جامعة محمد خيضر بسكرة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة ماستر

الحقوق
فرع: قانون عام
تخصص: قانون إداري

رقم: .....

إعداد الطالب:
سناء عبان

يوم:

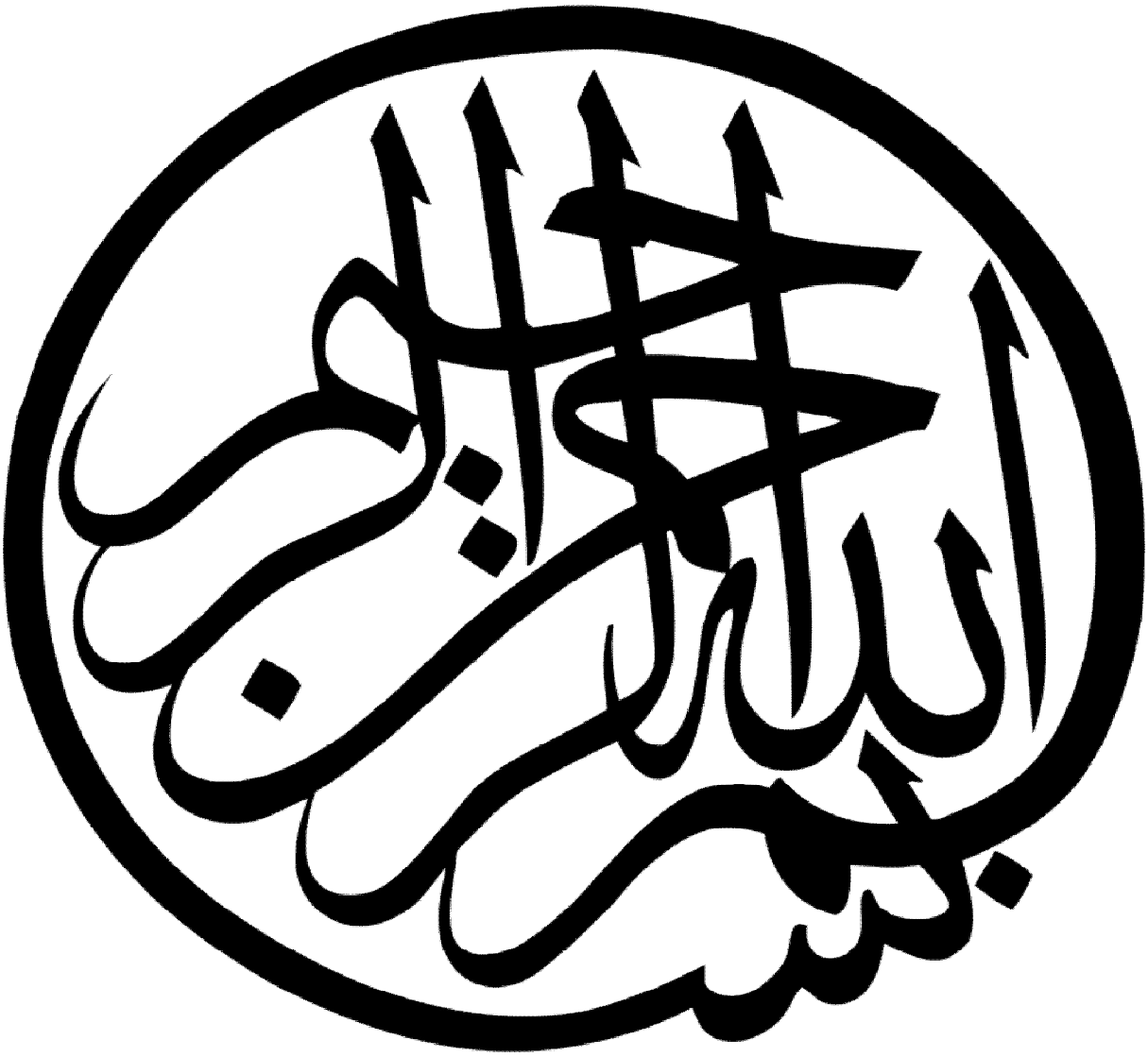
عنوان المذكرة:

الحماية الجنائية للوثائق البيومترية الصادرة عن الجماعات المحلية في التشريع الجزائري

لجنة المناقشة:

العضو 1	الرتبة	الجامعة	رئيسا
العضو 2 وردة شرف الدين	أستاذ محاضر	جامعة بسكرة	مشرفا
العضو 3	الرتبة	الجامعة	مناقشا

السنة الجامعية : 2018 - 2019


بسم الله الرحمن الرحيم

الإهداء

إلى روح جدتي الغالية رحمها الله وأسكنها فسيح جناته.

إلى من سعى و شقي لأنعم بالراحة والهناء الذي لم يبخل بشيء من أجل دفعي في طريق النجاح الذي علمني أن ارتقي سلم الحياة بحكمة وصبر إلى والدي العزيز أطال الله في عمره.

إلى الينبوع الذي لا يمل العطاء إلى من حاكت سعادتي بخيوط منسوجة من قلبها إلى والدتي العزيزة أطال الله في عمرها.

إلى من حبهم يجري في عروقي ويلج بذكراهم فؤادي إلى إخوتي وأخواتي وأخص بالذكر أخي عبد الغني الذي لم يبخل علي بالنصيحة والتوجيه طوال مشواري الدراسي.

إلى من سرنا سويا ونحن نشق الطريق معا نحو النجاح أصدقائي وزملائي وأخص بالذكر راضية.

إلى من علمونا حروفا من ذهب و كلمات من درر وعبارات من أسمى وأجلى عبارات في العلم إلى أساتذتنا الكرام.

إلى كل من ساعدني من قريب أو بعيد.

شكر وعرفان:

الحمد لله والشكر له سبحانه وتعالى على نعمه التي لا تعد ولا تحصى أن تفضل علي بالتوفيق لانجاز هذا العمل المتواضع، وأصلي وأسلم على الرحمة المهداة و السراج المنير سيدنا محمد صلى الله عليه وسلم وعلى آله وصحبه أجمعين في العالمين.

أتقدم بالشكر الجزيل في المقام الأول إلى أستاذتي الفاضلة، الأستاذة الدكتورة: (وردة شرف الدين) والتي تولت مهمة الإشراف على هذا البحث، أشكرها على كل نصائحها القيمة وجميل صبرها وحسن تواضعها وأسأل الله العلي القدير أن يزيدها رفعة وقدرا وعلما نافعا.

كما لا يفوتني أن أتقدم بالشكر، إلى كل أعضاء لجنة المناقشة المحترمة على مراجعتهم لما سيتم عرضه و تصويبهم له بما يرونه أصح.

مقـــدمة

مقدمـــــــــــــــة:

لقد دخلت البشرية في بداية الألفية الثالثة مرحلة جديدة من التطور الفكري والمعرفي الهائل غير المعهود، وذلك بفضل الثورة العلمية التكنولوجية في مجال الاتصالات والمعلومات التي اقتحمت بقوة في هذه المرحلة، حيث وفرت مناخا خصبا لنهضة علمية تكنولوجية شاملة غير مسبوقة في كافة مجالات الحياة الاقتصادية، الاجتماعية، الثقافية، والعلمية تهاوت أمامها الحدود السياسية والحواجز بين الدول والشعوب، وضاقت معها الأماكن وتقلصت فيها المسافات، واختزلت الأبعاد، بما تتميز به من عنصري السرعة والدقة في تجميع المعلومات.

وبالرغم من المزايا والفوائد الجمة التي تحققت وتتحقق يوما بعد يوم في كل مناحي الحياة بفضل تقنيات وسائل تكنولوجيا المعلومات والاتصال، إلا أن الاستخدام المتنامي لهذه التقنيات انطوى في الوقت ذاته على بعض الجوانب السلبية التي تمثل تهديدا خطيرا للأمن والاستقرار في المجتمع، جراء سوء استخدام هذه التقنية واستغلالها على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات، الشيء الذي استتبعه ظهور نمطا جديدا من الجرائم، لم يكن معهودا من قبل سمي بجرائم تقنية المعلومات أو الجرائم الالكترونية.

ولقد شمل التطور في استخدام تكنولوجيا المعلومات إلى اتجاه الدول ومن بينهم الجزائر نحو الأخذ بفكرة الإدارة الالكترونية لتسهيل إجرام المعاملات الالكترونية واستغلال الجهد والوقت في استكمال هذه المعاملات، وهذا ما حصل على مستوى قطاع الجماعات المحلية التي لجأت إلى استخدام الوثائق البيومترية الالكترونية بدل وثائق الهوية التقليدية، مثل بطاقة التعريف الوطنية البيومترية الالكترونية، جواز السفر البيومتري الالكتروني، رخصة السياقة البيومترية الإلكترونية، وقد حرص المشرع الجزائري على توفير حماية جنائية لهذه الوثائق بغية تحقيق الغرض الذي أنشأت من أجله وهذا ما سنتناوله في موضوع دراستنا.

أولا: أسباب اختيار الموضوع

هناك أسباب ذاتية وأخرى موضوعية دعتنا إلى اختيار هذا الموضوع. والتي تتمثل فيما يلي:

1- الأسباب الذاتية :

ترجع هذه الأسباب بالدرجة الأولى إلى الرغبة الشخصية في تناول هذا الموضوع بالدراسة والتعمق فيه، وهذا مرده الى اتجاه الدول في العصر الحديث إلى الأخذ بالإدارة الإلكترونية من جهة وتبني الجزائر هذا الأسلوب المتطور على مستوى إداراتها لتسهيل إبرام المعاملات للمواطن وتوفير السرعة والجهد والوقت لهم، وكانت الجماعات المحلية من بين الإدارات التي عرفت هذا التطور من خلال ما تصدره من وثائق بيومترية إلكترونية تلبية للمطالب الدولية بهذا الشأن من جهة ثانية.

2- الأسباب الموضوعية :

تكمن أهمية الموضوع في أنه من المواضيع الحديثة التي لم تتناولها الدراسات الدولية والوطنية بهذا الطرح فالكثير من الدراسات كتبت حول الوثائق البيومترية الإلكترونية دون اللجوء إلى دراسة الحماية الجنائية لها وأخرى بحثت حول: الحماية الجنائية من الجريمة الإلكترونية أو الحماية الجنائية للسندات الإلكترونية أو الحماية الجنائية للمعاملات الإلكترونية المصرفية أو التجارية أو الحماية الجنائية للعقود الإلكترونية أو الحماية الجنائية للتوقيع والتصديق الإلكتروني أو الحماية الجنائية للمعطيات الإلكترونية ذات الطابع الشخصي ....، أما الحماية الجنائية للوثائق البيومترية للجماعات المحلية فلم نعثر على دراسة علمية في هذا المجال على حد علمنا.

– إن هذا الموضوع يعتبر من المواضيع الجديدة والمتجددة ذات قيمة علمية حية ومفيدة في كافة مجالات الحياة العامة والخاصة، التي يجب ترصدها باستمرار ومعالجتها في صورة أبحاث علمية، كونه:

من جهة، يعالج الجريمة المعلوماتية التي تعد من أخطر الجرائم التي تمس بسيادة الدول وباقتصادها الوطني وأمنها القومي وبالحياة الخاصة بالأفراد حيث تعمل الدول جاهدة وباستمرار على إيجاد الأساليب الفعالة والمتطورة، المتناسبة مع التطور السريع لتكنولوجيا المعلومات وكذا الفكر الإجرامي البشري،

ومن جهة أخرى، كون دراستنا تتعلق بأسلوب الإدارة الإلكترونية، الذي يعتبر أسلوبا حديثا التجأت إليه الدول لتسيير وتطوير الإدارات، كمطلب أساسي نتيجة لتطور التكنولوجيا وسرعتها، من أجل تقليص والحد من التضخم الورقي، وتوفير الوقت والجهد على المواطن الذي عانى منذ سنوات من مشكلة البيوقراطية التي شلت سهولة ابرام المعاملات، كما أن هذا الأسلوب الحديث لتطوير الإدارات التقليدية يعرف هو أيضا منذ ظهوره التطور المستمر لإيجاد الآليات الجديدة الذي تضمن حسن سير المعاملات بسرعة وحسن ابرامها.

ثانيا : أهمية الموضوع

تتجلى أهمية الموضوع في الشقين العملي والعلمي حيث:

1- من الناحية العلمية:

تظهر الأهمية العلمية في موضوعنا من خلال ما يقدمه من أفكار ومعلومات متنوعة عن الوثائق البيومترية الالكترونية، من حيث بيان: مبررات لجوء الجماعات المحلية للأخذ بفكرة الوثائق البيومترية الالكترونية، والتعرف على أنواع هذه الوثائق والمتمثلة في بطاقة التعريف الوطنية البيومترية الإلكترونية، جواز السفر البيومتري الإلكتروني، رخصة السياقة

البيومترية الإلكترونية، وكيفية الحماية الجنائية الموضوعية في التشريع الجزائري من خلال التطرق إلى أهم الجرائم الماسة بهذه الوثائق والعقوبات المقررة لها، وكذا الحماية الجنائية الإجرائية لهذا النوع من الوثائق في التشريع الجزائري من خلال الوقوف على تعريف الدليل الإلكتروني الناتج عن ارتكاب الجرائم الماسة بهذه الوثائق وأيضا كيفية قبول القاضي الجنائي لهذا النوع من الجرائم في مجال الإثبات.

2- من الناحية العملية :

فموضوع الدراسة يمكن أن يستفيد منه من الناحية العملية العديد من الجهات إذ يبين لأفراد المجتمع أهم أنماط الجرائم المعلوماتية التي يمكن أن تمس بالوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية والتي قد تعرضهم في حال ارتكابها لمتابعة قضائية، وبالنسبة لرجال القانون، فتفيد هذه الدراسة المحققين من التعرف على خصائص الدليل الإلكتروني، الذي يختلف كل الاختلاف على الدليل المادي الناتج عن ارتكاب الجرائم التقليدية، كالسرقة والقتل والرشوة والاختلاس... وعلى أنواع الدليل الإلكتروني الناتج عن الجرائم الماسة بالوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية والأماكن التي يمكن أن يتواجد بها وتبين لهم أهم الإجراءات الجزائية المتبعة في جمع الدليل الإلكتروني التقليدية منها والحديثة.

ثالثا : أهداف الدراسة

نهدف من خلال هذه الدراسة إلى جملة من الأهداف، تتمثل في :

- بيان مفهوم الوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية، وأنواعها، ومبررات لجوء الجماعات المحلية إلى الأخذ بها بدل الوثائق التقليدية.

- بيان الجرائم الواقعة على الوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية والعقوبات المقررة لها.

- تحديد الإجراءات المتبعة في الجرائم الواقعة على الوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية.

– التعرف على مدى قبول القاضي الجزائي للدليل الإلكتروني الناتج عن الجرائم الواقعة على الوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الإثبات.

رابعا: إشكالية الموضوع

بالرجوع إلى الدور الأساسي التي أصحبت تلعبه الوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في وقتنا الراهن، ونظرا للقيمة القانونية التي اكتسبتها، فقد بات من الضروري توفير الحماية والأمن القانوني لها من جهة، إلى أن تصبح هذه الوثائق دليلا في الإثبات تقف على قدم المساواة مع الوثائق الورقية من جهة أخرى.

ومنه فانه يمكن طرح الإشكالية التالية:

ما مدى فعالية الحماية الجنائية التي خصها المشرع الجزائري للوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية؟

و تندرج هذه الإشكالية الرئيسية عدة إشكاليات فرعية تتمثل في :

1- ما مدى كفاية النصوص العقابية الموضوعية التقليدية في حماية الوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر؟

2- ما مدى كفاية الإجراءات الجزائية التقليدية في جمع الأدلة الإلكترونية الناتجة من ارتكاب الجرائم الماسة بالوثائق البيومترية الالكترونية؟

3- ما مدى حجية الدليل الإلكتروني الناتج عن ارتكاب الجرائم الماسة بالوثائق البيومترية الالكترونية في الإثبات الجنائي؟.

خامسا: صعوبات الموضوع

من بين الصعوبات التي واجهتنا عند معالجتنا لهذا الموضوع حداثة الموضوع خاصة في التشريع الجزائري، مما أدى معه إلى قلة المراجع والكتب المتخصصة في هذا المجال، الأمر الذي دفعنا إلى الرجوع للمؤلفات والمراجع العامة من أجل جمع المادة العلمية بخصوص هذا الموضوع.

سادسا: الدراسات السابقة

توجد بعض الدراسات السابقة، والتي تناولت مواضيع مختلفة للجريمة الالكترونية، والتي تتشابه في بعض النقاط مع بحثنا إلى أنها تختلف عنه في بعض الزوايا أيضا ومن بين هذه الدراسات نذكر:

- **الدراسة الأولى:**

أطروحة دكتوراه بعنوان: الإثبات الجنائي بالأدلة الإلكترونية – دراسة مقارنة–، من إعداد الطالبة: شرف الدين وردة، مقدمة لكلية الحقوق جامعة بسكرة، حيث تناولت الطالبة ماهية الدليلي الجنائي الإلكتروني، ثم ماهية الجريمة المعلوماتية كمحل للدليل الجنائي الإلكتروني وكذا وسائل الإثبات المتبعة في جمع الدليل الجنائي الإلكتروني من وسائل إثبات تقليدية وأخرى حديثة، تتشابه دراستنا من حيث تناولنا تقريبا للعديد من المواضيع المشابهة لها لأن هذه الدراسة دراسة عامة تنطبق على كل البحوث العلمية التي تمس بالإجرام المعلوماتي وكيفية التصدي له، وتختلف دراستنا عنها في أن دراسة الطالبة كانت دراسة مقارنة بين العديد من التشريعات الوطنية العربية منها والأجنبية والاتفاقيات الدولية الخاصة بالجريمة المعلوماتية مع التشريع الجزائري، بينما دراستنا كانت محددة ومحصورة في إطار التشريع الجزائري، كما أن دراستنا كانت متخصصة ومحددة في نوع من الإجرام المعلوماتي وهي الجرائم الإلكترونية التي ترتكب على الوثائق

البيومترية الإلكترونية الصادرة عن الجماعات المحلية وكذا تناولنا الإجراءات المتبعة في جمع الأدلة الإلكترونية الناتجة عن ارتكاب هذه الجرائم في التشريع الجزائري.

- الدراسة الثانية:

- أطروحة دكتوراه بعنوان : الحماية الجنائية للمحررات الالكترونية من التزوير، إعداد الطالبة الهام بن خليفة، مقدمة لكلية الحقوق، جامعة باتنة، حيث تحدثت الطالبة عن بيان مفهوم المحررات الالكترونية، انطلاقا من تعريفات الفقه والقانون، مبينة أسباب ظهورها و خصائصها واختلافها عن المحررات الورقية، تقترب هذه الأطروحة من دراستنا في تطرقها إلى الحماية الجزائية الموضوعية والإجرائية معا، إلا أن دراستنا تختلف عنها في تناول نوع من المحررات الإلكترونية الرسمية والمتمثلة في: الوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية في الجزائر.

الدراسة الثالثة:

- أطروحة دكتوراه بعنوان: جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، من إعداد الطالبة براهيمي حنان، مقدمة لكلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، حيث تطرقت الباحثة إلى مفهوم الوثيقة المعلوماتية، يلتقي بحثنا مع هذه الدراسة في أن الطالبة تحدثت عن الحماية الجزائية الموضوعية للوثيقة المعلوماتية، بينما تطرقنا في بحثنا بالإضافة إلى الحماية الموضوعية للوثائق المعلوماتية، الحماية الجزائية، كما أن دراستنا كانت متخصصة في نوع واحد من الوثائق الرسمية الإدارية ذات الصبغة المعلوماتية وهي الوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية في الجزائر.

الدراسة الرابعة:

– أطروحة الماجستير، بعنوان : الحماية الجنائية للمعاملات الالكترونية، للطالب طعبان أمين، كلية الحقوق، جامعة باتنة، حيث تناول الطالب كل ما يخص جرائم المعلوماتية، ويلتقي بحثنا مع هذه الدراسة في التطرق إلى الجوانب الموضوعية الخاصة بالإجرام المعلوماتي، بينما تختلف دراستنا في أن الطالب تحدث في أطروحته عن الحماية الجزائية الموضوعية فقط للمعاملات الإلكترونية، في حين دراستنا تضمنت بالإضافة لذلك إلى الحماية الجنائية الإجرائية.

والعديد من المراجع الأخرى التي تناولت بعض الجزئيات المتعلقة بالموضوع.

سابعا : منهج الموضوع

للإجابة عن الإشكالية المطروحة اتبعنا المنهج الوصفي التحليلي وذلك من خلال التطرق لأنواع الوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية بالجزائر، ووصف الجرائم الواقعة عليها، بالإضافة إلى التطرق للإجراءات الجزائية المستحدثة في إطار مكافحة الجريمة المعلوماتية في التشريع الجزائري، والعمل على تحليل مختلف النصوص العقابية المنظمة لها.

كما استعنا على سبيل الاستئناس بالمنهج الاستدلالي من خلال الاستدلال بالنصوص العقابية الجزائرية التي تم سنها في مجال البحث.

ثامنا : خطة الدراسة

لقد تم تقسيم موضوعنا إلى مبحث تمهيدي وفصلين رئيسيين.

حيث المبحث التمهيدي خصصناه لدراسة الإطار المفاهيمي للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية، والذي قسمناه إلى مطلبين حيث تناولنا في المطلب الأول : مفهوم الوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر، أما المطلب الثاني، فتحدثنا فيه عن مفهوم الشباك الالكتروني.

أما الفصل الأول فخصصناه لدراسة الحماية الجنائية الموضوعية للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر، حيث قسمناه إلى مبحثين، المبحث الأول تناولنا فيه مفهوم الجرائم الالكترونية المرتكبة على الوثائق البيومترية الالكترونية، بينما تحدثنا في المبحث الثاني عن نطاق تطبيق الحماية الجنائية الموضوعية للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر.

بينما بحثنا في الفصل الثاني، عن الحماية الجنائية الإجرائية للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر، حيث قسمناه بدوره إلى ثلاث مباحث، المبحث الأول تطرقنا فيه إلى الحماية الجنائية الإجرائية التقليدية للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر، أما المبحث الثاني فخصصناه لدراسة الحماية الجنائية الإجرائية الحديثة للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر، و المبحث الثالث، تناولنا فيه تقدير القاضي الجزائي للأدلة الرقمية الناتجة عن الجرائم الماسة بالوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر.

وفي ختام بحثنا، تطرقنا إلى أهم النتائج التي توصلنا إليها من خلال دراستنا لموضوع الحماية الجنائية للوثائق البيومترية الصادرة عن الجماعات المحلية في التشريع الجزائري، وإلى مجموعة من الاقتراحات التي نقترحها في هذا الموضوع والتي تعتبر إضافة لموضوع البحث، ونكون بذلك قد أجبنا على الإشكاليات القانونية التي طرحناها في مقدمة البحث.

المبحث التمهيدي:

الإطار المفاهيمي للوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية

تعتبر الوثائق البيومترية الالكترونية من الوثائق المستحدثة في مجال الإدارة الالكترونية، لذلك سنتطرق في هذا المبحث إلى مفهوم الوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في المطلب الأول، أما المطلب الثاني فسنتطرق إلى مفهوم الشباك الالكتروني باعتبار الحل التقني الذي يعمل على استقبال طلبات مختلف الوثائق البيومترية الإلكترونية وتسجيلها.

المطلب الأول: مفهوم الوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية.

ندرج هذا المطلب في أربعة فروع حيث نتكلم في الفرع الأول عن: مبررات لجوء الجماعات المحلية للأخذ بفكرة الوثاق البيومترية الالكترونية، وفي الفرع الثاني عن: مفهوم بطاقة التعريف الوطنية البيومترية الالكترونية، أما في الفرع الثالث نتحدث عن: مفهوم رخصة السياقة البيومترية الالكترونية، لنتختم في الفرع الرابع للحديث عن: مفهوم جواز السفر البيومتري الالكتروني.

الفرع الأول: مبررات لجوء الجماعات المحلية للأخذ بفكرة الوثائق البيومترية الالكترونية:

إن التحول السريع والمتواصل للمجتمع الجزائري تولدت عنه احتياجات[1]، جديدة للمواطنين في جميع المجالات، الشيء الذي استوجب ضرورة إعادة النظر في أعمال الإدارة لتكييفها مع هذه الاحتياجات، والتكفل بجميع مراحل هذا التطور الطموح.

ولتجسيد ذلك في الواقع الملموس، قامت وزارة الداخلية والجماعات المحلية والتهيئة العمرانية باتخاذ العديد من الإجراءات الهادفة للقضاء على الاختلالات المتسببة في تعطيل بعض مصالح المواطنين بفعل المعالجة الكلاسيكية اليدوية للملفات الإدارية وعدم الشفافية في التسيير والبيروقراطية وكثرة الوثائق المكونة للملفات وغيرها، وهي عوامل ساهمت في مراحل سابقة في التأثير السلبي على مصداقية العلاقة بين الإدارة والمواطن.[2]

وفي جملة هذه الإجراءات،كان لا بد من توفير الشروط المناسبة لعصرنة الإدارة، والانتقال التدريجي من مرحلة التسيير الكلاسيكي إلى مرحلة التسيير الآلي عن طريق إصلاح مرافق

[1]- المنشور الوزاري رقم 02، المؤرخ في 21 مارس 2018، **المتضمن تأطير مسار الشباك الالكتروني الخاص بالوثائق البيومترية وطرق استغلاله**، ص01.

[2]- المصدر نفسه، نفس الصفحة.

