيش والمراقبة، ومع تطور التقنيات لجأ بدوره إلى تطوير الإجراءات واستحداثها فكان أهمها؛ التسرب وفي صورة ما اذا شاب هذا التحقيق عيب يصبح باطلا ويتم استئنافه أمام غرفة الاتهام عن طريق إخطاره بطرق متعددة وذلك للفصل في صحة أو غلط هذا الاستئناف فتقرر تأييد التحقيق أو إلغائه وبهذا يصبح المشرع سلط الضوء واستوفى كل الإجراءات لحماية الخصوصية الرقمية من أي انتهاكات.

التوصيات:

على المشرع الجزائري وضع ضوابط اجرائية وعقابية صارمة تطبق في حالة اساءة استعمال الاجراءات من قبل السلطات المختصة وضرورة النص الصريح على بطلان هذه الاجراءات متى جاءت مخالفة للضوابط وذلك لحماية الحياة الخاصة.

ضرورة الدعوة الى اعتماد حلول تنظيمية مشتركة اقليميا وعربيا للمسائل المطروحة على جرائم الاعتداء على الخصوصية الرقمية وبذل جهد وتبادل الخبرات للإستفادة من التجارب الواقعية في هذا المجال.

جمع القوانين التي تعاقب على التعدي على الخصوصية الرقمية اثناء التحقيق الجنائي في قانون واحد يتم تقنينه عوض ع قوانين متفرقة.

قائمة المصادر والمراجع

القرآن الكريم

أولا: المصادر:

1. القوانين:

- قانون 23/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات. الجريدة الرسمية، الجمهورية الجزائرية. العدد84.
- القانون 40/90 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.
- القانون رقم 04/09 المؤرخ في 10، اوت 2009 يتضمن القواعد الخاصّة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الصادر في الجريدة الرسمية للجمهورية الجزائرية، العدد 47، المؤرخ في 16اوت 2009.
- القانون رقم 20/51 المؤرخ في 230 يوليو 2015 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، الجريدة الرسمية العدد04.
- القانون رقم 18-10 المؤرخ في 09 شعبان عام 2021 الموافق ل 5 أوت3118 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية للجمهورية الجزائرية/ العدد 02.

2. الأوامر:

- الأمر رقم 156/66 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات المعدل والمتمم، الصادر في الجريدة الرسمية للجمهورية الجزائرية، العدد48، المؤرخ في 10 يونيو1966.
- الأمر رقم 155/66 المؤرخ في 21يونيو2005، لمتضمن قانون الإجراءات الجزائية المعدل والمتمم، الصادر في الجريدة الرسمية، العدد10 المؤرخ في25يونيو 2005.

ثانيا: المراجع:

1. الكتب:

- أحسن بوسقيعة. التحقيق القضائي. ط7، دار هومة للنشر والتوزيع. الجزائر، 2009.
- أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي دون طبعة، دار النهضة العربية، مصر، سنة 2000.
- أحمد شوقي الشلقاني. مبادئ الإجراءات الجزائية في التشريع الجزائري. الجزء الثاني، الطبعة الخامسة، ديوان المطبوعات الجامعية الجزائر، دون سنة نشر.
- احمد عوض بلال، قاعدة استبعاد الأدلة المتحصل عليها بطرق غير مشروعة، ط1، دار النهضة العربية، 2010.
- أمال قارة، الحماية الجزائية للمعلومات في التشريع الجزائري الطبعة الأولى، دار هومة للنشر والطباعة، الجزائر، 2006.
- بوكر رشيدة، جرائم لاعتداء على نظم المعالجة الآلية للمعطيات في التشريع الجزائري والمقارن، الطبعة الأولى، منشوارت الحلبي الحقوقية، لبنان ، 2012.
- بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دون طبعة، منشوارت الحلبي الحقوقية، بيروت، 2009.
- جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي دون طبعة، دار النهضة العربية، مصر، سنة 2000.
- حسام الدين الأهوائي، الحق في احترام الحياة الخاصة، الحق في الخصوصية، دراسة مقارنة، طبعة ثانية، دار النهضة العربية، 2002.
- خالد عياد الحلبي، إجراءات البحث والتحقيق في جرائم الكومبيوتر والإنترانت، دون طبعة، دار الثقافة للنشر والتوزيع، الردن، 2011.
- خالد محمد عجاج، القاضي علي دايح جريان، "أصول التحقيق الجنائي"، دون طبعة، دار التعليم الجامعي، الإسكندرية، 2018.
- خالد ممدوح إبراهيم. فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2008.

- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دون طبعة، دار الفكر الجامعي، مصر، سنة 2004.
- زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دون طبعة، دار الهدى، الجزائر، 2011.
- سماتي الطيب، حماية حقوق ضحية الجريمة خلال الدعوى الجزائية، دون طبعة، مؤسسة البديع للنشر والخدمات الإعلامية، الجزائر، 2008.
- سهيل حسيب سماحة، معجم اللغة العربية، الطبعة الأولى، مكتبة سمير، 1984.
- السيد عتيق، جرائم الانترنت، دون طبعة، دار النهضة العربية، مصر، 2002.
- عبد الرحمان خلفي ، الإجراءات الجزائية في التشريع الجزائري والمقارن، دون طبعة، دار بلقيس للنشر، الجزائر ، 2015.
- عبد العال الديري ومحمد صادق إسماعيل .الجرائم الإلكترونية، ط10. المركز القومي للإصدارات القانونية: القاهرة 2012.
- عبد الفتاح بيومي حجازي. الإثبات في الجرائم الكمبيوتر والانترنت. دون طبعة، دار الكتب القانونية مصر، 2008.
- عبد الفتاح بيومي حجازي. مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، ط1. دار الفكر الجامعي. الإسكندرية، 2006.
- عبد الفتاح حجازي، الحماية الجنائية المعلوماتية للحكومة الإلكترونية، دون طبعة، دار الكتب القانونية، مصر، 2007.
- عبد الله عبد الكريم، جرائم المعلوماتية والأنترنت –الجرائم الإلكترونية– دون طبعة، منشورات الحلبي الحقوقية، بيروت، 2007.
- علي عبد القادر القهوجي. الحماية الجنائية لبرامج الحاسب الآلي. ط.1 دار الجامعة الجديدة للطباعة والنشر: بيروت، 1999.
- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، الأحكام الموضوعية والجوانب الإجرائية، دون طبعة، دار النهضة العربية، مصر، 2004.
- عوض محمد عوض، المبادئ العامّة في قانون الإجراءات الجنائيّة، دون طبعة، دار المطبوعات الجامعية، الإسكندرية، مصر، 1999.

- كامل عفيفي، جرائم الكمبيوتر دون طبعة، منشورات الحلبي الحقوقية، لبنان، 2003.
- كيث دفلين، الإنسان والمعرفة في عصر المعلومات، ترجمة: شادن اليافي، الطبعة الأولى، مكتبة العبيكان، السعودية، سنة2001.
- مأمون محمد سلامة، "الإجراءات الجنائية في التشريع المصري"، الجزء الأول، دون طبعة، دار النهضة العربية، القاهرة، 2008.
- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري . الطبعة02، دار هومة، الجزائر، 2010.
- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، الطبعة الثانية، دار هومة، الجزائر، 2009.
- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة الرابعة، دار هومة للنشر والتوزيع والطباعة، الجزائر، 2009.
- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دون طبعة، دار النهضة العربية، مصر، سنة 1994.
- محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، الطبعة الأولى، دار النهضة العربية، مصر، 2016.
- محمد هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، دون طبعة، مكتبة الآلات الحديثة، مصر، سنة 1992.
- محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإليكترونية، طبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، سنة 2014.
- مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، 2001.
- مصطفي محمد موسي، "التحقيق الجنائي في الجرائم الإلكترونية"، الطبعه الأولى، مطابع الشرطه، القاهره، 2009.
- منصور بن محمد الغامدي، البيانات الحيوية، البصمة الصوتية، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، 2005.

- نبيلة هبة هروال. الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات. دون طبعة، دار الفكر الجامعي. الإسكندرية: 2013.
- نجيمي جمال، إثبات الجريمة على ضوء الاجتهاد القضائي، دراسة مقارنة، دون طبعة، دار هومة للنشر والتوزيع والطباعة، 2011.
- نديم عبده، أمن الكمبيوتر، الفيروسات والقرصنة المعلوماتية وانعكاساتها على الأمن القومي، الطبعة الأولى، دار الفكر للأبحاث والدراسات، بيروت، 1991.
- نهلا عبد القادر المومني .الجرائم المعلوماتية.، ط20.دار الثقافة للنشر والتوزيع، عمان، 2010.
- هلالي عبد الله، التزام الشاهد في الجريمة المعلوماتية. دون طبعة، دار النهضة العربية، القاهرة، 2006.
- هلالي عبد الله، تفتيش نظام الحاسب الآلي، وضمانات متهم المعلومات، دراسة مقارنة ، الطبعة الأولى، دار النهضة
- ياسر الأمير فاروق، مراقبة الأحداث الخاصة في الإجراءات الجزائية الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، مصر، 2009.

2. أطروحات الدكتوراه

- براهيمي جمال، التحقيق الجنائي في المراقبة الإلكترونية، أطروحة مقدّمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية جامعة مولود معمري تيزي وزو، السنة الجامعية 2018/2017.
- مجراب الدوادي، الأساليب الخاصّة للبحث والتحرّي في الجريمة المنظّمة، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة الجزائر 10، بن يوسف بن خدّة، الجزائر، السنة الجامعية 2016/2015.
- محمد صلاح محمد عبد المنعم، "الجرائم الإلكترونية وتحدياتها – دراسة مقارنة"، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2005.