الإدارة المركزية وا إدارة الجماعات المحلية،وا إدخال التكنولوجيا الحديثة في مجالات التسيير والتنظيم،وبالتالي إعادة الاعتبار للمرفق العام وتحسين أدائه بصفة مستمرةوا إحداث أنماط عمل جديدة وعصرية ترتكز أساسا على الاستغلال الأمثل للتكنولوجيا المتطورة[1]وا إرساء قواعد عمل عصرية مدعومة بموارد بشرية مؤهلة وقد أحدثت وزارة الداخلية والجماعات المحلية والتهيئة العمرانية الشباك الالكتروني للوثائق البيومترية (جواز السفر وبطاقة التعريف الوطنية ورخصة السياقة)، وسيتم توسيعه بصفة تدريجية إلى وثائق أخرى...

الفرع الثاني: مفهوم بطاقة التعريف الوطنية البيومترية الالكترونية

يقتضي الوقوف على مفهوم بطاقة التعريف الوطنية، تعريفها ثم بيان كيفية إعدادها وتسليمها وكيفية تجديدها، وسنتكلم عن كل ذلك من خلال ما يلي:

أولا: تعريف بطاقة التعريف الوطنية البيومترية

هي وثيقة تثبت هوية صاحبها هي فردية تسلم لكل مواطن جزائري بدون شرط السن،[2] ولا يمكن لأي كان أن يحوز على أكثر من بطاقة تعريف واحدة في نفس الوقت،[3] كما تحدد مدة صلاحيتها بعشر سنوات (10) للأشخاص البالغين تسعة عشر (19) سنة فأكثر، وتحدد بخمس سنوات للقصر الذين يقل سنهم عن تسعة عشر سنة (19) وتسري مدة صلاحيتها ابتداء من تاريخ إعدادها[4]، وتحتوي بطاقة التعريف الوطنية البيومترية على شريحتين:

- تتضمن الشريحة الأولى: معلومات إدارية ومعلومات تخص صاحبها.
- تتضمن الشريحة الثانية: التطبيق من أجل التحقق من صاحبها.[5]

---

[1]- المنشور الوزاري رقم 02، المؤرخ في 21 مارس 2018، المتضمن تأطير مسار الشباك الالكتروني الخاص بالوثائق البيومترية وطرق استغلاله، المصدر نفسه، ص1.

[2]- المادة 03من المرسوم الرئاسي رقم 17-143 المؤرخ في 21 رجب عام 1438 الموافق 18 أفريل 2017، **المتعلق بتحديد كيفيات إعداد بطاقة التعريف الوطنية وتسليمها**، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد25، الصادرة بتاريخ 19 أفريل 2017، ص10.

[3]- المادة 04 من المصدر نفسه، نفس الصفحة.

[4]- المادة 05 من المصدر نفسه، نفس الصفحة.

[5]- المادة 06 من المصدر نفسه، نفس الصفحة.

كما أن بطاقة التعريف البيومترية تسلم مرفقة برمز سري في ظرف مغلق يوضع تحت مسؤولية صاحبها أووليه الشرعي، فيستعمل الرقم السري من أجل الولوج إلى الخدمات الالكترونية.[1]

ثانيا: إعداد بطاقة التعريف الوطنية البيومترية الالكترونية وتسليمها

1-إعداد بطاقة التعريف الوطنية:

تعد بطاقة التعريف الوطنية مصالح وزارة الداخلية والجماعات المحلية، وتودع ملفات طلب بطاقة التعريف الوطنية على مستوى إحدى بلديات ولاية الإقامة بالنسبة للمواطنين المقيمين في التراب الوطني أو لدى المراكز الدبلوماسية والقنصلية بالنسبة للمواطنين المسجلين في الخارج[2].

في حين تنص المادة 10 من المرسوم الرئاسي رقم 17-143 المتعلق بتحديد كيفيات إعداد بطاقة التعريف الوطنية وتسليمها على أنه :(تسلم السلطة المختصة التي أودع لديها ملف الطلب، بطاقة التعريف الوطنية لصاحبها فور إعدادها.)

ويبلغ الطالب بإعدادها بكل وسيلة ملائمة. تلغى وتتلف كل بطاقة تعريف وطنية تم إعدادها و لم تسحب من قبل صاحبها، في أجل "06" أشهر من تاريخ إشعاره بالسحب، ويجب على السلطة المختصة بالتسليم أن تعلم موقع تشخيص الوثيقة من أجل تعطيل الإمكانيات الوظيفية للبطاقةتحدد كيفيات إلغاء بطاقة التعريف الوطنية وا ٍتلافها بموجب قرار من الوزير المكلف بالداخلية[3].

[1]- المادة 07 من المرسوم الرئاسي رقم 17-143 المؤرخ في 21 رجب عام 1438 الموافق 18 أفريل 2017، المتعلق بتحديد كيفيات إعداد بطاقة التعريف الوطنية وتسليمها،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية. المصدر السابق، ص 10.

[2]- المادة 09 من المصدر نفسه، نفس الصفحة.

[3]- المادة 10 من المصدر نفسه، ص 11

2-تسليم بطاقة التعريف الوطنية:

أ-تسليم بطاقة التعريف الوطنية للمواطنين المقيمين في التراب الوطني:

في هذه الحالة تسلم من قبل الوالي أو أي موظف أخر يفوضه لهذا الغرض، على أساس ملف يحتوي على استمارة يملؤها ويوقعها المعني، أوالولي الشرعي بالنسبة للقصر، وترفق بما يأتي[1]:

- شهادة الجنسية
- شهادة إقامة سارية المفعول
- صورتان (02) شمسيتان للهوية حديثتان وبالألوان ومتماثلتان بخلفية موحدة بدون إطار وباللون الأبيض.

ب-تسليم بطاقة التعريف الوطنية للمواطنين المقيمين في الخارج:

في هذه الحالة تسلم من قبل رؤساء المراكز الدبلوماسية والقنصلية أو أي موظف قنصلي أخر مؤهل يفوض لهذا الغرض، على أساس ملف يحتوي على استمارة يملؤها ويوقعها المعني، أو الولي الشرعي بالنسبة للقصر، وترفق بما يأتي:[2]

- شهادة الجنسية.
- نسخة من بطاقة التسجيل القنصلية.
- صورتان (02) شمسيتان للهوية حديثتان وبالألوان ومتماثلتان، بخلفية موحدة وبدون إطار وباللون الأبيض.

جاء في نص المادة 13 على أن حضور طالب بطاقة التعريف الوطنية إجباري من أجل التقاط المعطيات البيومترية.

---

[1]- المادة 11، من المرسوم الرئاسي رقم 17-143 المؤرخ في 21 رجب عام 1438 الموافق 18 أفريل 2017، المتعلق بتحديد كيفيات إعداد بطاقة التعريف الوطنية وتسليمها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق، ص 11.

[2]- المادة 12 من المصدر نفسه، نفس الصفحة.

يعفى القصر البالغون أقل من اثنتي عشر (12) سنة من التقاط البصمات الإصبعية.تتأكد المصالح المختصة بالبلدية أو المراكز الدبلوماسية والقنصلية، حسب الحالة، من صحة المعلومات المتعلقة بالحالة المدنية لطالب بطاقة التعريف الوطنية[1].

يعفى كل مواطن يحوز على جواز سفر يتضمن معطيات بيومترية من إجراء التقاط هذه المعطيات عند طلبه بطاقة التعريف الوطنية.غير أنه يمكن للمواطن أن يطلب إعادة إجراء التقاط المعطيات البيومترية في حالة ما إذا استلزم الأمر ذلك[2].

في حالة وفاة صاحب بطاقة التعريف الوطني، تبلغ البلدية أو المركز الدبلوماسي والقنصلي التي سجلت لديها الوفاة، دون مهلة، سلطة الإصدار بغرض جعل هذه الوثيقة غير قابلة للاستعمال[3].

ثالثا: تجديد بطاقة التعريف الوطنية البيومترية الالكترونية

يمكن طلب تجديد بطاقة التعريف الوطنية في الحالات الآتية[4]:

1-خلال الثلاثة (03) أشهر التي تسبق تاريخ انقضاء صلاحيتها.

2-في حالة تغيير المعلومات المتعلقة بالحالة المدنية لطالبها.

3-عند بلوغ القاصر صاحب بطاقة التعريف الوطنية سن تسعة عشر (19) سنة.

4-عند التصريح بضياعها أو إتلافها أو سرقتها.

في حالة ضياع بطاقة التعريف الوطنية أو إتلافها أو سرقتها، يلزم صاحبها بالتصريح بذلك فورا. لدى أقرب مصلحة أمن أو لدى المراكز الدبلوماسية والقنصلية في الخارج.

---

[1]- المادة 14 من المرسوم الرئاسي رقم 17-143 المؤرخ في 21 رجب عام 1438 الموافق 18 أفريل 2017، المتعلق بتحديد كيفيات إعداد بطاقة التعريف الوطنية وتسليمها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق، ص 11.

[2]- المادة 15 من المصدر نفسه، نفس الصفحة.

[3]- المادة 16 من المصدر نفسه، نفس الصفحة.

[4]- المادة 17 من المصدر نفسه، نفس الصفحة

يجب على مصالح الأمن والمراكز الدبلوماسية والقنصلية أن تعلم دون مهلة، البلدية أو المركز الدبلوماسي والقنصلي مكان الإصدار بغرض جعل بطاقة التعريف الوطنية غير قابلة للاستعمال.كما يجب أن تعلم هذه المصالح مصلحة صحيفة السوابق القضائية المركزية في حالة ضياع أو سرقة بطاقة التعريف الوطنية[1].

يتكون ملف تجديد بطاقة التعريف الوطنية من استمارة يملؤها ويوقعها المعني أو الولي الشرعي بالنسبة للقصر ،وترفق بمايأتي:

1-بطاقة التعريف الوطنية منتهية الصلاحية أو التصريح بالضياع أو الإتلاف أو السرقة.

2-شهادة إقامة سارية المفعول في حالة تغيير الإقامة.

3-صورة (01) شمسية للهوية حديثة بالألوان بخلفية موحدة دون إطار باللون الأبيض.[2]

يتعرض كل شخص يقلد أو يزور أو يزيف بطاقة التعريف الوطنية أو يستعمل عمدا بطاقة تعريف وطنية مقلدة أو مزورة أو مزيفة، إلى العقوبات المنصوص عليها في التشريع المعمول به.[3]

الفرع الثالث: مفهوم رخصة السياقة البيومترية الالكترونية

في إطار الاستمرار في عصرنة المرفق العام الذي بادرت به وزارة الداخلية والجماعات المحلية والتهيئة العمرانية، من خلال تحديث وثائق الهوية والتنقل وكذا تبسيط إجراءات الحصول عليها وتخفيف مكونات ملفات طلب الحصول عليها، تم الشروع في إصدار نموذج جديد لرخصة السياقة من النوع البيومتريالالكتروني والقابل للقراءة آليا بموجب المنشور الوزاري المشترك رقم 03 المؤرخ في 04 جوان 2018. وسنتكلم في هذا الفرع للفئات المعنية باستصدار رخصة السياقة البيومترية الإلكترونية، الوثائق المكونة لملف طلب رخصة السياقة

[1]- المادة 18 من المرسوم الرئاسي رقم 17-143 المؤرخ في 21 رجب عام 1438 الموافق 18 أفريل 2017، المتعلق بتحديد كيفيات إعداد بطاقة التعريف الوطنية وتسليمها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق ذكره، ص 11.

[2]- المادة 19 من المصدر نفسه، نفس الصفحة.

[3]- المادة"20 من المصدر نفسه، نفس الصفحة.

البيومترية الإلكترونية وا ٍجراءات معالجة الملف، إجراءات تسليم رخصة السياقة البيومترية الإلكترونية وذلك من خلال التالي:

أو لا: الفئة المعنية باستصدار رخصة السياقة البيومترية الالكترونية

يتم إصدار رخص السياقة البيومترية الالكترونية حصريا للملفات الواردة في مديريات النقل الولائية والخاصة بـ:[1]

1-السائقين الجدد الذين نجحوا في اختبارات الحصول على رخصة السياقة النظرية والتطبيقية.

2-السائقين الذين تحصلوا على صنف جديد يضاف إلى الصنف أو الأصناف المتحصل عليها سابقا.

ثانيا: الوثائق المكونة لملف طلب رخصة السياقة البيومترية الإلكترونيةوا ٍجراءات معالجة الملف:

وتتمثل في الوثائق التالية:[2]

1-الوثائق المكونة لملف الطلب:

يحتوي الملف التنظيمي الوارد من مديرية النقل على جميع المعلومات الخاصة بالسائق الجديد (معلومات طبية، الإقامة، الزمرة الدموية، تاريخ ومكان الميلاد والصنف المتحصل عليه)، وذلك طبقا لأحكام القرار الوزاري المشترك المؤرخ في أول أوت 1989 المحدد لشروط تسليم رخصة سياقة السيارات وصلاحيتها.

إضافة إلى هذا يجب إدراج رقم هاتف المعني بالأمر عند حضوره لاستكمال إجراءات أخذ البيانات البيومترية.يطلب من الشخص المعني عند حضوره لاستكمال إجراءات أخذ البيانات البيومترية:

[1]- المنشور الوزاري رقم 06، المؤرخ في 05 نوفمبر 2018، **المتضمن الترتيبات التنظيمية المؤطرة للتحديثات المضافة للشباك الالكتروني لاسيما المتعلقة بإصدار رخصة السياقة البيومترية الالكترونية**، ص02.

[2]- المصدر نفسه، ص03.

أ) تقديم طابع جبائي أو قسيمة جبائية تتوافق قيمتها مع أحكام المادة 144 من الأمر رقم 76-103 المؤرخ في 09 ديسمبر 1976 المعدل والمتمم المتضمن قانون الطابع.

ب) إرفاق صورتين شمسيتين مطابقة للمعايير بخلفية بيضاء.

2-إجراءات معالجة الملف: تتمثل اجراءات معالجة الملف فيما يلي[1]:

أ) ينبغي على المصلحة المكلفة بإصدار رخص السياقة أن تبادر فور وصول الملف إلى حجز المعطيات البيومترية المتضمنة في الوثائق الإدارية المكونة له بواسطة التطبيقة المعلوماتية الموضوعية لهذا الغرض، لتقوم بعدها بدعوة المعني بجميع الوسائل المتوفرة (رسالة نصية قصيرة، هاتف...) للحضور من أجل أخذ معطياته البيومترية وفق نفس المنهج المتبع في معالجة طلبات بطاقة التعريف الوطنية وجواز السفر البيومتري الالكترونيين عبر الشباك الالكتروني.

ب) بعد دعوته، يتقدم المعني من المصلحة المختصة مرفوق بشهادة النجاح المسلمة من طرف مفتش السياقة والأمن في الطرق يسلمها للمصلحة المختصة التي تضعها ضمن ملف قاعدي.

ج) بعد التأكد من هوية المعني بالأمر وتفحص معطياته يتم معالجة الملف عبر الشباك الالكتروني وفق نفس الشروط والمعايير المتبعة في مجال إصدار بطاقة التعريف الوطنية وجواز السفر البيومتريين الالكترونيين وفقا للمنشور الوزاري المؤرخ في 21 مارس 2018 المتضمن تأطير مسار الشباك الالكتروني الخاص بالوثائق البيومترية وطرق استغلاله.

د) يسلم للمعني بالأمر بعد أخذ جميع معلوماته وصل استلام يدعى، حسب الحالة "وصل إيداع" أو "شهادة تأهيل مؤقتة" عملا بأحكام المادة 17 من القرار الوزاري المشترك المؤرخ في أول أوت 1989 والتي تتضمن جميع المعلومات الضرورية التي تسمح بتسييرها كرخصة سياقة، لا سيما بالنسبة لمصالح الأمن المكلفة بأمن الطرقات.

[1]- المنشور الوزاري رقم 06، المؤرخ في 05 نوفمبر 2018، المتضمن الترتيبات التنظيمية المؤطرة للتحديثات المضافة للشباك الالكتروني لاسيما المتعلقة بإصدار رخصة السياقة البيومترية الالكترونية، المصدر السابق، ص ص 03، 04.

و) لا يمكن أن تكون شهادة التأهيل المؤقتة موضوع تمديد صلاحية أو تجديدوفي حالة ضياعها يمكن للمعني بالأمر طلب استخراج نسخة ثانية لشهادة التأهيل المؤقتة وفق التنظيم ساري المفعول.

ثالثا: إجراءات تسليم رخصة السياقة البيومترية الالكترونية

بعد انجاز رخصة السياقة البيومتريةالالكترونية، يتم إرسالها إلى المصالح البلدية المكلفة بإصدارها وفق النظام المحدد من طرف مديرية السندات و الوثائق المؤمنة.يجب على هذه المصالح أن تقوم بما يلي:[1]

1-تبليغ الشخص المعني فورا وبجميع الوسائل المتوفرة للتقدم إلى المصلحة لاستلام رخصة سياقته.

2-يجب على المعني بالأمر التقدم شخصيا لاستلام رخصة سياقته مرفوقا بشهادة التأهيل المؤقتة أو وصل الإيداع.

3-يتم دعوة المعني بالأمر إلى قراءة المعلومات المسجلة على الدعامة للتأكد من صحتها.

4-يتم تسجيل تسليم رخصة السياقة البيومترية الالكترونية لفائدة صاحبها عبر الطريقة الالكترونية دون اللجوء إلى سجل الإيداع،ويتم التأكد من هوية المعني بالأمر عن طريق مطابقة البصمات.

5-لاتسلم رخصة السياقة للمعني بالأمر إلا بعد تفعيلها عن طريق تطبيقة خاصة والتي تستلزم تسجيلها في البطاقة الوطنية لرخص السياقة.

الفرع الرابع: مفهوم جواز السفر البيومتري الالكتروني

يحتاج أي شخص سواء كان مواطنا جزائريا أو أجنبيا أثناء تنقله بين الدول إلى الوثائق تسمح له بهذا التنقل، ولعل أهم هذه الوثائق وثيقة جواز السفر الذي يعتبر وثيقة رسمية لها

[1]- المنشور الوزاري رقم 06، المؤرخ في 05 نوفمبر 2018، المتضمن الترتيبات التنظيمية المؤطرة للتحديثات المضافة للشباك الالكتروني لاسيما المتعلقة بإصدار رخصة السياقة البيومترية الالكترونية، المصدر السابق، ص 04.

مواصفات قانونية خاصة. وسنتكلم في هذا الفرع عن: تعريف جواز السفر البيومتري الإلكتروني، خصائصه، أنواعه، وذلك من خلال التالي:

أولا: تعريف جواز السفر البيومتري الالكتروني

جواز السفر البيومتري هو وثيقة رسمية مؤمنة ومكونة من عدة صفحات من متعدد الكربونات (مادة صعبة الإتلاف) يتوفر على شريحة بيانات مدمجة بداخله، يتضمن جواز السفر البيومتري عناصر الأمان المرتكزة على التكنولوجيا الأكثر تطورا في هذا المجال حيث توفر حماية صاحبه ضد كل استعمال تدليسي لهذه الوثيقة في حالة ضياعها أو سرقتها أو في انتحال الشخصية، ويفضل الكتابة عن طريق النقش بالليزر، وكما أن لا يمكن تغيير ولا تحريف البيانات البيوغرافية الموجودة في الجواز، كما أن صورة حامله تأخذ بعين الاعتبار احترام معايير الوكالة الدولية للطيران المدني[1].

ثانيا: خصائص جواز السفر البيومتري الالكتروني

إن التطور الذي عرفته الأنظمة الداخلية للدول ومنها الجزائر أصبح للأبد بل أمر حتمي مساير التطور الدولي الذي يعرف تطورا تكنولوجيا في كل الأنظمة حتى في مجال البيانات الشخصية للمواطنين كالحالة المدنية مثلا وأصبح هناك نظام يخص كل من وثائق السفر، فأصبح من الضروري إدخال مثل هذه الأنظمة للدولة الجزائرية، فأصدر جواز سفر جديد يعرف باسم جواز السفر البيومتري الالكتروني. ومن خصائص جواز السفر البيومتري الإلكتروني ما يلي:

أ-من حيث الشكل الخارجي:

يضم جواز السفر البيومتري الالكتروني شريحة الكترونية من دون صلة تحتوي على الشهادات الالكترونية للدولة الجزائرية وعلى معلوماته البيومترية الرقمية من ضمنها الصورة الشمسية وتوقيعه وبصماته، أن من ضمن المميزات التي أضيفت إلى جواز السفر هي الشريحة الالكترونية التي تخزن فيها مجموعة من المعلومات التي توضح لنا صاحب جواز السفر حيث

[1]- المادة 06 من القانون رقم 14-03 المؤرخ في 2014/02/24، **المتعلق بسندات ووثائق السفر**، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 16، الصادرة في 2014/03/23، ص04.

أنها تحتوي رمز الدولة الجزائرية والمعلومات الخاصة بصاحب جواز السفر، بالإضافة إلى الصورة الرقمية الخاصة به، مع إدراج توقيعه والبصمة ضمن هذه الشريحة[1].

إن جواز السفر البيومتري الالكتروني وثيقة مغلفة مستطيلة الشكل طولها 125مليمتر، وعرضها 88 مليمتر، ويركب غلاف الوثيقة من مادة بلاستيكية صلبة سمكها 0،85 مليمتر من لون "أخضر" داكن بالنسبة لجواز السفر العادي، و"أحمر" بالنسبة لجواز السفر الدبلوماسي، "أزرق" بالنسبة لجواز السفر المصلحة ومن خلال رغبة المشروع في تلوين جواز السفر إلى ثلاثة ألوان بغية تحديد جواز السفر أي كل لون مشهور بصاحبه[2].

ب-من حيث الشكل الداخلي:

إن التطور الملحوظ عالميا وتطور التقنيات أراد المشرع الجزائري أن يكون جواز السفر أكثر فاعلية وقد أضاف تقنية الختم المضلل والشفاف وقد بينها كالتالي:

- تكون الصفحات الداخلية ذات صبغية عامة أصفر فاتح سمكها 105 مكرون تحتوي في الوسط وفي العمق على ختم الدولة، قطره 50 مليمترا، في شكل مضلل ومرئي من خلال الاستشفاف[3].

- إن التطور الحاصل على جواز السفر قد أضاف عدة تطورات منها كتابة الأرقام بالليزر ويكون جواز السفر البيومتري الالكتروني في شكل دفتر من 14 ورقة مزدوجة وترقم صفحاته من 3 إلى 28.[4]

تحتوي الصفحات من 3 إلى 28 على رقم جواز السفر مثقوبة بالليزر في أسفل الصفحة ولقد بين لنا المشرع الجزائري الاختلاف في الأوراق الخاصة بنوعية جواز السفر العادي والدبلوماسي والمصلحة أي لكل نوع لون ورق معين خاص به، وقد وضحت من قبل المشرع

[1]- المادة 02 من القرار المؤرخ في 2011/11/26، **يحدد المواصفات التقنية لجواز السفر البيومتري الالكتروني**، الجريدة الرسمية للجهورية الجزائرية الديمقراطية الشعبية، العدد 01، الصادر في 2012/01/14، ص 01.

[2]- المادة 03 المصدر نفسه، نفس الصفحة.

[3]- المادة 04 من المصدر نفسه، نفس الصفحة

[4]- المادة 06 من المصدر نفسه، نفس الصفحة.

كالتالي، تكون الأوراق الداخلية باللون الأخضر بالنسبة لجواز السفر العادي والرماني لجواز السفر الدبلوماسي، والأزرق بالنسبة لجواز سفر المصلحة، ويحتوي العمق الأمني المعالج بلونين اثنين[1]،

ولقد أضاف المشرع الجزائري مجموعة من الملاحظات التي تخص جواز السفر والتوصيات الخاصة بالمحافظة عليه وهي كالتالي[2]:

1-جواز السفر شخصي لا يمكن إعارته ولا يجوز إرساله عن طريق البريد.

2-يحتوي هذا الجهاز على شريحة الكترونية ذات حساسية بالغة، نوصي صاحبه بالحفاظ عليها، كل عطب يصيب الشريحة قد يجعلها غير صالحة للقراءة ويسبب إلغاء الوثيقة.

3-كل تزييف يعرض الوثيقة للإلغاء.

4-في حالة ضياع الجواز أو إصابته بعطب يجب على صاحبه إخطار السلطة الإدارية أو القنصلية المختصة فورا.

ثالثا: أنواع جواز السفر

لقد قسم المشرع الجزائري جواز السفر إلى ثلاثة أنواع، لكل منها صلاحياته والشخص المسموح له بحمله وكما أنه يجب عدم نسيان الوثيقة الخاصة بجواز السفر للحج إلى الأراضي المقدسة الإسلامية، لقد أقر المشرع الجزائري أنه من خلال الاتفاقيات المبرمة ما بين الجزائر وباقي الدول بخصوص جواز السفر في حال ما إذا أراد أحد المواطنين السفر إلى دولة أجنبية كما يجب أن يكون حاملا إحدى الوثائق التالية: أما جواز السفر العادي أو جواز السفر الاستعجالي أو جواز السفر الدبلوماسي أو جواز سفر المصلحة أو جواز السفر الخاص بالحج إلى البقاع المقدسة، وهذا ما سوف نتطرق إليه من خلال تعريف هذه الوثائق.

[1]- المادة 07 من القرار المؤرخ في 2011/11/26، **يحدد المواصفات التقنية لجواز السفر البيومتري الالكتروني**، الجريدة الرسمية للجهورية الجزائرية الديمقراطية الشعبية، المصدر السابق، ص 1.

[2]- المادة 08 المصدر نفسه، نفس الصفحة.

1-جواز السفر العادي:

هو عبارة عن وثيقة رسمية تصدرها جهة إدارة مختصة لإثبات هوية صاحبها وتسمح له بالفر والتنقل عبر الحدود، تقوم الإدارة المختصة بتسليمها لكل شخص يرغب في الحصول عليها على اعتبار أن حق الدخول إلى التراب الوطني والخروج منه حق مضمون[1]، وهو سند فردي يمنح بدون شرط السن لكل مواطن ما لم يكن محكوما عليه نهائيا في جناية ولم يرد اعتباره.

2-جواز السفر الاستعجالي:

يمنح هذا النوع والمقصود به جواز السفر الاستعجالي إلى المواطنين الجزائريين المقيمين في الخارج والمسجلين لدى مركز دبلوماسي أو قنصلي[2]، وهم غير حائزين على جواز سفر بيومتري الكتروني والذين يضطرون للتنقل لأسباب عائلية أو مهنية أو إدارية أو صحية إلى خارج بلد إقامتهم.وفي هذه الحالة يتقدم طالب جواز السفر الاستعجالي إلى السلطات المعنية ويعد ويسلم إلى المواطنين الجزائريين من طرف المراكز الدبلوماسية أو القنصلية للمواطنين الجزائريين المقيمين في الخارج.

وأيضا يستفيد من جواز السفر الاستعجالي المسجلين لدى مركز دبلوماسي أو قنصلي والمواطنين الجزائريين الحاصلين على إقامة مؤقتة في بلد غير بلد إقامتهم وضاع منهم جواز السفر أو أتلف أو سرق، والمضطرين إلى الالتحاق ببلد أجنبي أو أكثر قبل عودتهم إلى الجزائر، وفي هذه الحالة يعد ويسلم من طرف المراكز الدبلوماسية أو القنصلية[3]،

المواطنين الجزائريين المقيمين في الخارج والمسجلين لدى مركز دبلوماسي أو قنصلي الذين يوجدون في إقامة مؤقتة في الجزائر وضاع منهم جواز السفر أو أتلف أو سرق أو انقضت مدة صلاحيته، والجزائريين المضطرين للعودة إلى بلد إقامتهم، وفي هذه الحالة يعد ويسلم

---

[1]- المادة 55 من القانون رقم 16-01 المؤرخ في 2016/03/06، **المتضمن التعديل الدستوري**، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 14، الصادرة في2016/03/07، ص 13.

[2]- المرسوم التنفيذي رقم 16-58 المؤرخ في 2016/02/03**المتعلق بشروط إعداد وإصدار جواز السفر الاستعجالي**، الجريدة الرسميةللجمهورية الجزائرية الديمقراطية الشعبية، العدد 07، الصادر في 2016/02/07، ص19.

[3]- المصدر نفسه، نفس الصفحة.

من طرف المصالح المؤهلة للوزارة المكلفة بالشؤون الخارجية،ولقد ذكر المشرع أيضا الفئة التي تقيم في الجزائر ويضطرون إلى التنقل بسرعة إلى دولة أجنبية وهم غير حائزين على جواز السفر ومضطرين إلى التنقل خارج التراب الوطني، وفي هذه الحالة يسلم من طرف الوالي.[1]

3-جواز السفر الدبلوماسي:

هو وثيقة سفر شخصي، يصدر من مصالح وزارة الخارجية لفائدة مستخدميها العاملين بالخارج كالسفراء، والقناصل العاملين خارج الوطن، وكذا إطارات الدولة، والملحقين العسكريين ومساعديهم لدى البعثات الدبلوماسية بالخارج مدة مهمتهم[2]، كما تمنح لأزواجهم وأبنائهم القصر وبناتهم الغير متزوجات الذين يعيشون معهم تحت نفس السقف، ويمنح عند الاقتضاء لأبويهم الذين هما في كفالتهم وفقا للتنظيم المعمول به[3].

ولقد حدد المشرع الجزائري أن جواز السفر الدبلوماسي يسلم من قبل السلطات المختصة لوزارة الشؤون الخارجية، وكما أن له لون خاص يميزه عن باقي أنواع جواز السفر الأخرى، وهم اللون الأحمر.

4-جواز سفر المصلحة:

هو بمثابة وثيقة رسمية تمنح لموظفي الدولة أو أعضاء تقنيين وإداريين لغرض إتمام مصلحة معينة في إحدى الدول وكذا لإنجاز مهمة محددة ومثل هؤلاء لا يصنفون من الدبلوماسيين أو من الأشخاص المخول لهم حمل جواز السفر الدبلوماسي[4].

---

[1]- المرسوم التنفيذي رقم 16-58 المؤرخ في 2016/02/03،المتعلق بشروط إعداد وإصدار جواز السفر الاستعجالي، الجريدة الرسميةللجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق، ص 19.

[2]- المرسوم الرئاسي رقم 97-02 المؤرخ في 1997/01/04، **يحدد شروط منح وثائق السفر الرسمية التي تسلمها وزارة الشؤون الخارجية**، الجريدة الرسميةللجمهورية الجزائرية الديمقراطية الشعبية، العدد 01، الصادر في 1997/01/05.

[3]- المادة 02 من القانون رقم 14-03 المؤرخ في 2014/02/24، المتعلق بسندات ووثائق السفر، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق، ص03.

[4]- المادة 02 من المصدر نفسه، نفس الصفحة.

5-جواز السفر الخاص بالحج:

هو جواز سفر خاص يتم إصداره من طرف السلطة المختصة (الولاية، الدائرة) لفائدة الحجيج وهو صالح للاستعمال مرة واحدة ذهابا وإيابا إلى البقاع المقدسة بالمملكة العربية السعودية ولا يسلم في الواقع إلا لشخص واحد[1].

المطلب الثاني: مفهوم الشباك الالكتروني

في إطار السعي إلى عصرنة الإدارة بالانتقال التدريجي من مرحلة التسيير الكلاسيكي إلى مرحلة التسيير الآلي، تعمل وزارة الداخلية والجماعات المحلية والتهيئة العمرانية على إدخال التكنولوجيا الحديثة في مجالات التسيير والتنظيم، من أجل تحسين أداء المرفق العام بصفة مستمرة وإعادة الاعتبار له وكذا إحداث أنماط عمل جديدة وعصرية[2].

ولتجسيد ذلك على أرض الواقع،قامت وزارة الداخلية والجماعات المحلية والتهيئة العمرانية باتخاذ العديد من الإجراءات الهادفة للقضاء على البيروقراطية والتوجه نحو المعالجة الإلية للمعلومات لتحسين العلاقة بين الإدارة و المواطن[3].

وفي جملة هذه الإجراءات أحدثت وزارة الداخلية الشباك الالكتروني للوثائق البيومترية. لذا سنتكلم في هذا الفرع المطلب عن: تعريف الشبك الإلكتروني وذلك في الفرع الأول، أهدافه في الفرع الثاني، دور مقدم طلب الحصول على الوثيقة في الفرع الثالث، مهام الشباك الإلكتروني في الفرع الرابع، وذلك من خلال التالي:

الفرع الأول: تعريف الشباك الالكتروني

هو حل تقني يعمل على استقبال طلبات مختلف الوثائق البيومترية على مستوى البلديات، وتسجيلها بصفة أنية في قاعدة معطيات مركزية وهذا باستغلال الربط المباشر مع

---

[1]- المرسوم الرئاسي رقم 97-02 المؤرخ في 1997/01/04، يحدد شروط منح وثائق السفر الرسمية التي تسلمها وزارة الشؤون الخارجية،المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق.

[2] **www.interieur .gov.dz**، بتاريخ 2017/05/20، الساعة 10:00.

[3] - المرجع نفسه.

قواعد معطيات مركزية مثل قاعدة معطيات الوثائق البيومترية، السجل الوطني الآلي للحالة المدنية ومستقبلا قاعدة للمعطيات لرخص السياقة[1].

يرتكز عمل الشباك الالكتروني على مقاطعة ومقارنة قاعدة معطيات الوثائق البيومترية المنجزة سلفا مع معطيات السجل الوطني الآلي للحالة المدنية بصفة آلية، والتسامح بالتأكد بصفة أنية من صحة المعلومات الخاصة بطالب الوثيقة.

وقد تمت تجربة استغلال هذا النمط الحديث في التسيير ميدانيا على مستوى جميع بلديات ولاية الجزائر كمرحلة أولى ابتداء من 2017/12/13، وكمرحلة ثانية سوف يعمم بصفة تدريجية على جميع بلديات الوطن[2]

الفرع الثاني: أهداف إنشاء الشباك الالكتروني

سيتم بفضل هذا الانجاز تحقيق عدة أهداف منها[3]:

1-تحسين ظروف الاستقبال والعلاقة بين الإدارة والمواطن.

2-فتح المجال للولوج التدريجي إلى عالم الإدارة الالكترونية.

3-السرعة في دراسة ومراقبة ومعالجة الملفات.

4-إعفاء المواطن من تقديم الوثائق الموجودة بياناتها في قاعد المعطيات ما لم يتم تغييرها، بما في ذلك ملخص شهادة الميلاد الخاص EC12S.

5-إعفاء المواطن في الملأ اليدوي لاستمارة طلب الوثائق البيومترية.

6-إلغاء عملية أخذ البيانات للمواطنين الحائزين سلفا على الوثائق البيومترية ماعدا في حالات الضرورة التقنية أو التنظيمية.

---

[1] www.interieur .gov.dz، المرجع السابق.

[2] - الو جع نفسه.

[3] - المنشور الوزاري رقم 02، المؤرخ في 21 مارس 2018، المتضمن تأطير مسار الشباك الالكتروني الخاص بالوثائق البيومترية وطرق استغلاله، المصدر السابق ، ص03

7-تخليص الأخطاء الناتجة عن العجز لأن الحل يعتمد على الاطلاع المباشر على البيانات الموجودة في قواعد المعطيات المركزية.

الفرع الثالث: دور مقدم طلب الحصول على الوثيقة

سنتحدث في هذا الفرع عما يجب على مقدم الوثيقة القيام به، ثم الوثائق المكونة للملف وذلك كالتالي:

أولا: ما يجب على مقدم الوثيقة القيام به

على مقدم طلب حصول الوثيقة البيومترية أن يقوم بما يلي:[1]

1-تقديم ملف الطلب حسب نوع الوثيقة.

2-الحضور الشخصي إلزامي لطالب الوثيقة أو الولي الشرعي بالنسبة للبالغين سن 12 سنة فما فوق عند إيداع واستلام الوثيقة.

3-أما فيها بما يتعلق بالأطفال القصر، (أقل من 12سنة) فحضورهم إجباري عند الإيداع فقط.

ثانيا-الوثائق المكونة للملف:

يتكون ملف طلب الوثائق "بطاقة التعريف الوطنية وجواز السفر البيومتريين" من:[2]

-صورتين شمسيتين للهوية لألوان، حديثتين ومتماثلتين بخلفية موحدة بيضاء وبدون إطار.

-شهادة الإقامة، في حالة عدم امتلاك المعني لوثيقة بيومترية أو تغييره لمكان الإقامة، مع العلم أن القصر ما دون 19 سنة معفون من تقديم شهادة الإقامة.

- شهادة الجنسية، في حالة عدم امتلاك أي وثيقة بيومترية مسبقا.

[1]- المنشور الوزاري رقم 02، المؤرخ في 21 مارس 2018، المتضمن تأطير مسار الشباك الالكتروني الخاص بالوثائق البيومترية وطرق استغلاله، المصدر السابق، ص03.

[2]- المصدر نفسه، نفس الصفحة.

_ فصيلة الدم، في حالة عدم وجودها في قاعدة المعطيات.

_ شهادة العمل أو شهادة عدم العمل أو شهادة مدرسية، في حالة عدم وجودها في قاعدة المعطيات، بالنسبة لطالبي جواز السفر فقط.

- قسيمة أو طابع جبائي بمبلغ يتناسب ونوع الوثيقة.

الفرع الرابع:مهام الشباك الإلكتروني:

سنتكلم عن مهام الشبك الإلكتروني من خلال التطرق إلى مهام كل من: العون المكلف باستلام الملف وفحصه، العون المكلف بأخذ البيانات البيومترية، المسؤول التقني عن الأرضية البيومترية، رئيس المصلحة، العون المكلف بتسليم الوثائق البيومترية، مديرية السندات والوثائق المؤمنة، التحديات الجديدة المضافة للشباك الإلكتروني، وذلك من خلال الآتي:

أولا-مهام العون المكلف باستلام الملف وفحصه: تتمثل مهامه في الآتي[1]:

1-التأكد من الوثائق المكونة للملف الإداري لصاحب الطلب حسب الحالة.

2-التأكد من مطابقة صورة الهوية المقدمة للمعايير المعمول بها.

3-تحديد نوع الوثيقة المطلوبة في نظام الشباك الالكتروني.

4-البحث عن المعلومات الخاصة بالشخص في السجلالوطني الآلي للحالة المدنية، وذلك بحجز البيانات الخاصة بالشخص رقم التعريف الوطني الوحيد، أو رقم الوثيقة البيومترية.

5-التأكد من معلومات الشخص (بيانات الهوية والصورة إن وجدت).

6-حجز المعلومات الناقصة في حالة عدم وجودها، أو تغييرها في حالة حصول الشخص على وثيقة بيومترية أخرى من قبل.

7-التأكد من جميع البيانات قبل تسجيل الطلب.

[1]- المنشور الوزاري رقم 02، المؤرخ في 21 مارس 2018،المتضمن تأطير مسار الشباك الالكتروني الخاص بالوثائق البيومترية وطرق استغلاله، المصدر السابق، ص04.

8-التأكد من تناسب مبلغ القسيمة الجبائية من نوع الطلب ونوع الوثيقة، وذلك بمقارنته مع المبلغ المحسوب أليا في نظام الشباك الالكتروني.

9-تسجيل طلب الوثيقة البيومترية، الذي يرفق أليا برقم تسلسلي للملف.

10-طباعة استمارة الطلب وتقديمها للمعني بالأمر ليتأكد من المعلومات المسجلة.

11-التأكدمن كتابة اسم ولقب المعني بالأمر وا ٍمضائه على الاستمارة.

12-المسح الضوئي لصورة المعني بالأمر مع احترام المقاييس والجودة.

13-تثبيت الطلب وتقديم وصل إيداع للمعني في حالة عدم أخذ البيانات البيومترية.

ثانيا: مهام العون المكلف بأخذ البيانات البيومترية: يقوم العون المكلف بأخذ البيانات البيومترية بما يأتي:[1]

1-البحث عن الملف باستعمال الرقم التسلسلي للملف.

2-عرض المعلومات الشخصية عبر الشاشة لصاحب الطلب، أو قراءتها له في حالة عدم تمكنه من القراءة.

3-المصادقة على الصورة الملتقطة بالماسح الضوئي من طرف العون المكلف باستلام الملف ومقارنتها مع الشخص مقدم الطلب لأخذ البيانات البيومترية.

4-التأكد من علامات الخصوصية وحالة الأصابع.

5-إمكانية إعادة الملف للتصحيح في حالة اكتشاف خطأ، أو التدقيق في حالة كون الصورة الممسوحة غير مطابقة للمعايير المعمول بها.

6-أخذ بصمات مع الحرص على أن تكون ذات جودة عالية (يمنع منعا باتا وضع أصابع العون على الماسح الضوئي للبصمات عند عملية الالتقاط).

[1]- المنشور الوزاري رقم 02، المؤرخ في 21 مارس 2018، المتضمن تأطير مسار الشباك الالكتروني الخاص بالوثائق البيومترية وطرق استغلاله، المصدر السابق ، ص05.

7-إزالة أثار البصمات من الجهاز مسح البصمات بعد كل عملية التقاط.

8-التقاط الصور والتي تكون وجوبا مطابقة للمعايير التقنية المعمول بها.

9-أخذ الإمضاء الرقمي لصاحب الطلب أو الولي الشرعي حسب الحالة.

10-بعد أخذ البيانات البيومترية تتم أليا عملية تشفير المعلومات، ثم يقدم العون وصل إيداع الطلب للمعني.

ثالثا: مهام المسؤول التقني عن الأرضية البيومترية: نذكر مهامه في التالي:[1]

1-الحرص على ضمان استمرارية عمل الأرضية البيومترية من الناحية التقنية بصفة دائمة.

2-تسيير حسابات المستعملين.

3-تثبيت التطبيقات المستعملة في الأرضية البيومتريةوكذا التحديثات مباشرة بعد استلامها.

4-إدارة الأنظمة وقاعدة البيانات.

5-القيام بعملية حفظ قاعدة البيانات وملف الصدور يوميا.

6-حلالمشاكل التقنية بسرعة وا ذا تعذر ذلك يتصل مباشرة بالخلية التقنية الموجودة على مستوى الولاية.

7-تكوين المستخدمين على استعمال الحلول التقنية.

8-تقديم الاقتراحات التقنية والملاحظات.

رابعا: مهام رئيس المصلحة: تتمثل في الآتي[2]:

1-معاينة وضعية الطلبات على المستويين المحلي والمركزي.

---

[1]-المنشور الوزاري رقم 02، المؤرخ في 21 مارس 2018،المتضمن تأطير مسار الشباك الالكتروني الخاص بالوثائق البيومترية وطرق استغلاله، المصدر السابق ، ص ص 05-06.

[2]- المصدر نفسه، ص 06.

2-معاينة المعلومات المحجوزة وتصحيحها في حالة وجود خطأ حتى بعد تثبيت الطلب.

3-تحميل الملفات المرفوضة مؤقتا من مركز الإنتاج والتي تستلزم تأكيدا أو تصحيحا أو تغييرا في البيانات البيومترية، بما فيها المرفوضة مؤقتا بعد معاينة صحيفة السوابق العدلية.

4-إعلام المعني بالأمر بالرفض المؤقت والقيام بالإجراءات المرتبطة بكل حالة رفض مؤقت.

5-تأكيد وتثبيت طلبات الإجراء السريع بعد معاينة القسيمة الجبائية المرفقة في الملف.

6-الاطلاع على الإحصائيات الخاصة بطلبات الوثائق البيومترية وطباعتها لاستغلالها عند الحاجة.

في حالة رفض الملفات المرفوضة مؤقتا بعد معاينة صحيفة السوابق العدلية فعليه أن يقوم ب:

1-تحويل الملفات إلى السلطة المخولة (الوالي أو الوالي المنتدب أو رئيس الدائرة) لإبداء الرأي النهائي.

2-تبليغ المعني وإعلامه بأي وسيلة من الوسائل المتاحة بحقه في طلب إعادة النظر في ملفه.

3-حجز الرأي النهائي للسلطة المخولة (الوالي، الوالي المنتدب، رئيس الدائرة).

خامسا: مهام العون المكلف بتسليم الوثائق البيومترية: تتمثل بدوره مهامه في الآتي[1]:

1-سجيل الوثائق المستلمة من مصالح الولاية أو المقاطعة الإدارية أو الدائرة.

2-تسليم الوثائق البيومترية لأصحابها بعد قراءة الشريحة ومقارنة البصمات.

3-تسليم أظرفة الرقم السري.

[1]- المنشور الوزاري رقم 02،المؤرخ في 21 مارس 2018، المتضمن تأطير مسار الشباك الالكتروني الخاص بالوثائق البيومترية و طرق استغلاله، المصدر السابق، ص 06.

4-تحويل الوثائق التي تعذرت فيها عملية مقارنة البصمات بسبب رداءتها إلى رئيس المصلحة للبت فيها.

5-إعادة الوثائق التي تحتوي على أخطاء أو عيوب مادية إلى مركز الإنتاج عن طريق السلم الإداري.

6-طباعةوصل الإعادة وا ٍرفاقه مع الوثيقة.

سادسا: مهام مديرية السندات والوثائق المؤمنة.

يتم إنتاج الوثائق البيومترية (جواز السفر وبطاقة التعريف الوطنية) بمقر مديرية السندات والوثائق المؤمنة بعد مرورها بعدة مراحل، ابتداء من إيداع الملف من طرف المواطن على مستوى البلدية أو الملحقة البلدية أو المقاطعة الإدارية أو الدائرة إلى غاية استلامه الوثيقة المطلوبة، وذلك كما يأتي:[1]

1-تحويلالملفات المسجلة الكترونيا عبر الشبكة الخاصة بوز ارة الداخلية والجماعات المحلية والتهيئة العمرانية.

2-القيام بعملية التأكد من الهوية ألياوذلك من خلال مقارنة الرقم التعريفي الوطني وكذا مقارنة البصمات.

3-مراقبة البيانات البيومترية (الصورة والبصمة والإمضاء) من أجل التأكد من مدى مطابقتها للمعايير المطلوبة، وفي حالة عدم مطابقتها ترفض مؤقتا ويشعر موقع أخذ البيانات البيومترية الكترونيا والمواطن عبر رسالة نصية لإعادة التقاطها أو تحميلها.

4-معاينة صحيفة السوابق العدلية على مستوى المديرية لطالب جواز السفر البيومتري، ليتم بعد ذلك الموافقة على انجازه أو وضعه بصفة مؤقتة قيد الدراسة من طرف السلطة المصدرة.

[1]-المنشور الوزاري رقم 02، المؤرخ في 21 مارس 2018،المتضمن تأطير مسار الشباك الالكتروني الخاص بالوثائق البيومترية وطرق استغلاله، المصدر السابق، ص 07.

5-تحويل الملف المستوفي للشروط التنظيمية والتقنية إلى ورشة الإنتاج من أجل طباعة الوثيقة المطلوبة.

6-مراقبة كل وثيقة منتجة للتأكد من سلامتها وخلوها من كل عيب مادي أو مطبعي.

7-وضعالوثائق المنتجة والتي تمت مراقبتها في أظر فة خاصة مع جداول إرسال باسم كل ولاية ومقاطعة إدارية ودائرة وبلدية.

8-تتولى مصلحة خاصة عملية تسليم الوثائق البيومترية إلى العون المؤهل الخاص بكل ولاية بعد إحصائها و الإمضاء على جداول الإرسال الخاصة بها، تتكفل المقاطعات الإدارية بالنسبة لولاية الجزائر بهذه العملية.

9-توجيه كل الإشكاليات المحتملة ذات الطابع التنظيمي إلى المديرية العامة للحريات العامة والشؤون القانونية للاختصاص.

10-موافقة المديرية العامة للحريات العامة والشؤون القانونية بطريقة الكترونية بالإحصائيات المختلفة بصفة دورية بتحليلها واستغلالها.

سابعا: التحديثات الجديدة المضافة إلى الشباك الالكتروني.

بالإضافة لما يحمله الشباك الالكتروني من مزايا، أضيفت له عدة تحديثات تهدف إلى تحسين آليات عمله والاستجابة إلى مقترحات مستخدميه،حيث[1]:

1-تم إضافة **"دور عون الاستقبال"** والذي تتمثل مهمته في:

- معاينة حالة طلبات الوثائق البيومترية للمواطنين الذين يقصدون المصلحة من أجل الاستفسار عن طلباتهم.

- يقوم عون الاستقبال بتوجيه المواطنين إلى الشباك المناسب حسب كل حالة وهذا من أجل تفادي الفوضى والتنقل العشوائي للمواطنين داخل مختلف المكاتب.

[1]- المنشور الوزاري رقم 06، المؤرخ في 05 نوفمبر 2018، المتضمن الترتيبات التنظيمية المؤطرة للتحديثات المضافة للشباك الالكتروني لاسيما المتعلقة بإصدار رخصة السياقة البيومترية الالكترونية، المصدر السابق، ص 05-06.

2-تم إضافة دور **"المراقب"** وجاء استجابة لاقتراحات بعض الولايات، يوفر هذا الدور لمستخدميه ما يلي:

- الاطلاع على كل الإحصائيات الخاصة بالملفات الالكترونية المعالجة لمراقبة السير الحسن للمصلحة.

- الاطلاع على مراحل معالجة طلبات المواطنين.

3-إضافة إلى معالجة الفئتين السابق ذكرهما في هذه المرحلة، تم الأخذ بعين الاعتبار إمكانية معالجة حالات تجديد رخصة السياقة البيومترية الالكترونية والتي تشمل الضياع، الإتلاف، السرقة وكذا حالة إضافة صنف جديد إلى رخصة السياقة البيومترية الالكترونية.

4-تم وضع آلية من أجل تحديد مدى صلاحية الصور الفوتوغرافية المأخوذة سابقا والمطبوعة على الوثائق البيومترية بالنسبة إلى أعمار أصحابها الحالية وبالتالي توجيه عون التدقيق، في حالة قدم الصورة، إلى مسح صورة جديدة حديثة للمعني توافق هيئته الفسيولوجية الحالية.

الفصل الأول:

الحماية الجنائية الموضوعية للوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية في الجزائر

كانت الجريمة المعلوماتية تندرج ضمن الجرائم التقليدية مثل السرقة، الغش، والتزوير...، ولم تصبح جريمة قائمة بذاتها بمفهومها وأركانها الخاصة إلا بعد دخول الانترنيت في مطلع التسعينات، حيث ظهرت أنماط جديدة من الجرائم[1]،كجرائم الدخول والبقاء غير المصرح به، جريمة التلاعب بمعطيات الحاسوب، جريمة التعامل في معطيات غير مشروعة...، حيث أن القاضي الجنائي لم يعد يجد لها وصف ضمن قائمة الجرائم التقليدية، الأمر الذي أدى إلى وجوب وجود حماية جنائية لهذا النوع من الجرائم، لهذا سنتطرق في هذا الفصل إلى نطاق تطبيق هذه الحماية (المبحث الثاني) لكن أولا يجب التطرق إلى مفهوم الجريمة الالكترونية (المبحث الأول).

[1]- شرف الدين وردة، **الإثبات الجنائي بالأدلة الالكترونية (دراسة مقارنة)**، أطروحة لنيل شهادة الدكتوراه، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق، جامعة بسكرة، سنة 2017، ص87.