3. رسائل الماجستير

- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 12-13، مذكرة مقدّمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، السنة الجامعية، 2013/2012.
- بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة وهرن، 2013/2012.
- حريزي ربيحة، إجراء جمع الأدلة ودورها في الكشف عن الجريمة، رسالة ماجستير، جامعة الجزائر، 2001.
- ركاب أمينة، اسالب التحري الخاصة في جرائم الفساد القانون الجزائري، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة ابو بكر بالقايد، تلمسان، 2015/2014.
- زوزو زوليخة، جرائم الصفقات العمومية، رسالة ماجستير، جامعة محمد خيضر، بسكرة، 2011.
- سعيداني نعيم. آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. مذكرة لنيل شهادة الماجيستير علوم جنائية. جامعة الحاج لخضر – باتنة. 2013/2012.
- صغير يوسف، الجريمة المرتكبة عبر الانترنت. مذكرة لنيل شهادة الماجيستير في القانون، جامعة مولود معمري، تيزي وزو، 2013.

4. المقالات:

- ثابت دنيا زاد، مراقبة الاتصالات والحق في حرمة الحياة الخاصّة في القانون الجزائري، العدد السادس، مجلة العلوم الاجتماعية والإنسانية، جامعة تبسة ، 2012.
- حاجة عبد العالي، قلات سمية، المكافحة الإجرائية لجرائم الإلكترونية " دراسة حالة الجزائر "، مجلة الفكر، العدد السادس عشر ، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، ديسمبر 2017.

- مختار سيدهم، (موجز اختصاص غرفة الاتهام)، مجلة المحكمة العليا، الغرفة الجنائية، العدد الثاني، الجزائر، 2005.

5. الملتقيات:

- محمد احمد الحمادي، تشريعات مكافحة جرائم تقنية المعلومات بدولة الإمارات، بحث مقدم لندوة جرائم تقنية المعلومات بوازرة الداخلية ومؤتمر جرائم تقنية المعلومات بجامعة الشارقة، 2006.
- نائل عبد الرحمن صالح، واقع جرائم الحاسوب في التشريع الجزائي الأردني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنيت المنعقد في كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2000.

فهرس المحتويات

بسملة ..... –
مقدمة ..... و
مبحث تمهيدي 6
المطلب الأول: الخصوصية الرقمية 6
الفرع الأول: تعريف الحق في الخصوصية 6
الفرع الثاني: محل الخصوصية الرقمية 9
الفرع الثالث: مبررات الحق في الخصوصية الرقمية 11
المطلب الثاني: التحقيق الجنائي 13
الفرع الأول: تعريف التحقيق الجنائي 13
الفرع الثاني: التمييز بين التحقيق الجنائي والتحقيق التقليدي 15
الفصل الأول:
الحق في الخصوصية الرقمية في مواجهة مقتضيات التحقيق التمهيدي
المبحث الأول: الإجراءات التي تعد انتهاكا للخصوصية الرقمية 37
المطلب الأول: إجراءات خاصة بالبيانات 37
الفرع الأول: جريمة التخزين والإفشاء غير المشروع للبيانات الشخصية 37
الفرع الثاني: جريمة المعالجة الإلكترونية للبيانات الشخصية دون ترخيص وتجاوز الغاية من المعالجة الإلكترونية 40
المطلب الثاني: الإجراءات الإلكترونية 41
الفرع الأول: التجسس الإلكتروني 42
الفرع الثاني: اختراق الحاسبات الآلية والبريد الإلكتروني 43
المبحث الثاني: مظاهر حماية الحق في الخصوصية الرقمية في ظل قانون الإجراءات الجزائري 19
المطلب الأول: الإجراءات التقليدية 19
الفرع الأول: المعاينة 19
المطلب الثاني: الإجراءات المستحدث 31
الفرع الأول: الخبرة 31
الفرع الثاني: الشهادة 33

خلاصة الفصل 37

الفصل الثاني:

الحق في الخصوصية الرقمية في مواجهة مقتضيات التحقيق الابتدائي

المبحث الأول: الإجراءات التقليدية 48

المطلب الأول: التفتيش.....48

الفرع الأول: تعريف التفتيش 48

الفرع الثاني: ضوابط تفتيش 51

المطلب الثاني: المراقبة الإلكترونية 58

الفرع الأول: تعريف المراقبة الإلكترونية: 58

المبحث الثاني: الإجراءات المستحدثة..... 65

المطلب الأول: التسرب 65

الفرع الأول: تعريفه 65

الفرع الثاني: شروطه وإجراءاته 67

المطلب الثاني: اعتراض المراسلات.....71

الفرع الأول: تعريفها.....71

الفرع الثاني: القيود الواردة على عملية اعتراض المراسلات.....72

المطلب الثالث: التحقيق لدى غرفة الاتهام 74

الفرع الأول: إخطار غرفة الاتهام بالبطلان 74

الفرع الثاني: فصل غرفة الاتهام في التحقيق 76

الفرع الثالث: اجراءات التحقيق امام قاضي الحكم 76

خلاصة الفصل 78

خاتمة..... 80

قائمة المصادر والمراجع..... 84

فهرس المحتويات 93