المبحث الأول:

مفهوم الجرائم الالكترونية المرتكبة على الوثائق البيومترية الالكترونية

تعتبر الجريمة المعلوماتية من الظواهر الحديثة وذلك لارتباطها بتكنولوجية حديثة هي تكنولوجيا المعلومات والاتصالات والكومبيوتر، وقد أحاطت بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لها، ولكن الفقه لم يتفق على تعريف محدد، بل أن البعض ذهب إلى ترجيح عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب الكتروني، فالجريمة الالكترونية هي صنف جديد من الجرائم[1]. وسنتكلم في هذا المبحث عن تعريف الجريمة المعلوماتية في المطلب الأول، ثم بيان خصائصها في المطلب الثاني.

المطلب الأول: تعريف الجريمة الالكترونية

تعددت اراء الباحثين القانونيين حول وضع تعريف موحد للجريمة الالكترونية يشمل جميع عناصرها الجوهرية، إذ لم يعد هناك وجود لحراس، بل أصبحت توجد حدود مفتوحة بلا حراسة وانتهى زمن ودور الجواسيس الدوليين الذين كانوا يتبادلون الحقائب والدراسات والصور السرية أو كانوا يقومون بنقل معلومات مهمة حيث أصبح يمكن نقل كل المعلومات الخطيرة والممنوعة من معلومات استخبارية أو خطط تخريبية، أو صور سرية، بشكل سهل جدا، من خلال ضغطة خفيفة على زر لوحة مفاتيح الحاسوب[2].

من أجل الوقوف على تعريف جامع مانع لهذا النوع الحديث من الجرائم حتى يسهل تحديد ماهيتها وعناصرها وكيفية التعامل معها ظهرت عدة تقسيمات وضعها البعض من الفقهاء للوصول إلى تعريف لها، فمنها من اعتمد على تقسيم التعريفات إلى تعاريف ضيقة للجرائم المعلوماتية، وأخرى تعاريف موسعة لها، و هناك تقسيم أخر للتعريفات يعتمد في الأساس على معايير قانونية محددة،إذ نجد تعاريف تعتمد على معيار قانوني واحد (كمحل الجريمة، وسيلة

[1]- خالد ممدوح إبراهيم، **أمن الجريمة الالكترونية، الدار الجامعية**، مصر، سنة 2008، ص41.

[2]- شرف الدين وردة، المرجع السابق، ص94.

الجريمة، شخصية مرتكب الجريمة) وهذا ما سنتكل عنه في الفرع الأول، وتعاريف تعتمد على تعدد المعايير وتشمل سرى على التعريفات التي تبرر موضوع الجريمة وأنماطها وبعض العناصر المتصلة باليات ارتكابها أو بيئة ارتكابها، أو سمات مرتكبها وهذا ما سنتكلم عليه في الفرع الثاني.[1]

الفرع الأول: طائفة التعريفات التي تقوم على معيار واحد

ترتكز هذه الطائفة على وضع تعريفات ترتكز على معيار قانوني، كتعريف الجريمة المعلوماتية بدلالة موضوع الجريمة أو السلوك محل التجريم أو الوسيلة المستخدمة وتشمل أيضا تعريفات قائمة على معيار شخصي (مدى توفر المعرفة والدراية التقنية لدى الشخص مرتكب الجريمة المعلوماتية).

أولا:التعريفات التي تستند إلى موضوع الجريمة

ذهب إليه الفقيه Rosblatبأنها:" كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الوالي والتي تحول طريقه".[2]

وفي رأي أخر عرفت على أنه: "أي نمط من أنماط الجرائم المعروف في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات".[3]

وعرفت أيضا بأنها: "الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمةوا إساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر".[4]

---

[1]- شرف الدين وردة، المرجع السابق، ص95.

[2]- محمد محمد شتا، **فكرة الحماية الجنائية لبرامج الحاسب**، دار الجناية الجديدة للنشر، مصر، 2001، ص73.

[3]- أمير فرج يوسف، **الجريمة الالكترونية والمعلومات والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنيت**، مكتبة الوفاء القانونية، مصر، الطبعة الأولى، 2011، ص10.

[4]- المرجع نفسه، نفس الصفحة.

ويلاحظ من خلال هذه التعريفات المختلفة لجرائم الكمبيوتر، أنها تتسم بالعمومية والاتساع، لأنها تدرج ضمن جرائم الكمبيوتر كل سلوك أو فعل أو نشاط غير مشروع أو ضار بالمجتمع،وقد سعى كذلك الأستاذ "Solarz" إلى حصر جرائم الكمبيوتر عندما اشترط أن يكون الفعل مما يقع ضمن نطاق قانون العقوبات،ويكون هنا قد جزم بشمول قانون العقوبات لأنماط السلوك الإجرامي في جرائم الكمبيوتر، رغم الجدل القائم حول مدى انطباق نصوص التجريم التقليدية على هذه الأفعال.[1]

ثانيا: التعريفات التي انطلقت من وسيلة ارتكاب الجريمة

ينطلق أصحابها من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة، حيث عرفت أيضا بأنها: "كافة أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي".[2]

وكذلك عرفت بأنها: "فعل إجرامي يستخدم الحاسوب في ارتكابه كأداة رئيسية"[3]. وعرفها "Merwe" بأنها: " الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي أو هي الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية، أو هي مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات"[4].

وقد وجه لهذه التعريفات انتقادات، منها الانتقاد الذي يرى بأن تعريف الجريمة يستدعي "الرجوع إلى العمل الأساسي المكون لها وليس فحسب إلى الوسائل المستخدمة لتحقيقه"، ويعزز هذا النقد بأنه "ليس لمجرد أن الحاسب قد استخدم في الجريمة، أن نعتبرها من الجرائم المعلوماتية".[5]

---

[1]- شرف الدين وردة، المرجع السابق، ص96.

[2]- أمير فرج يوسف، المرجع السابق، ص11.

[3]- عبد الصبور عبد القوي علي مصري، **الجريمة الالكترونية**، دار العلوم للنشر والتوزيع، مصر، الطبعة الأولى، 2008، ص22.

[4]- المرجع نفسه، ص22.

[5]- وردة شرف الدين، المرجع السابق، ص96.

ثالثا: تعريفات قائمة على معيار شخصي

جانب من الفقه والبعض من المؤسسات ذات الصلة بالموضوع، وضع عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل وهي تحديدا سمة الدراية والمعرفة التقنية، من هذه التعريفات، تعريف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام 1973، حيث عرفها بأنها: " أية جريمة لفاعلها معرفة فنية بتقنية الحاسب"[1]

وعرفت أيضا على أنها: "أية جريمة يكون متطلبا لاقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب".[2]

كما عرفت بأنها: "أي فعل غير مشروع تكون المعرفة بتقنية الكومبيوتر أساسية لارتكابه والتحقيق فيه وملاحقته قضائيا".[3]

وفي تقييم هذه التعريفات، يمكن القول أن المعرفة التقنية لدى المجرم المعلوماتي قد لا توفر بالضرورة، إذ أن التطور الذي شهدته وسائل التقنية نفسها أدى إلى تحويل الأجهزة المعقدة في الماضي إلى أجهزة سهلة الاستخدام حتى من قبل شخص لا يعرف شيئا في علوم الحاسوب، فلم يعد يستلزم مثلا العلم والمعرفة العميقين ليتمكن شخص من إرسال رسائل البريد الالكتروني دفعة واحدة إلى أحد المواقع لتعطيل عمله.[4]

الفرع الثاني: طائفة التعريفات القائمة على تعدد المعايير

وتشمل التعريفات التي تبرز موضوع الجريمة وأنماطها وبعض العناصر المتصلة بأليات ارتكابها أو بيئة ارتكابها أو سمات مرتكبها.

[1] -وردة شرف الدين، المرجع السابق، ص97.

[2] - المرجع نفسه، نفس الصفحة

[3] - المرجع نفسه، نفس الصفحة.

[4] - المرجع نفسه، نفس الصفحة.

أمام نقض التعريفات المركزة على معيار واحد، سواء القائمة على معيار قانوني موضوعي أو شخصي ظهرت مجموعة من التعريفات تعتمد على أكثر من معيار لبيان ماهية جريمة الكمبيوتر، فيعرفها الأستاذ Sheldon. J. Hecht بأنها : "واقعة تتضمن تقنية الحاسب ومجني عليه يتكبد أو يمكن أن يتكبد خسارة و فاعل يحصل عن عمد أو يمكنه الحصول على مكسب".[1]

وقريب من التعريف السابق تعرف بأنها: "أي فعل معتمد يرتبط بشكل أو بأخر بأجهزة الكمبيوتر، يتعرض أو يمكن أن يتعرض فيها الضحية للخسارة، ويكسب أو يمكن أن يكسب فيها الفاعل مكسب".[2]

ويلاحظ في هذين التعريفين، خاصة الأولى منها، أنه تعريف وصفي للجريمة لا تحديد لماهيتها عوضا على أنه يعتمد من بين المعايير المتعددة معيار تحقق أو احتمال تحقق خسارة،و لا يتسع هذا المعيار لحالات اختراق النظام والبقاء فيه دون أي مسلك أخر من شأنه تحقيق أو احتمال تحقق خسارة[3].

ومن الفقه الفرنسي يعرف الفقيه "Masse" جريمة الكمبيوتر (يستخدم اصطلاح الغش ألمعلوماتي) بأنها: "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح".[4]

وجرائم الكمبيوتر لدى هذا الفقيه جرائم ضد الأموال، وهو في هذا التعريف يستخدم معيارين: أو لهما الوسيلة (بواسطة المعلوماتية) والأصوب استعمال مصطلح (تقنية المعلومات) لأن العملية هي المعالجة الآلية للبيانات لا وسيلة تنفيذها، أما المعيار الثاني والمتمثل في معيار محل الجريمة و المتمثل بتحقيق الربح، أي الحصول على المال، فينتقد هذا الفقيه في

[1]- وردة شرف الدين، المرجع السابق، ص99.

[2]- المرجع نفسه، نفس الصفحة.

[3] المرجع نفسه، نفس الصفحة.

[4]- يونس عرب، **جرائم الكمبيوتر والانترنت**، الجزء الأول، منشورات اتحاد المصارف العربية، الطبعة الأولى، 2002، ص ص 78،79.

هذه النقطة لأن الاعتداء في كثير من جرائم الكمبيوتر ينصب على المعلومات في ذاتها دون السعي لتحقيق الربح ودونها أن تكون المعلومات مجسدة لأموال أو أصول، عوضا عن عدم صواب اعتبار المعلومات في ذاتها مالا ما لم يقر النظام القانوني هذا الحكم لها لدى سعيه لتوفي الحماية للمعلومات.[1]

المطلب الثاني: خصائص الجريمة الالكترونية

مثلما للجرائم العادية خصائص وصفات تتسم بها، فان الأمر ينطبق على جرائم تكنولوجيا المعلومات، وتعد الجرائم التي ترتكب من خلال الحاسوب وشبكة الانترنت هي جرائم ذات خصائص متفردة خاصة بها لا تتوفر في أي من الجرائم التقليدية في أسلوبها وطريقة ارتكابها،[2] لذا سنتكلم في الفرع الأول عن الطابع الدولي للجريمة المعلوماتي، وفي الفرع الثاني عن: صعوبة إثبات الجريمة المعلوماتية، وسنخصص الفرع الثالث للحديث عن: وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات. وفي الفرع الرابع سنتكلم عن أن الجريمة المعلوماتية جريمة مستحدثة.

الفرع الأول: الطابع الدولي للجريمة المعلوماتية.

الطابع العالمي لشبكة الانترنت وما يرتبه من جعل معظم دول العالم في حالة اتصال دائم على الخط online، يسهل من ارتكاب الجريمة من دولة إلى دولة أخرى، فالجريمة المعلوماتية لا تعترف بالحدود بين الدول والقارات ولذلك فهي تعتبر شكلا جديدا من أشكال الجر ائم العابر للحدود الإقليمية بين دول العالم كافة، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل : جرائم التعدي على قواعد البيانات،وتزوير وا ٍتلاف المستندات الالكترونية، والاحتيال المعلوماتي، وسرقة بطاقات الائتمان، والقرصنة، وغسيل الأموال[3].

---

[1]- يونس عرب، المرجع السابق، ص 79.

[2]- جعفر حسن جاسم الطائي، **جرائم تكنولوجيا المعلومات**، رؤية جديدة للجريمة الحديثة، الطبعة الأولى، دار البلدية، عمان، 2007، ص140.

[3]ور دة شرف الدين، المرجع السابق، ص 101.

ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أصقاع الأرض، انعكست أيضا على طبيعة الأعمال الإجرامية التي يعتمد فيها المجرمون إلى استخدام هذه التقنيات في انتهاكاتهم للقانون، وهو ما يعني أن مساحة مسرح الجريمة المعلوماتية لم تعد محلية أي أنها أصبحت عالمية.[1]

والجريمة المعلوماتية أيضا هي من نوع الجرائم التي يتم ارتكابها عبر المسافات حيث لا يتواجد الفاعل على مسرح الجريمة بل يرتكب جريمة عن بعد وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز الكمبيوتر الفاعل وبين النتيجة أي المعطيات محل الاعتداء وبالتالي لا تقف الجريمة المعلوماتية عند الحدود الإقليمية لدولة معينة بل تمتد إلى الحدود الإقليمية لدولة أخرى مما يزيد من صعوبة اكتشافها.[2]

وهذا الأمر يشير أيضا إشكالية ثانية ذات صلة "بالتعارض مع سيادة الدولة" والتعارض مع سيادة الدولة قد يعقد من إمكانية القيام بعمل دولي مشترك للحد من جرائم تقنية المعلومات، بحيث يدفع بتلك الجهود إلى أن تتركز في الأطر القانونية لكل دولة على حدة[3].

الفرع الثاني: صعوبة إثبات الجريمة المعلوماتية

تتصف الجرائم المعلوماتية بالخفاء، أي عدم وجود أثار مادية يمكن متابعتها، وهي خطيرة، وصعبة الاكتشاف، أو هي صعبة في تحديد مكان وقوعها، أو مكان التعامل معها، بسبب اتساع نطاقها المكاني، وضخامة البيانات، ترجع صعوبة إثبات الجريمة المعلوماتية إلى عدة أمور منها:[4]

[1]- خالد ممدوح إبراهيم، المرجع السابق، ص44.

[2]- سوير سفيان، **جرائم المعلومات**، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الجرائم، جامعة أبو بكر بلقايد-تلمسان، كلية الحقوق والعلوم السياسية، 2010-2011، ص19.

[3] وردة شرف الدين، المرجع السابق، ص 101.

[4]- رصاص فتيحة، **الحماية الجنائية للمعلومات على شبكة الانترنت**، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبو بكر بلقايد-تلمسان، كلية الحقوق والعلوم السياسية، 2011-2012، ص45.

1-أنها لا تترك أي أثار مادية لها بعد ارتكابها، فهي جريمة تقع في بيئة الكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الالكترونية غير المرئية ولا توجد مستندات ورقية.

2-صعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية، إذ يستطيع المجرم المعلوماتي في أقل من ثانية أن يمحو أو يحرف أو يغير البيانات والمعلومات الموجودة في الكمبيوتر.

3-تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها، حيث تتطلب جرائم الكمبيوتر والانترنت إلمام خاص بتقنيات الكمبيوتر ونظام المعلومات سواء لارتكابها أو التحقيق فيها أو لملاحقتها قضائيا، لذلك يجد مأموري الضبط القضائي، أحيانا، أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذه النوعية من الجرائم فضلا عن صعوبة إجراءات التحري السري وتتبع مسار العمليات الالكترونية العابر للحدود.

4-تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها ومما يساعد في ازدياد عدم التعرف على مرتكبي الجرائم الالكترونية أحجام البنوك والشركات ومؤسسات الأعمال عن الإبلاغ عما يرتكب من جرائم معلوماتية قبلها تجنبا للإساءة إلى السمعة وهز ثقة العملاء فيها.

5-تعتمد على الذكاء في ارتكابها، فالجريمة المعلوماتية من النوع الذي يمكن أن نصفه بجرائم الذكاء، بالإضافة إلى أنها ليست جريمة منظمة في الغالب بل تتم على المستوى الفردي، وأهم دوافعها الطمع والجشع، والانتقام وأحيانا ترتكب بدافع إثبات الذات. وذلك أن الإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، كما أن المجرم المعلوماتي ذو مهارات تقنية عالية وا ٍلمام بتكنولوجيا النظم المعلوماتية.

الفرع الثالث: وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات

من خصائص الجريمة المعلوماتية أنها قع أثناء المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة المعلوماتية الخاصة بالتعدي على نظام معالجة البيانات، ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة المعلوماتية.

بالرغم في إمكانية ارتكاب الجرائم المعلوماتية أثناء أية مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات (الإدخال، المعالجة، الإخراج)، فان لكل مرحلة منها نوعية خاصة من الجرائم حيث:[1]

أولا: في مرحلة المداخلات

حيث تترجم المعلومات إلى لغة مفهومة من قبل الحاسب يسهل إدخال معلومات غير صحيحة وعدم إدخال وثائق أساسية وفي هذه المرحلة يرتكب الجانب الأكبر من الجرائم المعلوماتية.

ثانيا: في مرحلة المعالجة

يمكن إدخال أي تعديلات تحقق الهدف الإجرامي عن طريق التلاعب في برامج الحاسب، كدس تعليمات غير مصرح لها فيها، أو تشغيل برامج جديدة تلغي كليا أو جزئيا عمل البرامج الأصلية.

ثالثا:في المر حلة الأخيرة المتعلقة بالمخرجات

يقع التلاعب في النتائج التي يخرجها الحاسب بشأن بيانات ذلك أدخلت في معالجتها بطريقة صحيحة.

الفرع الرابع: الجريمة المعلوماتية جريمة مستحدثة

تعد الجرائم الالكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة، فلا غرابة أن تعتبر الجرائم المعلوماتية –سواء التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر تلك الأجهزة في ارتكابها-من الجرائم المستحدثة، حيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث

[1]- خالد ممدوح إبراهيم، المرجع السابق، ص49.

يتجاوز هذا التقدم بقدراته وا ٍمكاناته أجهزة الدولة الرقابية، بل أنه أضعف من قدراتها في تطبيق قوانينها، بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها.[1]

وعلى الرغم من المزايا والمنافع الايجابية المترتبة عن هذه العولمة وثورة المجتمع الالكتروني، إلا أنها ساعدت على ظهور وتعزيز أنواع جديدة من الجرائم، ومن أبرزها جرائم غسيل الأموال، وتهريب المخدرات واختراق قطاع الأعمال، و الإفلات بالتدليس والغش، والفساد ورشوة الموظفين العموميين، وسرقة الملكيات الفكرية، والاتجار غير المشروع في الأسلحة وفي السلاح والأطفال، والاتجار غير المشروع في الأعضاء البشرية، وسرقة المقتنيات الفنية والثقافية، والغش في التأمين، وجرائم الحاسب الآلي أو الجرائم الالكترونية.[2]

[1]- رصاص فتيحة، المرجع السابق، ص47.

[2]- خالد ممدوح إبراهيم، المرجع السابق، ص51، 52.

المبحث الثاني:

نطاق تطبيق الحماية الجنائية الموضوعية للوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية في الجزائر.

أدى التطور الحضاري الذي حققه الإنسان منذ منتصف القرن العشرين في مجالات الحياة المختلفة إلى دخول الإنسانية عصرا جديدا لم تألفه من قبل، بحيث انعكست نتائج استخدام تكنولوجيا المعلومات على لمجتمعات الحديثة، وأثرت تأثيرا كبيرا ليس فقط في سلوكات الإنسان، بل حتى في طريقة تفكيره من جهة، وطريقة عمله من جهة أخرى.[1]

وعلى الرغم من المزايا العظيمة الناتجة عن التطور العلمي الهائل، إلا أنه ترتب عليه مخاطر كثيرة ناجمة عن إساءة استخدام شبكة المعلومات واستعمالها لصالح المجرمين لممارسة أفعالهم الإجرامية، الشيء الذي استلزم سن نصوص قانونية تجرم هذه الأفعال، وسنتطرق في هذا المبحث إلى: الحماية الجنائية الموضوعية التقليدية للوثائق البيومترية الإلكترونية وذلك في المطلب الأول، ثم الحماية الجنائية الموضوعية الحديثة للوثائق البيومترية الإلكترونية في المطلب الثاني، من خلال ما يلي:

المطلب الأول: الحماية الجنائية الموضوعية التقليدية للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر

لم يكن هنالك قلق مع بداية شبكة المعلومات من جرائم يمكن أن ترتكب عليها أو بواسطتها، لا لأنها أمنة في تصميمها وبناءها، بل نظرا لحدود مستخدميها، علاوة على كونها مقصورة على فئة معينة من المستخدمين، إلا أنه ومع توسيع استخدامها ودخول جميع فئات المجتمع إلى قائمة مستخدميها، بدأت تظهر على الوجود ما يسمى بالجريمة المعلوماتية، نتيجة لهذا التطور في مجال المعلوماتية، أصبح لابد من توفير حماية جنائية لمكافحة أو التصدي لهذه الجرائم. وسنتكلم عن الحماية الجنائية الموضوعية للوثائق البيومترية من خلال التطرق

[1]- شرف الدين وردة، المرجع السابق، ص86.

لمدى خضوع الجرائم الواقعة على هذه الوثائق من خلال النصوص العقابية الموضو عية التقليدية لكل من جريمة التزوير (الفرع الأول)، جريمة الاتلاف (الفرع الثاني)، السرقة (الفرع الثالث).

الفرع الأول: الحماية الجنائية الموضوعية للوثائق البيومترية الإلكترونية من خلال تجريم التزوير

سنتناول في هذا الفرع جريمة من الجرائم التقليدية والمتمثلة في جريمة التزوير، من خلال تعريف التزوير التقليدي والالكتروني ومن ثم الوقوف على أركان جريمة التزوير.

أولا: تعريف جريمة التزوير التقليدية

يعرف التزوير في المجال القانوني على أنه: "عملية مادية وصورة من صور الكذب التي يقوم بها الشخص بغرض تغيير الحقيقة في محرر أو سند عمومي أو رسمي بإحدى الطرق المحددة في القانون، ومن شأنه إلحاق الضرر بالحقوق أو المراكز القانونية لأحد أو بعض أطراف السند أو المحرر محل الادعاء بالتزوير".[1]

كما يعرف بأنه: "تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط تحتج به يمكن أن ينتج عنه ضررا أدبيا أو ماديا أو اجتماعيا".[2]

ويعتبر التزوير " إظهار للكذب في محرز بمظهر الحقيقة وذلك غشا لعقيدة الغير".

[1]- حسام محمد نبيل الشنراقي، **الجريمة المعلوماتية** دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2003، ص233.

[2]- عباس حفصي، **جرائم التزوير الالكتروني** –دراسة مقارنة-أطروحة لنيل شهادة الدكتوراه، جامعة أحمد بن بلة، وهران 01، 2015، ص16.

من هذه التعريفات يتبين أن التزوير يرتبط بوجود محرر له قيمة في مجال الإثبات، وأن يقع تغيير للحقيقة فيه وهو الأساس الذي تقوم عليه جريمة التزوير، وذلك بنية الغش على نحو يوقع ضررا بالغير.[1]

ثانيا: تعريف جريمة التزوير الالكترونية

عرف الفقه التزوير الالكتروني بأنه: " تغيير الحقيقة في المستندات المعالجة أليا والمستندات المعلوماتية، وذلك بنية استعمالها، كما عرفه بأنه: "تغيير الحقيقة بأي وسيلة كانت سواء كان ذلك في محرر أو دعامة طالما أن هذه الدعامة ذات أثر في إنشاء حق، أو لها شأن في إحداث نتيجة معينة"[2].

كما عرف التزوير المعلوماتي بأنه: " تغيير الحقيقة في البيانات والمعلومات المعالجة عن طريق الحاسب الآلي والتي أصبح لها كين مادي ملموس يقابل أصل المحرر المكتوب"[3].

من خلال هذه التعريفات تبين أن التزوير المعلوماتي يرتبط بتغيير الحقيقة في وثيقة معلوماتي، وبالتالي هذه الوثيقة لا ترتبط بالشكل الورقي، فقد تكون دعامة معلوماتية حررت عليها معلومات لها قيمة قانونية، ولذلك فتغيير الحقيقية في هذه المعلومات يجب أن يظهر من خلال هذه الدعامة، والتي تتعدد أشكالها حسب ما تفرزه التكنولوجيا.

ثالثا: أركان جريمة التزوير

إن المساس بمحتوى الوثائق البيومترية الالكترونية وذلك عن طريق تزويره يكون أشد من تزوير وثيقة ورقية، ذلك لأن من يزور وثيقة بيومترية الكترونية لا يضر فحسب بالثقة العامة في الوثائق الرسمية لكنه يهدد بالضرر وكذلك مصلحة أخرى.

---

[1]- عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت**، دار الكتب القانونية، المجلة الكبرى، 2005، ص137.

[2]- حنان براهيمي، **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق، بسكرة، 2015، ص189.

[3]- عباس حفصي، المرجع السابق، ص18.

1- الركن الشرعي لجريمة التزوير

لا يعتبر تغيير الحقيقة تزويرا إلا إذا حصل بإحدى الطرق التي حددها القانون على سبيل الحصر في المادتين 214 و215 من قانون العقوبات وهي كالأتي:

تنص المادة "214" من قانون العقوبات على أنه: " يعاقب بالسجن المؤبد كل قاضي أو موظف أو قائم بوظيفة عمومية ارتكب تزويرا في المحررات العمومية أو الرسمية أثناء تأدية وظيفته:

- إما بوضع توقيعات مزورة.
- إما بإحداث تغيير في المحررات أو الخطوط أو التوقيعات.
- وا ٍما بانتحال شخصية الغير أو الحلول محلها.
- وا ٍما بالكتابة في السجلات أو غيرها من المحررات العمومية أو بالتغيير فيها بعد إتمامها أو قفلها"[1].

وجاء في نص المادة "215" من ق.ع الجزائري على أنه: "يعاقب بالسجن المؤبد كل قاض أو موظف أو قائم بوظيفة عمومية أقام أثناء تحريره محررات من أعمال وظيفة بترخيص جوهرها أو ظروفها بطريقة الغش وذلك بكتابة اتفاقات خلاف التي دونت أو أمليت من الأطراف أو بتقريره وقائع يعلم أنها كاذبة في صورة وقائع صحيحة أو بالشهادة كذبا بأن وقائع قد اعترف بها أو وقعت في حضوره أو بإسقاطه عمدا الإقرارات التي تلقاها"[2].

2- الركن المعنوي لجريمة التزوير:

تعتبر جريمة التزوير جريمة عمدية لا تقوم إلا بتوافر القصد الجنائي الذي يرتبط بأمرين:[3]

---

[1]- أمغار خديجة، **جريمة التزوير في محررات الرسمية (دراسة تحليلية مقارنة)**، مذكرة لنيل شهادة الماجستير، كلية الحقوق، جامعة الجزائر، 2014، ص 27.

[2]- المادة 215 من الامر رقم 156/66 المتعلق بقانون العقوبات من 724.

[3]- خيثر مسعود، **الحماية الجنائية لبرامج الكمبيوتر**، دار الهدى، الجزائر، 2010، ص138.

أ-العلم:

ويقصد به علم الجنائي بارتكاب الجريمة بجميع أركانها المكونة لها، فإذا تعلق الأمر بجريمة التزوير فان ذلك يعني علم الجاني وإدراكه بأنه يقوم بتغيير الحقيقة في وثيقة بإحدى الطرق المقررة قانونا تغييرا قد يلحق ضررا والمجتمع.

ب-الإرادة:

أي انصراف إرادة الجاني إلى تغيير الحقيقة في وثيقة بالطرق المقررة قانونا، وإلحاق الضرر بالغير أو احتمال حصول ذلك إذا استعملت الوثيقة المزورة فيما زورت من أجله.

3- الركن المادي لجريمة التزوير:

يشمل ما يقوم به الجاني من سلوك لتغيير الحقيقة في محرر بالطرق المنصوص عليها قانونيا، مما ترتب عليه ضررا بالغير، ويعني تغيير الحقيقة وإبدالها بما يخالفها، ويراد بذلك الحقيقة القانونية، وهي الحقيقة القانونية النسبية وليس الحقيقة الواقعية المطلقة، لأن تغيير الحقيقة في جريمة التزوير تعني أن يكون هناك مساس بحقوق الغير أو مراكزهم القانونية الثابتة في المحررات.[1]

وقد يكون التغيير كليا أو جزئيا، حيث تتعلق الصورة الأولى باصطناع وثيقة بأكملها مخالفة للحقيقة، أما الصورة الثانية فتتعلق بتغيير جزء من مضمون الوثيقة، أما إذا حصل التغيير عن طريق محو مضمون الوثيقة كلها أو إعدام قيمتها بحيث تصبح الكتابة غير مقروءة أو لا يمكن الاحتجاج بها فان ذلك يؤدي إلى قيام جريمة الإتلاف إذا توافرت أركانها.

وترتبط الوثيقة في جريمة التزوير تعتبر الكتابة التي ترتبط بالدعامة الورقية فالوعاء الذي تقع به جريمة التزوير ينصب على ورقة بالمفهوم المتعارف عليه.[2]

---

[1]- محمود نجيب حسني، **شرح قانون العقوبات**، القسم الخامس، دار النهضة العربية، مصر، ص ص198، 219.

[2]- فتوح الشاذلي، عفيفي كامل عفيفي، **جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون**، منشورات حلبي الحقوقية، لبنان، 2003، ص241.

ولا يمكن الاعتداء بالتزوير إلا إذا تم بالطر ق التي نص عليها القانون وهي على سبيل الحصر تتمثل في محو أو شطب أو إضافة كلمات، ووضع إمضاءات أو أختام مزورة، وضع أسماء وصور أشخاص آخرين مزورة، الاصطناع والتقليد.

كما قد يكون التزوير معنويا ويتم بطرق محصورا قانونا كتغيير إقرارات أولى الشأن، وجعل واقعة مزورة في صورة واقعة صحيحة.

رابعا: موقف المشرع الجزائري من مدى انطباق النصوص الموضوعية التقليدية لجريمة التزوير على الوثائق البيو مترية الالكترونية:

لم ينص المشرع الجزائري صراحة على جريمة التزوير الإلكتروني، وا ٍنما أشار لها عندما عرف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، في المادة 2-أ من قانون رقم 09-04 المؤرخ في 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على أنها: (جرائم المساس بأنظمة المساس المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية)[1] وبالتالي وفقا للمشرع الجزائري فان جريمة التزوير الإلكتروني هي جريمة التزوير التقليدية المنصوص عليها في قانون العقوبات كما سبق عرضه، على أن ترتكب جريمة التزوير أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

الفرع الثاني: الحماية الجنائية الموضوعية التقليدية للوثائق البيومترية من خلال تجريم الإتلاف:

عند تحقيق المجرم المعلوماتي لغايته باختراق النظام المعلوماتي أو البقاء فيه دون إذن يدفعه ذلك البقاء في غالب الأحيان إلى الاطلاع على المعطيات أو البيانات الموجودة داخل النظام، مما قد يدفعه في النهاية لإتلاف تلك البيانات أو المكونات المعنوية لنظام المعالجة

[1]- الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، الصادرة في 16 غشت 2009، ص 5.

الآلية للمعطيات، لهذا سنتطرق في هذا الفرع إلى تعريف جريمة الإتلاف التقليدية والالكترونية للتعرف على مدى انطباق النصوص المنظمة لها على إتلاف الوثائق البيومترية الالكترونية.

أو لا: تعريف جريمة الإتلاف التقليدي

تعني تخريب الشيء أو التقليل من قيمته يجعله غير صالح للاستعمال أو تعطيله، وقد يقصد بالإتلافإفناء مادة الشيء وهلاكه كليا أو جزئيا، أما التخريب فهو توقف الشيء تماما عن أداء منفعة كليا أو جزئيا دون إتلاف مادته، أما عدم الصلاحية للاستعمال فتعني جعل الشيء لا يقوم بوظيفته على النحو الأكمل، ويعني التعطيل توقف الشيء عن القيام بوظيفته فترة مؤقتة[1].

وقد يتحقق الإتلاف أو التخريب بوسائل مختلفة مادية أو معنوية سواء بالاعتداء على المعطيات والدعامة الموجودة عليها، أو محو المعطيات دون إصابة الدعامة أو تعطيل البرامج أو محوها باستخدام أداة لهذا الغرض.

ثانيا: تعريف جريمة الإتلاف الالكترونية

نصت العديد من التشريعات على جريمة إتلاف الوثائق البيومترية الالكترونية أو إتلاف البرامج والمعلومات المخزنة على الحاسب الآلي.

ويكون الإتلاف العمدي للبرامج والبيانات بمحوها كلية أو تدميرها الكترونيا، أو تشويهها على نحو يقع فيه الإتلاف بما يجعلها غير صالحة للاستعمال.[2]

[1]- أمال قارة، **الحماية الجزائي المعلوماتية في التشريع الجزائري**، الطبعة الأولى، دار هومة للنشر والتوزيع، الجزائر، 2006، ص106.

[2]- محمد أمين الشوابكة، **جرائم الحاسوب والانترنت، (الجريمة المعلوماتية)**، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2007، ص216.

وقد يتحقق الإتلاف أو التخريب بوسائل مختلفة مادية أو معنوية سواء بالاعتداء على المعطيات والدعامة الموجودة عليها، أو محو المعطيات دون إصابة الدعامة، أو تعطيل البرامج، أو محوها باستخدام أداة لغرض الغرض.[1]

وبالتالي يكون محل جريمة الإتلاف في نطاق الوثائق البيومترية الالكترونية هو كل من المكونات المادية والمتمثلة في الأجهزة كشاشات العرض وأجهزة الإدخال والإخراج والقرص الصلب...إضافة إلى المكونات المعنوية والمتمثلة في البرامج والبيانات والتي تحقق المعالجة الآلية للمعطيات شرط أن تكون ملكا للغير.[2]

ثالثا: أركان جريمة الإتلاف

1-الركن الشرعي:

تنص المادة 120 من قانون العقوبات الجزائري " يعاقب بالحبس من سنتين إلى عشر سنوات وبغرامة من 20000 إلى 100000 د.ج القاضي أو الموظف أو الضابط العمومي الذي يتلف أو يزيل بطريقة العبث وبنية الإضرار وثائق أو سندات أو عقود أو أموال منقولة كانت في عهدته هذه الصفة أو سلمت له بسبب وظيفته".

كما نص المشرع الجزائري على جريمة الإتلاف في المادة 407 من قانون العقوبات الجزائري على أنه: كل من خرب أو أتلف عمدا أموال الغير المنصوص عليها في المادة 396 بأية وسيلة أخرى كليا أو جزئيا يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 20000 إلى 100000 د.ج دون الإخلال بتطبيق أحكام المواد من "395" إلى "404" إذا تطلب الأمر ذلك.ويعاقب على الشروع في الجنحة المنصوص عليه في هذه المادة كالجنحة التامة[3].

[1]- براهيمي حنان، المرجع السابق، ص54.

[2]- طعباش أمين، **الحماية الجنائية للمعاملات الالكترونية**، مذكرة ماجستير في القانون، تخصص قانون دولي للأعمال، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2011، ص51.

[3]- عبد الفتاح بيومي حجازي، المرجع السابق، ص542.

2-الركن المادي لجريمة الإتلاف:

يتمثل الركن المادي لهذه الجريمة في الأفعال المادية التي يتكون منها السلوك المجرم، والذي يتمثل في التأثير في مادة الشيء، على نحو يذهب أو يقلل من قيمته الاقتصادية، عن طريق الإنقاص من كفاءته للاستعمال المعد له، فمثلا جهاز التلفاز قد يتم إتلافه عن طريق إدخال تيار كهربائي على الشدة فيتم حرق المكثفات داخل الجهاز، فبالرغم من أن الجهاز لم يتم تدميره كعنصر مادي، فهو محتفظ بهيكله وشكله ومكوناته المادية، إلا أنه يصبح غير صالح لما أعد له.[1]

وما يلاحظ أن فعل الإتلاف بصفة عامة له عدة صور، ومن الطبيعي أن يختلف مضمون وصور الإتلاف في قانون العقوبات على إتلاف البرامج والمعلومات، ويرجع ذلك الاختلاف إلى محل الجريمة، حيث يشترط أن يقع الإتلاف أو التعييب على مال منقول أو عقار، مملوك للغير.[2]

3-الركن المعنوي:

هذه الجريمة من الجرائم العمدية، يتطلب فيها توافر ركن معنوي يتمثل في القصد الجنائي العام بعنصريه العلم والإرادة، أي توجيه إرادة الجاني وهو مدرك كامل الإدراك إلى قيامه بالفعل، أي إلى الإزالة أو إتلاف الوثائق الموضوعة بحوزته أو تغيير مجرى الأموال المنقولة بغرض الأضرار لها، ويشترط أن يعلم الجاني أن المال الذي يقوم بإتلافه أو تعيبه مملوك للغير.[3]

---

[1]- عبد الفتاح بيومي حجازي، المرجع السابق، ص542.

[2] محمد أمين الرومي،**المستند الالكتروني**، الطبعة الأولى، دار الفكر الجامعي، مصر 2007، ص 92.

[3]- صالح شنين، **الحماية الجنائية للتجارة الالكترونية** دراسة مقارنة-، رسالة دكتوراه، كلية الحقوق، تلمسان، 2013، ص174.

رابعا: مدى انطباق النصوص الموضوعية التقليدية لجريمة الإتلاف على إتلاف الوثائق البيومترية الإلكترونية

بعض التشريعات العقابية التي لم تنص على جريمة الإتلاف الإلكتروني كما سبق تعريف هذه الجريمة، وانما حاولوا التوسيع في تطبيق النصوص العقابية التقليدية لجريمة التزوير على جريمة التزوير الإلكتروني منها تزوير الوثائق البيومترية الإلكترونية.

وعموما فقد اختلف الفقه بين مؤيد ومعارض لوقوع جريمة الإتلاف على المعلومات لذلك فان الإشكالية في هذا المقام تتمثل في مدى إمكانية تطبيق النصوص التقليدية التي تعاقب على أفعال الهدم والتخريب الواقعة على أملاك الدولة والأفراد على إتلاف المعلومات والبرامج المعلوماتية وبالتالي اتلاف الوثائق البيومترية الصادرة عن الجماعات المحلية؟

وللإجابة على هذه الإشكالية لابد من التطرق إلى الآراء المختلفة حول تحديد طبيعة المعلومات:

1-الرأي المؤيد لإمكانية تطبيق النصوص التقليدية لجريمة الإتلاف على الوثائق البيومترية الالكترونية:

إن المشكلة تكمن في وصف المال بأنه منقول وليس في الطبيعة المادية وغير المادية للنظام المعلوماتي بما تحتوي من معلومات وقواعد بيانات ونظم التشغيل اللازمة لها، وهذه الطبيعة المادية تمثل الجانب الأكبر من قيمة النظام كله، لذلك فان جوهر الإتلاف هو إفقاد صلاحية المال المتلف من الفرض المعد له، وهو ما يفقده قيمته الحقيقية[1].

إن البرامج والبيانات المنطقية هي مجموعة من المعلومات والأوامر لا يمكن الاستفادة منها إلا إذا وضعت في شيء مادي يمكن تعامله مع الجهاز، ومن هذا المنطلق ذهب البعض

[1]- محمد أمين الرومي، المرجع السابق، ص 93.

إلى اعتبار البرنامج الشيء مادي، وبالتالي إمكانية تطبيق النصوص التقليدية، كون الأسطوانة التي يوضع فيها، لها وجود مادي ملموس[1].

على ضوء ما تقدم، يمكن القول أنالبرنامج هو عبارة عن أوامر موضوعية بشكل منطقي، فلا يمكن الاستفادة منه إلا إذا وضع في شيء مادي، إلا أنه يجب الفصل بينه و بين الوسيط المادي، لأنه يمكن الدخول إلى البرنامج وا ٍتلاف المعلومات الموجودة بداخله دون المساس بالوسيط المادي[2].

2-الرأي المعارض لإمكانية تطبيق النصوص التقليدية لجريمة الإتلاف على الوثائق البيومترية الالكترونية:

اعتبر هذا الرأي أن المعلومات المبرمجة ألي كالنبضات الكهربائية، تفتقر إلى الطبيعة المادية، وأن هذه المعلومات ذات طبيعة معنوية، وهي تستقل من ناحية الأصل عن الوعاء المفرغة فيه من ناحية الشكل الخارجي، ولها ذات القيمة الاقتصادية للمال المادي، وبالتالي يتعين أن تخضع لأحكامه وتعامل تماما كما يعامل، فيعطيها الحماية والحقوق ذاتها، المقررة للمال المادي[3].

وقد أكد هذا الفقه على صعوبة تطبيق النصوص التقليدية من خلال القضية التي ظهرت في أسترالية، وكانت الأولى التي يتم فيها توجيه الاتهام باستخدام برنامج خبيث لإتلاف المعلومات، وتتلخص وقائع هذه القضية في قيام طالب بالدخول إلى الكمبيوتر في معهد سوين برن للعلوم التكنولوجية، وقيامه بإدخال برنامج تمهيدي يحتوي على فيروس مما ترتب على ذلك إتلاف جميع البيانات المسجلة على الأقراص الممغنطة، التي تم إدخالها إلى الكومبيوترات المتصلة بالنظام، فضلا عن إتلاف المكونات المادية، وقد قدم المتهم للمحاكمة بتهمتي الدخول غير المصرح به إلى النظام الكمبيوتر، و إتلاف ممتلكات الغير، إلا أن المحكمة برأته من التهمتين، كونه يملك حق الدخول باعتباره أحد طلاب المعهد، أما فيما يتعلق بإتلاف

[1]- محمد أمين الرومي، المرجع السابق، ص 93

[2]- المرجع نفسه، ص 94.

[3]- الصالح شنين، المرجع السابق، ص 176.

المعلومات محلا يمكن أن يقع عليه النشاط الإجرامي، وعلى الرغم من الخسائر، إلا أن عدم وجود نص تشريعي صريح يجرم فعله، أدى إلى تبرأته[1].

يمكن القول أن الرأي المعارض قد ميز بشكل واضح بين المعلومات كمنقول معنوي، وبين أدوات الكمبيوتر و آلاته التي تخضع للنصوص التقليدية، كونها شيئا ماديا بحتا، ومن هنا تظهر صعوبة تطبيق النصوص التقليدية[2].

بالإضافة إلى ذلك فان العقوبات التي تفرض لا توازي قيمة الضرر، فأضرار الشركات تقدر بالملايين، بل بالمليارات وبالتالي، فان النصوص التقليدية عاجزة عن المساواة بين الضرر وبين العقوبة، ومن هنا كانت الحاجة إلى تدخل المشرع لسد هذه الثغرات.[3]

3-موقف المشرع الجزائري:

لم ينص كذلكالمشرع الجزائري صراحة على جريمة الإتلاف الإلكتروني، وا ٍنما أشار لها عندما عرف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، في المادة 2-أ من قانون رقم 09-04 المؤرخ في 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السابق ذكره، على أنها: (جرائم المساس بأنظمة المساس المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية). وبالتالي وفقا للمشرع الجزائري فان جريمة الإتلاف الإلكتروني هي جريمة الإتلاف التقليدية المنصوص عليها في قانون العقوبات كما تم عرضه سابقا، على أن ترتكب جريمة الإتلاف أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

---

[1]- الصالح شنين، المرجع السابق، ص 177.

[2]- المرجع نفسه، نفس الصفحة.

[3]- ميساء مصطفى بركات، **جرائم التعدي على المعلوماتية (الإتلاف والتزوير)**، رسالة ماجستير، كلية الحقوق والعلوم السياسية، لبنان، 2009، ص27.

الفرع الثالث: الحماية الجنائية الموضوعية التقليدية للوثائق البيومترية الإلكترونية من خلال تجريم السرقة:

إذا كان الكيان المادي للمعلوماتية يخضع للنشاط الإجرامي لجرائم الأموال دون أي إشكال، لهذا سنجادل في هذا الفرع تعريف جريمة السرقة التقليدية ثم السرقة الإلكتروني، بيان أركان جريمة السرقة ثم دراسة مدى إمكانية خضوع سرقة الوثائق البيومترية الالكترونية للنشاط الإجرامي لجريمة السرقة ومدى تحقق الحماية الجزائية له وفقا لنصوص هذه الجريمة.

أولا: تعريف جريمة السرقة:

1- تعريف جريمة السرقة التقليدية:

السرقة هي أخذ مال الغير دون رضاه، فالسرقة تشكل جريمة اعتداء على مال الغير بإزالته من حيازة المالكوا إدخاله في حيازته دون وجه حق أو شرعي ودون علم أو رضا صاحب المال.

فالسرقة التقليدية إذن هي نزع المال من حيازة صاحبه دون رضاوعلمه وا إدخاله في حيازة السارق.[1]

2- تعريف جريمة السرقة الالكترونية:

هي أخذ نسخة من البيانات أو المعلومات أو برامج معينةوا إدخالها في حيازته لكن لم يخرج المعلومات من حيازة مالكها بل أبقاها في حياز ته، بناءا على هذا فإن السرقة بهذا المعنى تعارض تعريف السرقة المنصوص عليها في قانون العقوبات، وفي أن تكون البيانات أو البرامج محلا للسرقة لأنها أشياء غير محسوسة وغير مادية.[2]

[1] . https://M.facebook.com.posts بتاريخ 23 /2019/05،الساعة 11:42.

[2] - المرجع نفسه.

كمايمكن تعريف جريمة السرقة الالكترونية على أنها (استخدام الوسائط الحاسوبية وشبكات الانترنت لأخذ مال مملوك للغير بلغ نصابا، خفية من حرز مثله، من غير شبهة ولا تأويل).[1]

يستخلص من هذا التعريف أن السرقة في مجال المعاملات الالكترونية لا تستهدف الشريط الممغنط أو الأسطوانة أو الذاكرة أو الأسلاك التي تنقل الشارة لأن السارق لا يستهدف سرقتها للحصول على القيمة المادية بل يسرق ما هو مسجل عليه[2].

ثانيا: أركان جريمة السرقة

من خلال تعريف جريمة السرقة أنها اختلاس مال منقول مملوك الغير نية تملكه، يمكننا تقسيم جريمة السرقة إلى ركنين أساسيين هما:

1- الركن الشرعي لجريمة السرقة:

أ- عقوبة السرقة بوصفها جنحة:

- السرقة جنحة بسيطة: هي التي لا تكون مصحوبة بأي ظرف من ظروف التشديد المنصوص عليها في المواد "350" وما يليها.

* **العقوبة الأصلية:** المادة "350" من ق.عوالتي جاءفيها: "كل من اختلع شيئا غير مملوكا له يعد سارقا ويعاقب بالحبس من سنة إلى خمس سنوات وبغرامة 100000دج إلى 500000دج.

* **العقوبات التكميلية:** وجاءت بها نفس المادة وهي: "يجوز الحكم على الجاني بالحرمان من حق أو أكثر من الحقوق الواردة في المادة "09" مكرر لمدة سنة على الأقل وخمس سنوات على الأكثر وبالمنع من الإقامة طبقا للشروط المنصوص عليها في المادتين 12 و13 منق.ع[3].

[1]- ضياء مصطفى عثمان، **السرقة الالكترونية**، الطبعة الأولى، الأردن، ص211.

[2]- طعباش أمين، المرجع السابق، ص86.

[3]- **www.trubnaldg.com** ، بتاريخ 2019/05/23، على الساعة 10:47.

- السرقة جنحة مشددة:

نصت المادة "352" مكرر على أنه تكون عقوبة الحبس من سنتين إلى عشر سنوات أو الغرامة من 200000دج إلى 1000000دج في حالة ما ارتكبت السرقة مع استعمال العنف أو التهديد.

في حين نصت المادة "352" من ق.ع على أنه: "يعاقب بالحبس من خمس سنوات إلى عشر سنوات وبغرامة من 500000دج إلى غاية 1000000دج كل من ارتكب السرقة في الطرق العمومية أو في المركبات المستعملة لنقل المسافرين أو الأمتعة أو في داخل نطاق السكك الحديدة والمحطات والموانئ والمطارات وأرصفة الشحنوالتفريغ.[1]

ب) عقوبة السرقة بوصفها جناية:

تشكل جريمة السرقة جناية متى توافرت مجموعة من الظروف أو تزامنت مع وقت ارتكابها، فقد يكون حمل السلاح وقد يكون ظرف استثنائي وهي حالة الحريق، الثورة، الفتنة، تمرد أو في حالة تعدد الجناة، أو ظرف الليل.

- حالة أو ظرف حمل السلاح: وهو الظرف المنصوص والمعاقب عليه في المادة 351 من ق.ع.

- السرقة من شخصين أو أكثر: يعتبر ظرفا مشددا ويرجع ذلك إلى أن اجتماع عدة أشخاص يسهل من وقوع الجريمة من ناحية ويدل على الخطورةإجرام الجناة لوجود تخطيط وتصميم سابق على ارتكاب السرقة حيث أن المجني عليه يجد نفسه أمام مجموعة ن النصوص لا يستطيع فعل شيء أمامهم[2].

[1] www.trubnaldg.com، المرجع السابق.

[2] - المرجع نفسه.

2 -الركن المادي لجريمة السرقة:

إن البحث في مدى تحقق الركن المادي لجريمة السرقة في نطاق المعاملات الالكترونية هو مراعاة لمدى تحقق فعل الأخذ أو الاختلاس في هذه الجريمة، ويستوي فعل الاختلاس في أن يكون الجاني قد استولى على المال خلسة أو عنوة أو تسلمه بناءا على يد عارضة فغير نيته واستولى عليه، ومن ثم فان فعل الاختلاس يقتضي نقل حيازة المال موضوع الاختلاس أو السرقة من حيازة المجني عليه، إلى الجاني، بمعنى أن يظهر الجاني بوصفه صاحب السلطة والسيطرة الفعلية[1].

3-الركن المعنوي لجريمة السرقة:

يتخذ الركن المعنوي لجريمة السرقة في نطاق المعلوماتية صورة القصد الجنائي العام والخاص، ويتحقق القصد الجنائي العام، بتوافر العلم والإرادة.[2]

فيجب أن تتجه إرادة الجاني للاستيلاء على المعلومات المسجلة الكترونيا، والمخزنة على دعامة خارجية مثل الأسطوانات والشرائط الممغنطة، مع علمه بأنه المعلومات محل السرقة ملكا له، فإذا قام شخص بأخذ قرص ممغنط يحتوي على برامج معلوماتية واختلسه من صاحبه، ثم قام بتشغيله لمعرفة محتواه ثم رده فان إرادة الاختلاس تنتفي لديه ويختلف القصد العام عنده.[3]

ثالثا: مدى انطباق النصوص الموضوعية التقليدية لجريمة السرقة على سرقة الوثائق البيوميترية الإلكترونية

ولقد اختلف الفقهاء بخصوص فكرة السرقة المعلوماتية، فالرأي المؤيد لفكرة السرقة المعلوماتية يرى أن الركن المادي للسرقة المعلوماتية وهو فعل الاختلاس يتكون من عنصرين هما العنصر الموضوعي وهو النشاط أو السلوك الإرادي المؤيد إلى النتيجة مع وجود علاقة سببية بينهما، أما العنصر الأخر الشخصي هو نية الجاني في تملك الشيء وحيازته، حيث عند

[1]- طعباش أمين، المرجع السابق، ص87.

[2]- المرجع نفسه، ص160.

[3]- طعباش أمين، المرجع السابق، ص ص 99، 100.

تشغيل الحاسب الآلي والحصول على معلومات أو البيانات يكون قد اختلسها واستحوذ عليها بطريق غير مشروع.[1]

ولذلك أدانت محكمة (Grenoble) دائرة الجنح المستأنفة في 1995/02/15، عامل بتهمة السرقة كان قد أخرج من المؤسسة التي يعمل بها أوراقا سرية كان يقوم بتصويرها ثم يعيدها إلى المؤسسة[2].

أما الرأي المعارض فقد رأى عدم وجود إمكانية وقوع جريمة السرقة المعلوماتية لارتباط فعل الاختلاس بالمحل المادي للاختلاس في السرقة.

نلاحظ مما سبق أن التحجج بأن المال المعلوماتي غير قابل للسرقة، هي حجة تنافي المنطق ذلك أن التسليم بها يعني تجريد المال المعلوماتي من الحماية الجنائية مما يجعله عرضة للادعاء.

وبالتالي حفاظا على المصلحة العامة والخاصة ولكي لا يفلت المجرم من العقاب يجب تطبيق القواعد العامة التي تحكم جريمة السرقة، إلى أن يصدر تشريع خاص بها دون أن يكون في ذلك أي إخلال بالمبادئ العامة التي تحكم القانون الجنائي.[3]

وعن موقف المشرع الجزائري: لم ينص المشرع الجزائري صراحة على جريمة السرقة الإلكترونية، وا ٍنما أشار لها عندما عرف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، في المادة 2-أ من قانون رقم 09-04 المؤرخ في 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السابق ذكره، على أنها: (جرائم المساس بأنظمة المساس المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية) وبالتالي وفقا للمشرع الجزائري فان جريمة السرقة الإلكترونية هي جريمة السرقة

[1]- معتوق عبد اللطيف، **الإطار القانوني لمكافحة الجرائم المعلوماتية في التشريع الجزائري والتشريع المقارن**، مذكرة ماجستير في العلوم القانونية، تخصص قانون جنائي، جامعة باتنة، 2012، ص35.

[2]- محمد أمين الشوابكة، المرجع السابق، ص156.

[3]- المرجع نفسه، ص ص101، 102.

التقليدية المنصوص عليها في قانون العقوبات كما سبق عرضه، يضاف أن ترتكب جريمة السرقة أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

المطلب الثاني: الحماية الجنائية الموضوعية الحديثة للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر

نظرا لقصور الحماية الجنائية الجزائية الموضوعية للوثائق البيومترية الالكترونية بواسطة النصوص العامة التقليدية وبصفة خاصة نصوص جرائم الأموال وجرائم التزوير، لهذا ظهرت الحاجة إلى ضرورة سن نصوص عقابية موضوعية خاصة حديثة لمكافحة الجرائم الماسة بالوثائق البيومترية الالكترونية.

وفي هذا الشأن تدارك المشرع الجزائري خلال السنوات الأخيرة ولو نسبيا الفراغ القانوني في مجال الإجرام المعلوماتي عموما فلقد جرم المشرع الجزائري بعض الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات والتي تم إدراجها في القسم السابع مكرر من قانون العقوبات، هذه الجرائم محددة بموجب المواد 394 مكرر إلى 394 مكرر 07، وهذا ما سنتكلم عنه في الفرع الأول، كما أصدر قانون حماية المعطيات ذات الطابع الشخصي.

الفرع الأول: الحماية الجنائية الموضوعية الحديثة للوثائق البيومترية الالكترونية في إطار قانون العقوبات:

سنتناول في هذا الفرع جرائم المساس بأنظمة المعالجة الآلية للمعطيات من خلال التطرق أولا إلى جريمة الدخول أو البقاء غير المصرح به، ثم ثانيا لجريمة التلاعب بمعطيات الحاسب الآلي وثالثا وأخيرا إلى جريمة التعامل في معطيات غير مشروعة:

أولا: جريمة الدخول أو البقاء غير المصرح به

نص عليها المشرع الجزائري في قانون العقوبات من خلال نص المادة 394 مكرر في الفقرة الأولى منها، وسيتم تناول هاته الجريمة من خلال التطرق لأركانها المتمثلة في: الركن الشرعي، والركن المادي والركن المعنوي.

1-الركن الشرعي:

نصت المادة 394 مكرر يعاقب بالحبس من ثلاثة (03) أشهر إلى سنة (01) وبغرامة من 50000 د.ج إلى 200000د.ج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الالية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومةوا ٍذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (06) أشهر إلى سنتين (02) والغرامة من 50000 د.ج إلى 300000 د.ج.[1]

وبالتالي الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير مشروع بينما الصورة المشددة تتحقق بتوافر الظرف المشدد لها، ويكون في الحالة التي ينتج فيها عن الدخول أو البقاء الغير مشروع، إما محو أو تغيير المعطيات الموجودة في النظام أو التخريب لنظام اشتغال المنظومة.[2]

هناك جدل فقهي حول مدى تجريم فعلي "الدخول" و "البقاء" غير المصرح بهما في نظام معلوماتي، فالاتجاه الأول يرى أنه لا توجد ضرورة تستدعي تجريم مجرد لدخول أو البقاء غير المصرح بهما على النظام المعلوماتي، وخاصة إذا لم يكن لدى الفاعل نية لارتكاب جريمة لاحقة على هذا الدخول أو البقاء، ويبرز هذا الاتجاه رأيه أن هذا السلوك لا يخرج عن كونه طريقة لعرض القدرات التقنية أو الذهنية التي يتمتع بها الشخص الذي قام بهذا الفعل، وهذا الأمر لا يشكل بحد ذاته جريمة تستدعي معاقبة الفاعل[3].

[1]- القانون رقم 16-02، المؤرخ في 19 يونيو 2016، المعدل والمتمم للقانون رقم 66-156، المؤرخ في 08 يونيو 1966، **المتضمن قانون العقوبات**، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 37، الصادرة في في 22 يونيو 2016، ص 18.

[2]- أمال قارة، المرجع السابق، ص 107.

[3]- المرجع نفسه، ص108.

أما الاتجاه الثاني فيذهب إلى ضرورة تجريم الدخول والبقاء غير المصرح بهما إلى النظام المعلوماتي، حتى ولو لم يكن ذلك بقصد ارتكاب جريمة لاحقة فيما بعد[1].

فهذا الاتجاه يرى أن فعلي الدخول والبقاء غير المصرح بهما لهما تبعات مادية تتمثل في خسائر متعددة.

2- الركن المادي:

عالج المشرع الجزائري جريمة الدخول والبقاء غير المشروع في المادة 394 مكرر ق.ع.ج وعليه سوف نتطرق لفعل الدخول أولا ثم فعل البقاء.

أ- الدخول غير المصرح به:

تقوم هذه الجريمة بتحقق فعل الدخول إلى النظام المعلوماتي، ومدلول كلمة الدخول تشير إلى كل الأفعال التي تسمح بالولوج إلى نظام معلوماتي و الإحاطة أو السيطرة على المعطيات والمعلومات التي يتكون منها، وفعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه، بل يقصد به الدخول باستخدام الوسائل الفنية والتقنية إلى النظام المعلوماتي أي الدخول المعنوي أو الالكتروني، ويتساوى في هذا المجال إن تم الدخول بطريق مباشر إلى المعلومات أو تم عن طريق الاعتراض غير المشروع لعمليات الاتصال من أل الدخول إلى النظام المعلوماتي.[2]

ولا يعتبر فعل الدخول إلى النظام المعلوماتي بحد ذاته سلوكا غير مشروع، وا ٍنما ينفذ هذا الفعل وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق، أو بمعنى أخر دون تصريح.

لم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم بها الدخول إلى النظام لذلك تقع الجريمة بأي وسيلة أو طريقة، وذلك عن طريق كلمة السر الحقيقية متى كان الجاني غير

[1]- نهلا عبد القادر المومني، **الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع، الأردن، 2008، ص156.

[2]- نهلا عبد القادر المومني، المرجع السابق، ص158.

مخول في استخدامها، أو باستخدام برنامج أو شفرة خاصة، أو عن طريق استخدام الرقم الكودي لشخص أخر أو الدخول من خلال شخص مسموح له بالدخول.[1]

ب-فعل البقاء غير المصرح به:

وهو الفعل الثاني المنصوص عليه في المادة 394 مكرر من قانون العقوبات الجزائري، ويقصد به التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة صاحب ذلك النظام أو من له سيطرة عليه[2]، ويتحقق الركن المادي لجريمة البقاء غير المصرح به داخل النظام عن طريق الخطأ أو الصدفة إلا أنه يقرر البقاء داخل النظام وعدم قطع الاتصال، والبقاء المعاقب عليه قد يتحقق مستقلا عن الدخول إلى النظام وقد يجتمعان ويكون البقاء معاقب عليه استقلالا، حيث يكون الدخول إلى النظام المعلوماتي مشروعا.[3]

2-الركن المعنوي:

جريمة الدخول أو البقاء داخل النظام، جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي، والقصد الجنائي يتكون من علم وإرادة، فيلزم لكي يتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو البقاء، وأن يعلم الجاني أنه ليس له الحق في الدخول إلى النظام أو البقاء فيه.[4]

أ-القصد العام:

يتطلب القصد العام أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة، فكل ما يتطلبه القانون من وقائع لبناء أركان الجريمة، واستكمال عناصرها يتعين أن يشمله علم الجاني، ولكن علم الجاني لا يقتصر نطاقه على الوقائع التي تدخل في تكوين الجريمة، وانما يتعين أن يحيط أيضا بالتكييف الذي تتصف به بعض هذه الوقائع، وتكتسب به

[1]- خيثر مسعود، المرجع السابق، ص 115.

[2]- بومعيزة جابر، **الاعتداء على المعطيات الآلية في الحكومة الالكترونية**، مجلة البحوث الدراسات القانونية والسياسية، العدد الثاني عشر، كلية الحقوق والعلوم السياسية، جامعة البليدة 02، ص132.

[3]- طعباش أمين، المرجع سابق، ص38.

[4]- علي عبد القادر القهوجي، **الحماية الجنائية لبرامج الحاسب الالي**، دار الجامعة الجديدة، مصر، 2010، ص136.

أهميتها في نظر القانون، حيث أن عددا من الوقائع التي تقوم بها الجريمة لا تمثل أهمية في نظر القانون إلا إذا اكتسب وصفا معينا، فان تجر د من هذا الوصف، فقد تجرد من الأهمية القانونية ولم يعد صالحا لتقوم به الجريمة.[1]

ب-القصد الخاص:

هناك بعض النصوص الخاصة ببعض التشريعات المجرمة لفعل الدخول غير المصرح به، تتطلب قصدا خاصا إلى جانب القصد العام، كالقانون الدانمركي الذي يشدد العقوبة متى ارتكب فعل الدخول، بنية الإحاطة بمعلومات تتعلق بالأسرار المتعلقة بعمل إحدى الشركات، واستراليا التي تشدد العقوبة لكل من يقوم بفعل الدخول غير المصرح به إلى النظام المعلوماتي بنية الإضرار بالغير.[2]

والإشكالية التي تثور في هذا الصدد، متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء؟

يذهب رأي راجح من الفقه إلى أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام أو يستمر في التجول داخله بعد انتهاء الوقت المحدد، أي منذ علم الجاني أنه ليس له حق الدخول، فإذا دخل وظل ساكنا تظل الجريمة، جريمة الدخول إلى النظام، أما إذا بدأ في التجول فان جريمة البقاء داخل النظام تبدأ من تلك اللحظة لأنه يتجول في نظام يعلم مسبقا أن دخوله واستمراره فيه غير مشروع ومنذ تلك اللحظة تبدأ جريمة البقاء داخل النظام.[3]

ثانيا: جريمة التلاعب بمعطيات الحاسب الآلي

يطلق عليها أيضا اسم "جريمة المساس العمدي للمعطيات"، وهي الجريمة المنصوص عليها في المادة "394" مكرر من قانون العقوبات، وتتمثل هاته الجريمة في القيام بجملة من الأفعال

[1]- نائلة عادل محمد فريد قورة، **جرائم الحاسب الالي الاقتصادية –دراسة نظرية وتطبيقية-**، منشورات الحلبي الحقوقية، الأردن، 2005، ص365.

[2]- نائلة عادل محمد فريد قورة، المرجع السابق، ص ص 366، 367.

[3]- خثير مسعود، المرجع السابق، ص117.

التي تعتبر اعتداءات عمدية على المعطيات، وتتم هذه الاعتداءات باستعمال جملة من الوسائل وهذا ما سنبينه في الأتي:

1- الركن المادي:

تقوم جريمة التلاعب بمعطيات الحاسب الآلي المنصوص عليها في المادة "394" مكرر "01" من قانون العقوبات الجزائري، بإتيان إحدى السلوكات الثلاث الآتية: الإدخال، التعديل أو الإزالة.

أ- الإدخال:

يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها، سواء كانت خالية أم كان يوجد عليها معطيات من قبل، و يتحقق هذا الفعل في الغرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة التي يسحب بمقتضاها النقود من أجهزة السحب الآلي و ذلك حين يستخدم رقمه الخاص و السري للدخول، لكي يسحب مبلغا من النقود أكبر من المبلغ الموجود في حسابه، و كذلك الحامل الشرعي لبطاقة الائتمان و التي سدد عن طريقها مبلغا (للتاجر أو شخص يتعامل معه) أكثر من المبلغ المحدد له، وبصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب (فيروس، حصان طروادة، قنبلة معلوماتية زمنية) يضيف معطيات جديدة.[1]

كما يقصد به أيضا، إضافة معطيات جديدة على الدعامة الخاصة به، سواء كانت خيالية أو يوجد عليها معطيات من قبل، وهذه الجريمة تقع غالبا بمعرفة المسؤول عن القسم المعلوماتي والذي يسند إليه وظائف المحاسبة والمعاملات المالية، لأنه يكون في أفضل وضع يؤهله لارتكاب هذا النمط من التلاعب غير المشروع.[2]

[1]- علي عبد القادر القهوجي، المرجع السابق، ص 144.

[2]- أمال قارة، المرجع السابق، 120.

ب- الإزالة:

يقصد بفعل المحو، إزالة جزء من المعطيات المسجلة على دعامة والموجود داخل النظام أو تحطيم تلك الدعامة، أو نقل جزء من المعطيات من المنطقة الخاصة بالذاكرة.[1]

ج- التعديل:

يقصد بفعل التعديل تغير المعطيات الموجودة داخل نظام، و استبدالها بمعطيات أخرى، و يتحقق فعل المحو و التعديل، عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أ, جزئيا أو بتعديلها، و ذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات، أو برامج الفيروسات بصفة عامة، و هذه الأفعال المتمثلة في الإدخال، المحو و التعديل، وردت على سبيل الحصر، فلا يقع تحت طائلة التجريم أي فعل أخر غيرها، حتى لو تضمن اعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات، فلا يخضع لتلك الجريمة فعل نقل البيانات أو التنسيق أ, القريب بينها، لأن كل تلك الأفعال لا تنطوي على إدخال و إلا تعديل بالمعنى السابق.[2]

ما تجدر الإشارة إليه، أنه لا يشترط اجتماع هذه الصور الثلاث: الإدخال، التعديل، المحو، لقيام الركن المادي، بل يشترط تحقق النتيجة عن قيام إحدى هاته السلوكات غير المشروعة، والمتمثلة في تغير حالة المعطيات.

2- الركن المعنوي:

الركن المعنوي هو القصد الإجرامي، أي القيام بالفعل عن علم إرادة.

أ- القصد العام:

يتمثل القصد العام في جريمة التلاعب بمعطيات الحاسب الآلي، في كل من الإرادة والعلم يجب أن تتجه إرادة الجاني في هاته الجريمة، إلى ارتكاب إحدى السلوكات الإجر امية

[1]- عبد الفتاح بيومي حجازي، المرجع السابق، ص 365.

[2]- أمال قارة، المرجع سابق، 122

المذكورة سابقا، والمتمثلة في فعل الإدخال، فعل التعديل، فعل الإزالة، وتعد هذه الإرادة الإجرامية دليلا على خطورة شخصية الجاني، وتعد كذلك جوهر لركن المعنوي، هذا الأخير الذي يمثل ركن المسؤولية الجنائية فإذا انتفى الركن المعنوي كنا بصدد مانع من موانع المسؤولية[1].

أما العنصر الثاني من القصد العام والمتمثل في العلم، فانه في جريمة التلاعب بمعطيات الحاسب الآلي، يجب على الجاني أن يعلم بالسلوكات الإجرامية المتمثلة في الإدخال، التعديل، الإزالة.

ب- القصد الخاص:

يقصد بالقصد الخاص في الركن المعنوي لأي جريمة هو وجوب تحقق نتيجة تخرج عن الركن المادي، وفيما يخص جريمة التلاعب بمعطيات الحاسب الآلي، فالقصد الخاص بها لا يتطلب أي نتيجة تخرج عن الركن المادي.

- الإزالة والتعديل: سلوكات معنوية في الركن المعنوي.
- التغيير والحذف: سلوكات غير عمدية في الركن المعنوي.

فالفرق في السلوكات الإجرامية في جريمة الدخول والبقاء غير المصرح به، والسلوكات الإجرامية في جريمة التلاعب بمعطيات الحاسب الآلي، هو أن الأولى ظروف مشددة والأخرى سلوكات عادية.

وهنا تجدر الإشارة إلى أن الاختلاف بين عقوبة الجريمتين، جريمة الدخول والبقاء غير المصرح به وجريمة التلاعب بمعطيات الحاسب الآلي هو "عنصر العمد".

3- الركن الشرعي:

تنص المادة 394 مكرر 01 من قانون العقوبات الجزائري على ما يلي: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500000دج إلى 2000000دج، كل من أدخل

[1]- محمد عبيد الكعبي، المرجع السابق، ص 480.

بطريق الغش معطيات في نظام المعالجة الالية للمعطيات أو أزال أو عدل بطريق الغش، المعطيات التي يتضمنها[1].

فنلاحظ أن المشرع الجزائري قد حرم فعل التلاعب بمعطيات الحاسب الآلي، سواء كان ذلك عن طريق الإدخال، التعديل، أو الإزالة، والتي يترتب عنها تغيير في حالة المعطيات.

ثالثا: جريمة التعامل في معطيات غير مشروعة

تعد جريمة التعامل في معطيات غير مشروعة الصورة الثالثة من صور جرائم المساس بأنظمة المعالجة الآليةللمعطيات، و التي ينص عليها المشرع الجزائري في نص المادة 394 مكرر 02من قانون العقوبات الجزائري، و هي أيضا أحد الجرائم التي تمس عمدا في المعطيات المعلوماتية، وتختلف هذه الجريمة من حيث المعطيات، على أساس الحالة التي توجد عليها المعطيات محل الجريمة و النظم الذي توجد به هذه المعطيات.

1- الركن المادي:

بتحليل المادة 394 مكرر 02 من قانون العقوبات الجزائري، نستنتج أن "جريمة التعامل في معطيات غير مشروعة"، حسب المشرع الجزائري، يقوم سلوكها الإجرامي على صورتين:

الصورة الأولى الواردة في الفقرة الأولى من نص المادة 394 مكرر 02 من قانون العقوبات، و المتمثلة في القيام بأفعال: التصميم، البحث، التجميع، التوفير، النشر، الإتجار، ويكون محل هاته الأفعال: معطيات مخزنة/ معالجة أو مرسلة، وذلك عن طريق منظومة معلوماتية[2].

والصورة الثانية الواردة في الفقرة الثانية من نص المادة 394 مكرر 02 من قانون العقوبات، و المتمثلة في القيام بأفعال: الحيازة، الإفشاء، النشر أو الاستعمال و يكون محل هاته الأفعال المعطيات التي تم التحصل عليها من ارتكاب جريمة من جرائم المساس بأنظمة

[1]- المادة 394 مكرر 01 ، قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق.

[2]- المادة 02 من قانون رقم 09- 04 الصادر في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ، الجريدة الرسمية الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق.

المعالجة الآلية للمعطيات، سواء الدخول، أو البقاء غير المصرح به م294 مكرر أ، التلاعب بمعطيات الحاسب الآلي م394 مكرر01 أو... مهما كان الهدف من ذلك.

ما تجدر الإشارة إليه، أن الأفعال المذكورة في نص المادة 394 مكرر 0é من قانون العقوبات الجزائري: التصميم، البحث، التجميع، التوفير، النشر، الإتجار، الحيازة، الإفشاء، النشر، الإستعمال، هي أفعال مذكورة على سبيل الحصر لا المثال، و السلوك المجرم في الركن المادي لجريمة التعامل في معطيات غير مشروعة، يتمثل في فئتين من الأفعال:

- التعامل في معطيات صالحة لارتكاب جريمة التعامل بمعطيات غير مشروعة (م394 مكرر 02 فقرة 01).
- والتعامل في معطيات متحصل عليها من إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في م394 مكرر 02 فقرة 02 من قانون العقوبات[1].

2- الركن المعنوي:

فيما يخص الركن المعنوي لجريمة التعامل في معطيات غير مشروعة، فيتمثل في توافر القصد الجنائي العام دون القصد الجنائي الخاص، أي توافر النية الإجرامية المتمثلة في القيام بالأفعال المنصوص عليها في الفقرتين (1-2) النشر، الإتجار بمعطيات لاستعمالها في ارتكاب جرائم (بالنسبة للصورة الأولى المنصوص عليها في الفقرة الأولى من نص المادة 394 مكرر 03)، أو القيام بفعل الحيازة، الإفشاء، النشر، الإستعمال لمعطيات متحصل عليها من الجرائم المنصوص عليها في القسم السابع (بالنسبة للصورة الثانية المنصوص عليها في الفقرة الثانية من المادة 394 مكرر 02) و في كلتا الصورتين يجب أن يكون الجاني "عالما" بأنه يتعامل في معطيات غير مشروعة.

ما تجدر الإشارة إليه أن جريمة التعامل في معطيات غير مشروعة جريمة عمدية كباقي الجرائم التي سبق دراستها (جريمة الدخول والبقاء غير المصرح به، جريمة التلاعب بمعطيات

[1]- المادة 394 مكرر 02 ، قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق.

الحاسب الآلي)، فهي تعتمد على الغش، والغش يكمن في العلم بطبيعة هذه المعطيات وصفتها غير المشروعة ومع ذلك يقوم الجاني بالتعامل فيها.[1]

3- الركن الشرعي:

نصت المادة 394 مكرر 02 على ما يأتي: "يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000000دج إلى 5000000دج كل من يقوم عمدا وعن طرق الغش بما يأتي:

- حيازة أو إفشاء أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم[2].

- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان، للمعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم، والملاحظ من نص المادة أن هذه الجريمة تفرق بين الصورتين، تعامل في معطيات صالحة لارتكاب الجريمة والصورة الثانية معطيات محصلة من الجريمة المعلوماتية.

الفرع الثاني: الحماية الجنائية الموضوعية الحديثة للوثائق البيومترية الالكترونية في إطار قانون حماية المعطيات ذات الطابع الشخصي

أصدرت الجزائر القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[3]، من أجل سد فراغ تشريعي كبير في الجزائر يضفي الحماية القانونية اللازمة للحياة الشخصية للأفراد و منها المعطيات ذات الطابع الشخصي، وفي إطار مواصلة تحديث المنظومة التشريعية الوطنية مع المستجدات الحاصلة على المستوى

---

[1]- محمد خليفة، **الحماية الجنائية لمعطيات الحاسب الالي في القانون الجزائري والمقارن**، دار الجامعة الجديدة، مصر،2007، ص 218.

[2]- المادة 394 مكرر 02، قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق.

[3]- القانون رقم 18 -07 المؤرخ في 10 يونيو سنة 2018، **يتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي** الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 34، الصادرة في 10 يونيو سنة 2018، ص 12.

الدولي كما يمكن هذا القانون الجهات القضائية من صلاحيات واسعة للوصول إلى المعلومات الشخصية و بشكل أكبر في إطار عمليات التحقيق و المتابعة بشكل قانوني، لاسيما في ظل سياسة عصرنة العدالة التي تنتهجها الجزائر و لتلتحق الجزائر بركب أغلبية الدول التي سنت تشريعا خاصا بحماية المعطيات الشخصية بالنظر إلى خصوصيتها و حساسيتها.

إن الهدف من القانون رقم 18-07 هو تحديد قواعد حماية الأشخاص الطبيعيين ذات الطابع الشخصي في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألا تمس بحقوق الأشخاص و شرفهم و سمعتهم وهذا تماشيا مع مبادئ الدستور الجزائري الذي يكرس مبدأ احترام القانون الذي يشدد على أنه لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا ب "الموافقة الصريحة" للشخص المعني الذي يمكنه التراجع عن موافقته في أي وقت، كما استثنى هذا القانون حسب المادة "06" منه المعالجة من طرف شخص طبيعي لغايات لا تتجاوز الاستعمال الشخصي أو العائلي، بشرط عدم إحالتها للغير أ، نشرها، وكذا المعالجة لمصلحة الدفاع والأمن الوطنيين و أخيرا المعالجة لأغراض الوقاية من الجرائم ومتابعة مرتكبيها وقمعها.[1]

ومن هنا سنتناول في هذا الفرع كل من الإجراءات الإدارية والإجراءات الجزائية التي تناولها المشرع من خلال القانون رقم 18-07، والذي خصص لها الباب السادس والذي يشتمل على "29" مادة.

أولا: الإجراءات الإدارية

جعل المشرع كل من الإنذار، الإعذار، السحب المؤقت للرخصة أو السحب النهائي والغرامة جزاءات الإخلال بأحكام هذا القانون، تصدر هذه العقوبات السلطة الوطنية وتكون قراراتها قابلة للطعن أمام مجلس الدولة، كما تستطيع السلطة الوطنية فرض غرامة مالية قدرها

[1]- يوسف رزوق، **حماية المعطيات الشخصية في الجزائرية على ضوء القانون رقم 18،07**، مجلة معالم الدراسات القانونية والسياسية، العدد 05، ص 117.

500 ألف دينار جزائري مند كل مسؤولين المعالجة وقع في حالات معينة حددتها المادة (47) من ذات القانون كما يمكنها سحب وصل التصريح أو الترخيص ودون مراعاة منها لأي أجال.[1]

متى تعلق الأمر بالمساس بالأمن الوطني أو الأخلاق أو الآداب العامة ولها الحق في معاينة المحلات والأماكن التي تتم فيها المعالجة ما لم تكن محلات سكنية، كما لها الحق في الولوج إلى أي معطيات معالجة وجميع المعلوماتوالوثائق مهما كانت دعامتها.

كما يمكن للسلطة الوطنية الاستعانة بأعوان رقابة من أجل بحث ومعاينة جرائم الاعتداء على المعطيات الشخصية تحت إشراف وكيل الجمهورية، إلى جانب ضباط وأعوان الشرطة القضائية حسب المادة (50).[2]

يمكن لأي شخص تم المساس بحقوقه في هذا المجال أن يتقدم للجهة القضائي المختصة لاتخاذ أي إجراءات تحفظية لوضع حد للتعدي أو للمطالبة بالتعويض (52).[3]

أما و من خلال المادة (53) نجد أن المشرع قد أحال إلى المادة (588) من قانون الإجراءات الجزائية التي تنص على قواعد الاختصاص التي يجب مراعاتها من طرف الجهات القضائية الجزائية التي تنص على قواعد الاختصاص التي يجب مراعاتها من طرف الجهات القضائية الجزائية عند متابعتها للجرائم المنصوص عليها في هذا القانون، كما عقد المشرع و من خلال المادة (53) الاختصاص للجهات القضائية الجزائية لمتابعة جرائم الاعتداء على المعطيات الشخصية، التي ترتكب خارج إقليم الجمهورية من طرف جزائري أو شخص أجنبي مقيم في الجزائر أو شخص معنوي خاضع للقانون الجز ائري.[4]

[1]- يوسف رزوق، ص 127.

[2]- المادة 50 من القانون 18-07 المتعلق بحماية المعطيات الشخصية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق، ص 22.

[3]- المادة 52 من المصدر نفسه، نفس الصفحة.

[4]- المادة 52 من المصدر نفسه، نفس الصفحة.

ثانيا: الأحكام الجزائية

شدد المشرع من خلال القانون 18-07 في الفصل المعنون ب "الأحكام الجزائية" العقوبات الناجمة عن خرق أحكام هذا القانون و التي يتراوح الحبس فيها من شهرين إلى 05 سنوات وتتراوح الغرامة من 20000دج إلى 1000000دج، وتختلف الجزاءات بحسب اختلاف المخالفات التي يرتكبها الشخص المعالج أو المعالج من الباطن أو أي شخص أخر أدى تصرفه لخرق أحكام هذا القانون، ومن الحالات: معالجة معطيات ذات طابع شخصي رغم اعتراض صاحبها أو عدم القيام بتصريحات كاذبة أو الاستمرار في العمل رغم سحب الرخصة أو التصريح أو عالج معطيات لأغراض أخرى غير تلك المصرح بها أو جمع معطيات ذات طابع شخصي رغم اعتراض صاحبها، أو عند القيام بتصريحات كاذبة أو الاستمرار في العمل رغم سحب الرخصة أو التصريح أو عالج معطيات لأغراض أخرى غير تلك المصرح بها أو جمع معطيات بطريقة تدليسية و غير نزيهة أو سمح لأشخاص غير مؤهلين بالولوج إلى المعطيات أو عرقل عمل السلطة الوطنية وكذا أوضع عقوبات لكل من يلج دون سبب مشروع حقوق الإعلام و الولوج إلى السجل الوطني أو كل معالج يرفض دون سبب مشروع حقوق الإعلام والولوج أو التصريح أو الاعتراض وكل من لا يقوم بإعلام السلطة الوطنية عن الانتهاكات للمعطيات الشخصية وتبلغ العقوبات أقضاها في حالة نقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا للقانون أو كل من احتفظ بمعطيات ذات طابع شخصي بخصوص جرائم أو إدانات أو تدابير أمن.

أما الشخص المعنوي الذي يقوم بخرق القانون فقد أحالالمشر ع إلى قانون العقوبات، كما قرر ومن خلال المادة (73) لأي محاولة لارتكاب إحدى الجنح المذكورة نفس عقوبة الجريمة التامة وتضاعف العقوبات في حالة العود.[1]

[1]- المادة 73 من القانون 18-07 المتعلق بحماية المعطيات الشخصية ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق، ص 23.

الفصل الثاني:

الحماية الجنائية الإجرائية للوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية في الجزائر.

تعد متابعة الجريمة المعلوماتية بصفة عامة ومتابعة جرائم الوثائق البيومترية الالكترونية خاصة، من أهم التحديات التي تواجه رجال الضبطية القضائية بالنظر إلى طبيعة الجريمة المعلوماتية وهذا من حيث أنها تتعلق بمحل غير مادي بالإضافة إلى صعوبة دور الشرطة ومختلف الأجهزة الأمنية في مراقبتها وضع حدوثها وكذا التحري في مرتكبيها.

كما أن المجرم المعلوماتي، عادة ما يكون ذا خبرة وذكاء ودهاء خارق، قد لا يستطيع المحقق الجنائي العادي التعامل معه كما أن الأدلة المتحصل عليها من مسرح الجريمة تختلف عن الأدلة التقليدية.

وعليه سنتطرق في هذا الفصل إلى أهم القواعد الإجرائية التي جاء بها المشرع الجزائري لمواجهة هذه الأنماط المستجدة من الجرائم.حيث سنخصص في المبحث الأول لدراسة الحماية الجنائية الإجرائية التقليدية للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر، والمبحث الثاني للحديث عن الحماية الجنائية الإجرائية الحديثة للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر.

المبحث الأول:

الحماية الجنائية الإجرائية التقليدية للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر.

إن البحث عن أدلة إثبات الجريمة المعلوماتية، لا يمكن أن يترك إلى فعل الصدفة، بل يجب أن يكون مخططا ومنظما، فهذه الأدلة لا تكتشف إلا بإجراء أبحاث سواء في مكان وقوع الجريمة مما يستوجب الانتقال للمعاينة وقد تجري حتى في منازل الأشخاص ونكون هنا بصدد تفتيش، ولا يكفي اكتشاف أدلة الإثبات بل يجب ضمان الاحتفاظ بها خلال سير الدعوى الجنائية، لذلك عمد القانون إلى وضع أحكام تتعلق بالاحتفاظ بالأشياء المضبوطة، كما استدعى اللجوء إلى شهادة الشهود وإجراء الخبرة للحصول على الأدلة التي تظهر الحقيقة[1].

إلا أن تميز الجريمة المعلوماتية، بطبيعتها غير المادية للأدلة التي تخلفها، أثبت عدم كفاية القواعد العامة المقررة لإجراءات التحري والتحقيق التقليدية لكل من المعاينة والتفتيش والضبط والشهادة والخبرة، لذا لجأت السياسة الجنائية ومن أجل إمكانية تتبع الدليل الرقمي، وجمعه، ونسب الجريمة إلى مرتكبها، إلى ضرورة **تطوير هذه الإجراءات** بصورة تتلائم مع هذه الخصوصية، وذلك بإضافة قواعد جديدة وخاصة إلى القواعد العامة التي تحكم كل إجراء من إجراءات التحري والتحقيق[2]،ويتعين على المحقق في هذا المجال أن تتوفر فيه شروطا خاصة حتى يتمكن من التحقيق على أكمل وجه.

لذا عمل المشرع الجزائري على تطوير أساليب التحري والتحقيق فيما يخص الجرائم المعلوماتية لتتلاءم مع خصوصية هذه الجرائم، وذلك من خلال تعديل قانون الإجراءات الجزائية بالقانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 وإصدار قانون 09-04 المؤرخ في 05 أوت سنة 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

---

[1]– شرف الدين وردة، المرجع السابق، ص 180

[2]– المرجع نفسه، نفس الصفحة.

لذلك سنخصص هذا المبحث للحديث عن حماية الوثائق البيومترية الإلكترونية من خلال الإجراءات الجنائية التقليدية المستنبطة من الوقائع أوالأشياء في المطلب الأول، ثم حماية الوثائق البيومترية الإلكترونية من خلال الإجراءات الجنائية التقليدية المستنبطة من تصريحات الأشخاص في المطلب الثاني.

المطلب الأول: حماية الوثائق البيومترية الإلكترونية من خلال الإجراءات الجنائية التقليدية المستنبطة من الواقع أو الأشياء.

تقتضي حماية الوثائق البيومترية الإلكترونية من خلال الإجراءات الجنائيةالتقليدية المستنبطة من الوقائع والأشياء، إتباع جهات القضائية الإجراءات التالية:الانتقال للمعاينة حيث سنتكلم عن هذا الإجراء من خلال (الفرع الأول)، التفتيش والضبط والذي سنخصص لهما بالدراسة (الفرع الثاني) من المذكرة،

الفرع الأول: الانتقـــــــال والمعاينـــــــــــــة.

سنتناول في هذا الفرع أسلوب الانتقال والمعاينة، والذي يعتبر أسلوب من الأساليب المستنبطة من الواقع أو الأشياء.

إن الغاية من هذا الإجراء هو انتقال الشخص المكلف بالتحقيق إلى مكان وقوع الجريمة لمباشرة التحقيقات التي من الممكن القيام بها هناك، والانتقال إلى مكان وقوع الجريمة كإجراء يمكن أن يباشر في كل مرحلة من مراحل الدعوى العمومية لكن ليس بنفس الطريقة[1].

عرفها مجموعة من الفقهاء بأنها: "إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة يشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة[2].

[1]– محمد مروان، **نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري**، الجزء الثاني، ديوان المطبوعات الجامعية، الجزائر، 1999، ص343.

[2]– شرف الدين وردة، المرجع السابق، ص182.

هذه بالنسبة للانتقال والمعاينة في حالة الجرائم في صورتها التقليدية، أما الانتقال والمعاينة في الجريمة المعلوماتية فيجب التمييز دائما بين حالتين أساسيتين[1]:

الحالة الأولى: المعاينة في حالة الجرائم الواقعة على المكونات المادية للحاسب الآلي كجرائم الاعتداء على أشرطة الحاسب وكابلاته وشاشة العرض الخاصة به ومفاتيح تشغيل الأقراص وغيرها من مكونات الكمبيوتر ذات الطابع المادي والملموس.

الحالة الثانية: المعاينة في حالة الجرائم الواقعة على المكونات غير المادية أو بواسطتها، وتتمثل في تلك الجرائم الواقعة على برامج الكمبيوتر وبياناته أو بواسطته، وهنا تثور الصعوبات تحول دون فعالية المعاينة من بين هاته الصعوبات نذكر:

- قلة الآثار المادية المختلفة من الجرائم التي تقع على برامج الحاسوب والشبكات.
- إمكانية حدوث تغيير أو تلف أو تلفيق أو عبث بالآثار المادية أو زوال بعضها.
- نقص الدراية ومعرفة المحقق بالجوانب الفنية والتقنية لاستخدام شبكة الانترنت والحاسوب.

وتكون المعاينة بعد الانتهاء من جمع المعلومات اللازمة عن الحادث حيث يبدأ المحقق بتحديد خطة العمل المناسبة وطريق العمل اللازم للتحري، وهذا بمجرد انتهائه من رسمه الصورة الأولية للواقعة قصد الانتقال للمعاينة، فعلى المحقق الأخذ بعين الاعتبار، حجم ونوع الحادث لتعيين فريق التحقيق وكفاءته، والظروف المحيطةبالحادث.

وإذا تمت المعاينة بعد وقوع الجريمة في المجال الالكتروني، فيجب مراعاة ما يلي[2]:

1- تصوير الحاسب والأجهزة الظرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

---

[1]- ناني لحسن، **التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية، (بين النصوص التشريعية والخصوصية التقنية)**، النشر الجامعي الجديد، الجزائر، 2017، ص71.

[2]- شرف الدين وردة، المرجع السابق، ص186.

2- العناية بملاحظة الطريقة التي تم بها إعداد النظام.

3- ملاحظةوإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حتى عرض الأمر فيما بعد على المحكمة.

4- عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال تقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.

5- التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة، وفحصها ويرفع من عليها من البصمات ذات الصلة بالجريمة.

6- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من البصمات.

7- قصر مباشرة المعاينة على الباحثين والمحققين الذي تتوافر لهم الكفاءة العالية والخبرة الفنية في مجال الحسابات.

وكذلك يختلف الانتقال والمعاينة في العالم الافتراضي عن الكيفية المتبعة لمعاينة مسرح الجريمة التقليدية، حيث يمكن لزجل الضبطية العدلية الانتقال إلى مسرح الجريمة في العالم الافتراضي، من خلال الحاسوب الموجود في مكتبه، أو عبر مقهى الانترنت، أو اللجوء إلى مقر مزود الخدمة، الذي يعبر أحسن الأماكن لإمكانية إجراء المعاينة.

إن الأصل أن انتقال المحقق الجنائي لإجراء عملية المعاينة أو لمباشرة أي إجراء أخر من إجراءات التحقيق أمر متروك للسلطة التقديرية له، فلا يقوم به إلا إذا كانت مصلحة من ورائه، لذلك جرى أن المعاينة هي من إجراءات التحقيق التي يترك أمر تقدير لزوم القيام بها إلى السلطة التي تباشر بالتحقيق، وهذا ما قضت به نص المواد 42، 79، 80 من قانون الإجراءات الجزائية الجزائري على أن المعاينة تجري أما من طرف قاضي التحقيق إذا استدعت

ضرورة الحالة إلى دوائر اختصاص محاكم مجاورة، كما يتم أيضا إجراء المعاينة من طرف ضباط الشرطة القضائية الذين عليهم إخطار وكيل الجمهورية فور وصول خبر وقوع الجريمة إلى عملهم و انتقالهم بدون تمهل إلى أماكن الواقعة الإجرامية.[1]

وأثناء معاينة مسرح الجرائم المعلوماتية بتولي قاضي التحقيق معاينة الآثار التي خلفها مستخدم شبكة الانترنت والتي تتمثل في الرسائل المرسلة منه والتي يستقبلها وكل الاتصالات التي قام بها من خلال الكمبيوتر والشبكة العالمية، وكما أن الآثار الرقمية المستمدة من أجهزة الكمبيوتر قد تكون ثرية فيما تحتويه من معلومات مثل صفحات المواقع المختلفة والبريد الالكتروني والملفات المخزنة في الكمبيوتر الشخصي... الخ، أن معظم التشريعات الجنائية الحديثة لم تهتم بتعريف مسرح الجريمة و لم تقم بتحديد النطاق المكاني له كما هو بالنسبة للتفتيش وبالتالي فان معظم التشريعات تعبر عنه بمحل الواقعة.[2]

الفرع الثاني: التفتيـــــــش والضبـــــــــــــط

إن من أهم وسائل الإثبات المستخلصة من الوقائع أو الأشياء التفتيش والحجز، إلا أن أهمية هذا الإجراء وخطورته جعلته يرتقي إلى مرتبة القواعد الدستورية فعملت الدساتير على النص عليها، ومن ثم على السلطات أن تسير على منوالها وعلى المشرع أن يستلزم أحكام القانون منها دون تعارض أو مخالفة معها[3].وستكلم أولاعن إجراء التفتيش ثم الضبط وذلك من خلال ما يلي:

أولا: التفتيـــــــــــــش

يعد إجراء التفتيش من أهم وسائل الإثبات المتبعة في جمع أدلة الإثبات، فهو يقتضي البحث في مستودع سر المتهم سواء في مسكنه أو شخصه عن كل ما يدل من إمكانية ارتكابه للجريمة ونسبها إليه.

[1]– محمد مروان، المرجع السابق، ص .344

[2]– المرجع نفسه، ص 345.

[3]– شرف الدين وردة، المرجع السابق، ص193.

انه وبالإضافة إلى المعاينة من الجائز لعضو الضبط القضائي أثناء التلبس بجرائم الانترنت أن يقوم بتفتيش شخص المشتبه به و ما تحمله من حاسوب نقال أو هاتف نقال أو حاسوب صغير أو مسكنه وما يتضمنه من موجودات ومن بينها الحاسوب، والتفتيش إجراء من إجراءات التحقيق يهدف إلى البحث عن الأشياء تتعلق بالجريمة وكل ما يفيد بصفة عامة في كشف الحقيقة، وعلى الرغم من أن التفتيش بالمعنى التقليدي يهدف إلى حفظ أشياء مادية تتعلق بالجريمة وتفيد في كشف الحقيقة، بينما البيانات الالكترونية ليس لها بحسب جوهرها مظهر مادي ملموس في العالم الخارجي، ومع ذلك فيمكن أن يرد التفتيش على هذه البيانات غير المحسوسة عن طريق الوسائط الالكترونية لحفظها وتخزينها كالأسطوانات والأقراص الممغنطة ومخرجات الحاسب[1].

ولقد أجاز المشرع الجزائري التفتيش في الجرائم المعلوماتية المتلبس فيها في المادة 3/47 حيث يجوز إجراء المعاينة في كل محل سكني أو غير سكني في كل من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص.

ويتضح موقف المشرع الجزائري من تفتيش المنظومات المعلوماتية من خلال نص المادة 05 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها حيث نصت على أنه[2]:

يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة "04" أعلاه الدخول بغرض التفتيش، ولو عن بعد إلى:

أ) منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب) منظومة تخزين معلوماتية.

[1]- عبد الفتاح بيومي حجازي، المرجع السابق، ص378.

[2]- المادة 05 من القانون رقم 09-04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق، ص06.

في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية وأن هذهالمعلومات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فان الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعطيات الضرورية لإنجاز مهمتها.

ثانيا: الضـــــــــــــــبط

يعرف الضبط في البيئة الالكترونية على أنه وضع اليد على الدعائم المادية المخزنة فيها البيانات الالكترونية أو المعلومات التي تتصل بالجريمة المعلوماتية التي وقعت وتفيد في كشف الحقيقة عنها وعن مرتكبها، كما يعرف أيضا بأنه استخدام البرامج الهامة من أجل الولوج للبيانات المراد ضبطها إلى جانب وضع اليد على تلك الدعائم المادية[1].

يعد ضبط الأشياء التي لها علاقة بالجريمة هدفا من أهداف التفتيش ولها ما لها من فائدة في التحقيق الجاري بشأنها، سواء كان هذا الشيء أدوات استعملت في ارتكاب الجريمة أو شيئا نتج عنها أو مما يفيد في كشف الحقيقة.[2]

[1]– الهام بن خليفة، **الحماية الجنائية للمحررات الالكترونية من التزوير**، أطروحة دكتوراه في العلوم القانونية والإدارية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2016، ص291.

[2]– هشام فريد، **الجوانب الإجرائية للجرائم المعلوماتية (دراسة مقارنة)**، مكتبة الألات الحديثة، مصر، 1992، ص75.

وقد نظم المشرع الجزائري في القواعد الخاصة بضبط البيانات المعلوماتية وفقا للقانون رقم 09-04 تحت تسمية "حجز المعطيات المعلوماتية" حيث نصت المادة 06 من نفس القانون على نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة الكترونية التي تكشفها السلطات المختصة عند القيام بالتفتيش في المنظومة المعلوماتية، و تكون هذه المعطيات تفيد إظهار الحقيقة و قابلة للحجز، وتوضع في الإحراز مع وجوب قيام السلطة المختصة بحماية سلامة المعطيات المخزنة في المنظومة المعلوماتية، كما يجوز استخدام الوسائل التقنية وفقا لما يستهدف التحقيق لتشكيل أو إعادة تشكيل هذه المعطيات بشرط عدم المساس بمحتوى المعطيات.[1]

أما المادة 07 من نفس القانون نصت على أنه في حالة استحالة إجراء الحجز وفقا لما نصت عليه المادة 06 وذلك لأسباب فنية فعلى السلطة المختصة بالتفتيش القيام بالتقنيات الواجبة للمنع من الوصول إلى محتوى المعطيات أو نسخها مع الاحتفاظ بها من طرف الأشخاص المصرح لهم بذلك،، كذلك نص المادة 08 تعلقت بالمعطيات التي يشكل محتواها الجريمة، فعلى السلطة المباشرة بالتفتيش أن تصدر أمر بتكليف أي شخص مؤهلا فنيا وتقنيا لاستخدام الوسائل التقنية المناسبة من أجل منع الاطلاع على محتوى هذه المعطيات، أما المادة 09 من نفس القانون فيتضح من خلالها أن المعلومات المحصل عليها عن طريق المراقبة وفقا لهذا القانون لا يجوز استخدامها إلا في الحدود الضرورية التي يقتضيها التحري أو التحقيق القضائي، وذلك تحت طائلة العقوبات التي نص عليها التشريع المعمول به.[2]

المطلب الثاني: حماية الوثائق البيومترية الإلكترونية من خلال الإجراءات الجنائية التقليدية المستنبطة من تصريحات الأشخاص

سوف نتطرق في هذا المطلب إلى الإجراءات ذات الطبيعة الشخصية والتي غالبا ما يتوسط فيها الشخص بين القيام بالإجراء والحصول على الدليل. وتتمثل هذه الإجراءات في

[1]– هشام فريد، المرجع السابق، ص 76.

[2]– المرجع نفسه، نفس الصفحة.

الشهادة (الفرع الأول)، الخبرة (الفرع الثاني)، الاستجواب (الفرع الثالث) وسنكلم عن كل إجراء من هذه الإجراءات من خلال ما يلي:

الفرع الأول: الشـــــــــــــــــهادة

تعتبر الشهادة أحد الوسائل المتبعة في جمع الأدلة الناتجة عن الجريمة المرتكبة، فهي عبارة عن إدلاء شخص أمام الجهات المتخاصمة بما رآه أو سمعه أو تذوقه[1]، فهذه الشهادة تنير درب السلطات القضائية المختصة بالتحقيق والمحاكمة إلى الحقيقة المنشودة عن قيام الجريمة من عدمه، وسنتطرق في هذا الفرع إلى أولا تعريف الشهادة ثم بيان إجراءات الشهادة في الجرائم الماسة بالوثائق البيومترية الإلكترونية وفقا للتشريع الجزائري.

أولا: تعريـــــف الشهـــــــــادة

الشهادة هي ما يقوله أحد الأشخاص عما شاهده أو سمعه أو أدركه بحواسه ن واقعة بطريقة مباشرة، فهي تحضى باهتمام القاضي إلا أنه غالبا ما يحتاج في مقام وزن الأدلة إلى من رأى الواقعة أو سمع عنها أو أدركها بحواس، حتى قيل أن الشهود هم عيون المحكمة وأذانها[2].

كما أن الشهادة كإجراء من الإجراءات التحقيق هي المعلومات التي تتعلق بالجريمة التي يدلي بها الشاهد أمام سلطة التحقيق.

ويختلف الشاهد التقليدي عن الشاهد المعلوماتي ذلك أن الشاهد في الجريمة المعلوماتية هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي، والذي تكون لديه معلومات جوهرية اللازمة للدخول إلى نظام المعالجة الآلية للبيانات متى كانت مصلحة التحقيق تتطلب التنقيب عن المعلومات الداخلية وتنحصر طوائف وفئات الشاهد المعلوماتي فيما يلي[3]:

1- مشغلو الحاسب الآلي.

---

[1]- شرف الدين وردة، المرجع السابق، ص244.

[2]- أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، دار النهضة، مصر، 1981، ص29.

[3]- شرف الدين وردة، المرجع سابق، ص257.

2-خبراء البرمجة.

3-المحللون.

4-مهندسو الصيانة والاتصالات.

5-مديري النظام.

كما أن الشاهد المعلوماتي في مجال الالتزام بالإعلام في الجريمة المعلوماتية شروط تتمثل في:

- أن نكون بصدد جريمة مست بالفعل المستند الالكتروني سواء كانت جناية أو جنحة.

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

- أن تقتضي مصلحة التحقيق الحصول على هذه المعلومات الجوهرية.

ثانيا: إجراءات الشهادة في الجرائم الماسة بالوثائق البيومترية الالكترونية وفقا للتشريع الجزائري

اهتم المشرع الجزائري بدور الشاهد المعلوماتي في مساعدة السلطات العامة في مكافحة الجرائم المعلوماتية، وهذا عن طريق إلزامه بالإعلام عن المعلومات الجوهرية التي تسمح بالدخول إلى الحاسوب وجمع الأدلة المخزنة به ذلك في المادة 05 الفقرة الأخيرة من القانون 09-04[1].

كما نصت المادة 04/19 من اتفاقية بودابست لمكافحة جرائم الكمبيوتر لعام 2001 على إمكانية الاستعانة بالشاهد المعلوماتي بقولها يجب على كل طرف أن يتبين الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل تحويل سلطاته المختصة سلطة

[1]- القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق.

إصدار الأمر لأي شخص لديه معلومات عن تشغيل النظام أو الإجراءات المطبقة من أجل حماية البيانات المعلوماتية التي تضمن تقديم كل المعلومات الضرورية على نحو معقول يسمح بتطبيق الإجراءات المشار إليها في الفقرتين 1 و2.[1]

الفرع الثاني: الخبـــــــــــــــرة:

تعتبر الخبرة وسيلة من وسائل الإثبات المتبعة من قبل السلطات المختصة بمكافحة الإجرام بغية الحصول على الدليل المثبت لقيام الجريمة، وسنتكلم في هذا الفرع عن تعريف الخبرة أولا ثم إجراءات الخبرة في الجرائم الماسة بالوثائق البيومترية الإلكترونية ثانيا وذلك من خلال ما يلي:

أولا: تعـــــــريف الخبـــــــــــرة

الخبرة هي إجراء يستهدف استخدام قدرات شخص الفنية والعلمية والتي لا تتوافر لدى رجل القضاء أو المحقق من أجل الكشف عن دليل يفيد معرفة الحقيقة بشأن وقوع الجريمة[2].

الخبير المعلوماتي أو الرقميهو الخبير المتخصص والمدرب على معالجة جميع أنواع الأدلة الرقمية وفحصها وتخليلها. وتكون للخبرة القانونية قواعد قانونية وأخرى تقنية.[3]

قواعد ما قبل التشغيل والفحص:وتتمثل فيما يلي:[4]

- التأكد من مطابقة محتويات إحراز المضبوطات لما هو مدون عليها.
- التأكد من صلاحية وحدات نظام التشغيل.
- تسجيل بيانات وحدات المكونات المحجوزة كالنوع و الطراز و الرقم المسلسل و غيرها.

---

[1]– شرف الدين وردة، الإثبات الجنائي بالأدلة الإلكترونية، المرجع السابق، ص260.

[2]– سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة ماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة لحاج لخضر، باتنة، 2013، ص165.

[3]– المرجع نفسه، نفس الصفحة.

[4]– إلهام بن خليفة، المرجع السابق، ص299.

قواعد التشغيل والفحص: والتي تتمثل في:[1]

– عمل نسخة أصلية من الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية استغلال الدليل.

– عمل نسخة من كل وسائط التخزين المضبوطة وعمل رأسها القرص الصلب لإجراء عملية الفحص المبدئي على هذه النسخة للحماية الأصل من أي فقد أو تلف أو تدمير سواء من سوء الاستخدام أو لوجود فيروسات أو قنابل برمجية.

– إظهار الملفات المخبأة والنصوص المخفية داخل الصور.

– استكمال تسجيل باقي المعطيات من خلال قراءات الجهاز.

– تحديد مدى الترابط بين الدليل المادي والدليل التقني.

– مرحلة تدوين النتائج وإعداد التقارير.

ثانيا: إجراءات الخبرة في مجال الجرائم الماسة بالوثائق البيومترية الالكترونية وفقا للتشريع الجزائري: والتي يمكن إيجازها في النقاط التالية[2]:

تجدر الإشارة إلى أن المشرع الجزائري نظم أحكام الخبرة في المواد من 143 إلى 156 من قانون الإجراءات الجزائية.

كما نص المشرع الجزائري في المادة 04 من المرسوم الرئاسي رقم 15–216 المؤرخفي 08 أكتوبر سنة 2015 المحددة لتشكيلة وتنظيمية وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على الخبرة القضائية.

[1]– سعيداني نعيم، المرجع السابق، ص172.

[2]– شرف الدين وردة، المرجع السابق، ص283.

كذلك يقوم المعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي الجزائر العاصمة بإجراء الخبرات في إطار التحريات الأولية والتحقيقات القضائية وهذا لغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح.

الفرع الثالث: الاستجـــــــــــــواب

الاستجواب هو مسائلة المتهم ومناقشته عن وقائع القضية المنسوبة إليه عن الجريمة التي ارتكبها ومجابهته بالأدلة وسماع ما لديه من دفوع التهمة المنسوبة ليه.[1]

والاستجواب في الجريمة المعلوماتية تحكمه ذات القواعد العامةلاستجواب المتهم في الجريمة التقليدية.[2]

ومن بين حقوق المتهم أثان الاستجواب، حق المتهم في الاستعانة بمحامي، وحق المحامي في الاطلاع على التحقيق.[3]

والاستجواب كإجراء من إجراءات التحقيق له طبيعة مزدوجة، فهو طريق للدفاع عن طريق تقييد الأدلة المقدمة ضده وطريق للبحث والاستكشاف لأنه يسمح لقاضي التحقيق بأن يجد في حيرة المتهم و تردده في إجاباته وعدم تماسك أقواله وثبوت كذبها عناصر لإثبات التهمة ضده.[4]

وبمعنى أخر الاستجواب إجراء من إجراءات التحقيق يسمح للمتهم بنفي التهمة عنه والإدلاء بأقواله بكل حرية دون ضغط أو تأثير عن إرادته ويقع في استجواب المتهم حسب المادة "100" من ق.إ.ج. بعد تأكد قاضي التحقيق من هويته، ثم يحيطه علما بالتهمة المنسوبة إليه، وينبهه بأنه حر في عدم الإدلاء بأي قرار وينوه عن ذلك في المحضر[5].

[1] - مروك نصر الدين، **محاضرات في الإثبات الجنائي**، الجزء الأول، دار هومة، الجزائر، 2014، ص371.

[2] – مروك نصر الدين، المرجع السابق، ص371

[3] – المرجع نفسه، ص372

[4] – المرجع نفسه، نفس الصفحة.

[5] – المرجع نفسه، ص373.

والاستجواب في الماضي وسيلة للحصول على اعتراف المتهم بأية طريقة ولو بالتعذيب وكثيرا ما أدت هذه الوسيلة إلى صدور اعترافات كاذبة وأدين بمقتضاها أبرياء كثيرون في حين أفلت المذنبون الحقيقيون، وقد لاقت هذه الوسيلة اعتراضات كثيرة وأسفرت هذه الاعتراضات عن اعتبار تعذيب المتهمين أمرا منكرا يستوجب المساءلة بل وصل في بعض التشريعات إلى حد اعتباره جريمة، وقد نصت المادة 110 مكرر من قانون العقوبات في فقرتها الثالثة على عقاب كل موظف أو مستخدم يمارس أو يأمر بممارسة التعذيب للحصول على إقرارات بالحبس من 06 أشهر إلى 03 سنوات[1].

[1]– مروك نصر الدين، المرجع السابق، ص373.

المبحث الثاني:

الحماية الجنائية الإجرائية الحديثة للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر

إن الأنظمة المعلوماتية وفي ظل المعطيات الحديثة للمجتمعات المعاصرة تشهد انفتاحا غير مسبق ومحدود وإتاحة للمعلومة غير مشروط وهو ما يجعلها مجالا مفتوحا تهدده أخطار الاعتداءات المعلوماتية بكل أشكالها.

مما جعل العديد من الدول تقوم بتطوير سياستها الجنائية تبعا لهذه الخصوصية وتمكن رجال الشرطة القضائية من الكشف عن الجرائم، من خلال سن إجراءات حديثة للتحري والتحقيق عن الجرائم المعلوماتية ومنها الجرائم الماسة بالوثائق البيومترية الالكترونية، ومنه سنتطرق في هذا المبحث إلى حماية الوثائق البيومترية الإلكترونية من خلال الإجراءات الحديثة المستنبطة من الوقائع أو الأشياء (المطلب الأول)، وحماية الوثائق البيومترية الإلكترونية من خلال الإجراءات المستنبطة من تصريحات الأشخاص في (المطلب الثاني).

المطلب الأول: حماية الوثائق البيومترية الإلكترونية من خلال الإجراءات الجنائية الحديثة المستنبطة من الوقائع أو الأشياء

تتمثل هذه الإجراءات في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور (الفرع الأول) بالإضافة إلى إجراء المراقبة الالكترونية (الفرع الثاني) وإجراء جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها (الفرع الثالث) وذلك من خلال الآتي:

الفرع الأول: اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور

سنتطرق في هذا الفرع إلى تعريف إجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور، ثم الإجراءات المتبعة في اعتراض المراسلات السلكية واللاسلكية

وتسجيل الأصوات والتقاط الصور في الجرائم الماسة بالوثائق البيومترية الإلكترونية وفقا للتشريع الجزائري وذلك من خلال ما يلي:

أولا: تعريف اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور

قد تضطر الشرطة القضائية لاستعمال كاميرات خفية أو أجهزة تنصت لكن يجب أن يكون ذلك في إطار احترام الشرعية الإجرائية حفاظا على كرامة الحياة الخاصة للإنسان كما يمكن لضباط الشرطة القضائية تصوير جسم ومكان الجريمة بشكلها العام في إطار ممارسة عملهم، لكنه يمنع من الاطلاع أو تسجيل المكالمات أو الأحاديث الخاصة إلا بإذن مسبق من طرف السلطات القضائية، وفقا لما نص عليه الدستور الجزائري في المادة "99".[1]

ويقصد باعتراض المراسلات بأنه إجراء يتم من خلاله رصد كل كلمة أو كل المحادثات التي تجري بين الأشخاص وهذا الكلام أو الحوار يتم أولا التقاطه ثم تثبيته بتسجيله و بثه عند الحاجة ومن ثم يستعمل كدليل يواجه به المتهم.[2]

والمقصود بالمراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية حسب الماجة 8-21 من القانون رقم 2000-3 المؤرخ في 2000/08/05 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.[3]

أما تسجيل الأصوات والتقاط الصور فيقصد تسجيل المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة في مكان عام أو خاص، وكذلك التقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان واحد خاص[4].

---

[1]- ناني لحسن، المرجع السابق، ص73.

[2]- المرجع نفسه، نفس الصفحة.

[3]- شرف الدين وردة، **مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية في التشريع الجزائري**، مجلة المفكر، العدد الخامس عشر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 15 جوان 2017، ص542.

[4]- الهام بن خليفة، المرجع السابق، ص310.

ومن بين صحة شروط اعتراض المراسلات والتقاط الصور وتسجيل الأصوات[1]:

– أن تكون الجريمة الواقعة على الوثائق البيومترية الالكترونية على درجة معينة من الجسامة.

– أن تكون هناك فائدة في ظهور الحقيقة.

هذا بالنسبة للشروط الموضوعية أما الشروط الشكلية فتتمثل في:

– لابد من صدور أمر باعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور.

– أن يسبب الأمر باعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور.

– تحرير محضر بعملية الاعتراض بالمراسلات أو تسجيل الأصوات أو التقاط الصور.

– يجب أن تكون السلطة المختصة بالتحقيق الابتدائي، سواء كان قاضي التحقيق أو النيابة العامة وحدها دون غيرها هي من تطلع على المراسلات أو الصور.

ثانيا: إجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وفقا للتشريع الجزائري

تمم قانون الإجراءات الجزائية الجزائري بالباب الثاني من الكتاب الأول بالقانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 بفصل رابع بعنوان " في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" ويشمل المواد من 65 مكرر 05 إلى 65 مكرر 10 حيث:

يجوز لرجال الشرطة القضائية إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي، القيام باعتراض المراسلات، تسجيل الأصوات والتقاط الصور لكنه قيدهم بجملة من الشروط لتكون إجراءاتهم صحيحة ومنتجة لأثارها وهي[2]:

[1]– شرف الدين وردة، المرجع السابق، ص ص 295، 299.

[2]– شرف الدين وردة، المرجع السابق، ص 321، 324.

– أن يقوم الضباط بهذه الأعمال سعيا للكشف عن جرائم حددها المشرع في المادة 65 مكرر 05 وهي: جرائم المخدرات، الجرائم المنظمة العابرة بالحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد.

ما يلاحظ أن المشرع الجزائري عدد هذه الجرائم على سبيل الحصر وقد يرجع هذا للخطورة الإجرامية لهذه الأفعال وأثرها على السياسة العامة في الدولة واقتصادها، أما إذا كانت هذه الأعمال في غير هذه الجرائم فإجراؤها باطل.

– أن يصدر الإذن إلى ضباط الشرطة القضائية للقيام بالأعمال المحددة في المادة 65 مكرر 05، مكتوبا من وكيل الجمهورية أو قاضي التحقيق المختصين، بأن يأذنوا بما يلي:

* اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

*وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أمكان خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

يسمح الإذن المسلم بوضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم الحق على تلك الأماكن.

تنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص، في حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة.

– ضابط الشرطة القضائية مقيد أثناء قيامه بالعمليات المحددة في المادة 65 مكرر 05، بالحفاظ على السر المهني حرصا على نجاحها من جهة وخوفا من فشلها من جهة أخرى وهذا راجع لخطورة هذه الأفعال الإجرامية التي تنفذ أعلى مستوى من الاحتراف والسرية، وإذا اكتشفت

جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي، فان ذلك لا يكون سببا لبطلان الإجراءات العارضة.

– يجب أن يتضمن الإذن المذكور، كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها كتحديد رقم الهاتف واسم المشترك، وتحديد الأماكن المقصودة سكنية أو غيرها، وتحديد الجريمة التي تبرر اللجوء إلى هذه التدابير.

– يسلم الإذن مكتوبا بالمدة أقصاها أربعة (04) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية.

– يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له، ولقاضي التحقيق وضابط الشرطة القضائية الذي ينيبه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65 مكرر 05.

– يحرر ضابط الشرطة القضائية المأذون له أو الناب من طرف القاضي لمختص محضرا عن كل عملية اعتراض وتسجيل المرسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري، ويذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها.

– يصف أو ينسخ ضابط الشرطة القضائية المأذون له أو المناب المراسلات أو الصور أو المحادثات المسجلة والمفيدة في إظهار الحقيقة في محضر يودع بالملف، وتنسخ وتترجم المكالمات التي تتم باللغة الأجنبية، عند الاقتضاء بمترجم يسخر لهذا الغرض.

الفرع الثاني: مراقبـــة الاتصـــالات الالكترونيـــــة

طبقا لنص المادة (03) من القانون 09-04 سابق الذكر فقد وضع المشرع الجزائري بين أيدي الجهات المختصة بمكافحة الجريمة المتصلة بتكنولوجيا المعلوماتية وسيلة قانونية وجديدة

من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتحميل وتسجيل محتواها في حينها وهو ما أطلق عليه مصطلح مراقبة الاتصالات الالكترونية.[1]

وقد تم تعداد الحالات التي يمكن اللجوء فيها إلى هذه الوسيلة من وسائل البحث والتحري من خلال المادة 04 من ذات القانون وهي أربع حالات[2]:

– في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة والاقتصاد الوطني.

– للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

– لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

– في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

ولمباشرة المراقبة الالكترونية يجب الحصول على إذن مكتوب من السلطات القضائية المختصة طبقا لن المادة 04 من القانون 09-04.

يحمي المشرع الجزائري على غرار باقي التشريعات الأخرى الحق في الخصوصية وما يتفرع عنه من حرية المراسلات وذلك عن طريق تجريمه لكل سلوك من شأنه الاعتداء على حرمة الحياة الخاصة في المادة 303 مكرر من قانون العقوبات والتي جاء فيها أنه يعاقب بالحبس من 06 أشهر إلى 03 سنوات وبغرامة من 50000دج إلى 30000دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت وذلك:[3]

– بالتقاط أو تسجيل أو نقل المكالمات أو الأحاديث الخاصة أو السرية بغير إذن صاحبها أو رضاه.

[1]– ناني لحسن، المرجع السابق، ص 80.

[2]– المرجع نفسه، ص81.

[3]– الهام بن خليفة، المرجع السابق، ص318.

– ويشمل مصطلح المراسلات حتى مراسلات البريد الالكتروني.

الفرع الثالث: جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها

نظم المشرع الجزائري هذا الإجراء ضمن القانون 09-04 السابق الذكر وجعله من التزام مقدمي الخدمات في مساعدة السلطات حيث تنص المادة "10" أنه في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها ذلك تحت طائلة العقوبات المكررة لإفشاء أسرار التحري والتحقيق.[1]

المطلب الثاني: الإجراءات الحديثة المستنبطة من تصريحات الأشخاص:

سنتكلم في هذا المطلب عن كل من إجراء التسرب في (الفرع الأول)، وإجراء جمع وتسجيل المعطيات المتعلقة بحركة السيرفي (الفرع الثاني)، ثم إلى إجراء الأمر بإنتاج بيانات معلوماتية في (الفرع الثالث).

الفرع الأول: التســــــــــرب

نظم المشرع الجزائري هذا الإجراء من خلال المواد من 65 مكرر 11 إلى غاية المادة 65 مكرر 18 من ق.إ.ج، وسنتكلم عن تعريف التسرب أولا ثم إجراءات التسرب في مجال الجرائم الماسة بالوثائق البيومترية الإلكترونية ثانيا وذلك كالتالي:

أولا: تعريف التســــــــــرب

[1]– القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحاتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق.

عرفت المادة 65 مكرر 12 من ق.إ.ج.ج. التسرب بأنه: "قيام ضابط عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص والمشتبه في ارتكابهم الجناية والجنحة بإيهامه بأنه فاعل معهم أو شريك لهم أو خاف".[1]

ويعرفه البعض بأنه تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية وهذا بهدف مراقبة أشخاص مشتبه فيهم.[2]

ويعرفه البعض بأنه: "أكثر وسائل التحري تعقيدا أو خطورة، لأنه يتطلب من ضابط الشرطة القضائية وأعوانه القيام بالمناورات وتصرفات توحي بأن القائم بها مساهم في ارتكاب الجريمة مع بقية أفراد العصابة، ولكنه في حقيقة الأمر يخدعهم ويتحايل عليهم فقط، يوهمهم بأنه فاعل وشريك لهم وذلك حتى يطلع على أسرارهم من الداخل، ويجمع ما يستطيع من أدلة إثبات ويبلغ السلطات بذلك فتتمكن من ضبط المجرمين ووضع حد للجريمة.[3]

ثانيا: إجراءات التسرب في مجال الجرائم الماسة بالوثائق البيومترية الالكترونية

استحدث المشرع الجزائري في قانون الإجراءات الجزائية بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 إجراء التسرب كأسلوب من أساليب التحري والتحقيق عن الجرائم الخطرة منها المعلوماتية وذلك في المواد من 65 مكرر 11 إلى 65 مكرر 18، فتعرف المادة 65 مكرر 12 التسرب على أنه "يقصد بالتسرب قيام ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم الجناية أو الجنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف"، حيث تتم هذه الإجراءات وفقا للقيود و الشروط المقررة في الأحكام المقررة قانونا والتي تتمثل فيما يلي.[4]

---

[1]– ناني لحسن، المرجع السابق، ص74.

[2] –عبد الرحمان خلفي، **الإجراءات الجزائية في التشريع الجزائري والمقارن**، الطبعة الثانية، دار بلقيس، الجزائر، 2016، ص105.

[3]– شرف الدين وردة، مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية في التشريع الجزائري، المرجع السابق، ص545.

[4]– شرف الدين وردة، الإثبات الجنائي بالأدلة الالكترونية، المرجع السابق، ص343، 345.

– أن تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم الموصوفة بالإرهابية وجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد والتهريب، عملا بحكم المادتين 65 مكرر 05 و65 مكرر 11 من قانون الإجراءات الجزائية، والمادة 24 مكرر من قانون الوقاية من الفساد ومكافحته والمادتين 33 و34 من قانون التهريب.

– يجب أن يتم الإذن بعملية التسرب من طرف وكيل الجمهورية أو من طرف قاضي التحقيق، بعد إخطار وكيل الجمهورية.

– يجب أن يكون الإذن المسلم مكتوبا ومسببا وذلك تحت طائلة البطلان مع ذكر الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (04) أشهر ويمكن أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية، ويجوز للقاضي الذي رخص باجراها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة وتدع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب.

– لا يجوز إظهار الهوية الحقيقة لضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تخت هوية مستعارة في أي مرحلة من مراحل الإجراءات، ويعاقب كل من يكشف هوية ضباط وأعوان الشرطة القضائية بالحبس من سنتين (02) إلى خمس (05) سنوات وبغرامة من 50000دج إلى 200000دج.

وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من (05) الى عشر (10) سنوات وبغرامة من 200000دج إلى 500000دج.

– إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في رخصة التسرب، وفي حالة عدم تمديدها، يمكن للعون المتسرب مواصلة إجراءات التسرب للوقت الضروري الكافي لتوقيف

عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا، على ألا تتجاوز تلك المدة أربعة (04) أشهر، وفي هذه المدة يتعين إخبار القاضي الذي رخص بإجراء عملية التسرب تلك في أقرب الآجال، إذا انقضت مهلة الأربعة (04) أشهر تلك دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه، أمكن لهذا القاضي أن يرخص بتمديدها لمدة أربعة (04) أشهر على الأكثر.

– يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدا على العملية.

الفرع الثاني: جمع وتسجيل المعطيات المتعلقة بحركة السير

تحدث المشرع الجزائري في الفصل الرابع من القانون رقم 09-04 المؤرخ في 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وفي المادتين 10 و11 على أنه من بين التزامات مقدمي الخدمات مساعدة السلطات المكلفة بالتحريات بحفظ المعطيات.حيث نصت المادة 10 على أنه في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية... ويوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة "11" (حفظ المعطيات المتعلقة بحركة السير)، تحت تصرف السلطات المذكورة، ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.[1]

بينما فصلت المادة 11 في إجراء حفظ المعطيات المتعلقة بخط السير حيث نصت على أنه: مع مراعاة طبيعة ونوعية الخدمات، يلتزموا مقدمو الخدمات بحفظ:

أ) المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

[1]– شرف الدين وردة، الإثبات الجنائي بالأدلة الالكترونية، المرجع السابق، ص357، أنظر كذلك: طرشي نورة، **مكافحة الجريمة المعلوماتية**، مذكرة ماجستير في العلوم القانونية، كلية الحقوق و العلوم السياسية، جاعة يوسف بن خدة، الجزائر، 2007، ص134.

ب) المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

ج) الخصائص التقنية وكذا تاريخو وقت و مدة كل اتصال.

د) المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها.

هـ) المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال و كذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه الماجة و كذا تلك التي تسمح بالتعرف على مصدر الاتصال و تحديد مكانه.

تحدد مدة حفظ المعطيات المذكورة بسنة واحدة ابتداء من تاريخ التسجيل، دون الإخلاء بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في المادة "11" من نفس القانون، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (06) أشهر إلى خمس (05) سنوات وبغرامة من 50000دج إلى 500000دج.

وقد حدد هذا القانون المدة اللازمة لحفظ المعطيات بنسبة واحدة من تاريخ التسجيل كما أوجب من خلال المادة "12" من القانون رقم 09-04 على مقدمي الخدمات التزامات خاصة هي[1]:

- واجب التدخل الفوري لسحب المعطيات المخالفة للقانون وتخزينها أو منع الدخول إليها باستعمال وسائل فنية وتقنية.

- وضع الترتيبات التقنية لحصر إمكانيات الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام وأن يخبروا المشتركين لديهم بوجوده.

[1]- طرشي نورة، المرجع السابق، ص 134.

كما نص المشرع الجزائري في المادة 04 من المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر سنة 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، على أنه: من بين المهام المكلفة للهيئة حفظ المعطيات الرقمية و تحديد مصدرها و مسارها من أجل استعمالها في الإجراءات القضائية، وأنه لم يحدد المدة القصوى التي تلتزم بها الهيئة لحفظ هذه المعطيات كما فعل بالنسبة لحفظ المعطيات المتعلقة بخط السير على مستوى مقدمي خدمات الانترنت بمقتضى المادة 11 من القانون 09-04.[1]

الفرع الثالث: الأمر بإنتاج بيانات معلوماتية

هو إجراء جديد للتحري والتحقيق على الجرائم المعلوماتية، لم تنص عليه معظم الدول ومنها الجزائر لكن تم النص عليه ضمن اتفاقية بودابست لمكافحة جرائم المعلوماتية سنة 2001 وهذا في نص المادة "18" من الاتفاقية.

كما تم النص عليه ضمن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة سنة 2010، والتي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 08 سبتمبر سنة 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 سبتمبر سنة 2010، وهذا في نص المادة 25 من الاتفاقية ويشير هذا الأمر إلى أن تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى: أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين، أو مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته.[2]

[1]- القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحاتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق، ص 16.

[2]- الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 57، الصادرة في 28 سبتمبر 2014، ص08، أنظر كذلك: شرف الدين وردة الإثبات الجنائي بالأدلة الإلكترونية، المرجع السابق، ص366.

المبحث الثالث:

تقدير القاضي الجزائي للأدلة الرقمية الناتجة عن الجرائم الماسة بالوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر

تعتمد المجتمعات المعاصرة في تسيير شئونها على تقنيات الحاسبات والمعلومات، مما أدى إلى تقلص الدور التقليدي للوثائق في الإثبات، وازدياد مطرد في كم المعلومات المنتجة أو المعروضة في أوعية –لا ورقية مستحدثة–، مما يتعين على أجهزة إنفاذ القانون، أن تتعامل في ممارستها لحق المجتمع في الدفاع عن كيانه ضد الإجرام مع أشكال مستحدثة من الأدلة غير المادية (أدلة رقمية)، وذلك في مجال الإثبات الجنائي.[1]

لذا خصصنا المطلب الأول من هذا المبحث للحديث عن ماهية الأدلة الرقمية.

كما أن هذه الأدلة الرقمية، يشترط لقبولها أمام القاضي الجزائي مهما كان نظام الإثبات الجنائي للدولة، أن تتوافرها فيها مجموعة من الشروط لقبول هذه الأدلة كحجة يبني القاضي الجزائي حكمه عليها بالإدانة أو البراءة، وهو ما سنتطرق له في المطلب الثاني من هذا المبحث.

وسنتطرق في هذا المبحث إلى: مفهوم الدليل الرقمي في (المطلب الأول)، ثم إلى شروط قبول القاضي الجزائي للأدلة الرقمية الناتجة عن الجرائم الماسة بالوثائق البيومترية الالكترونية في (المطلب الثاني).

[1]– عبد الفتاح بيومي حجازي، المرجع السابق، ص 10.

المطلب الأول: مفـــــهوم الـــــدليل الرقمـــــــــي

الدليل الجنائي هو " الوسيلة المبحوث عنها في التحقيقات بغرض إثبات صحة واقعة تهم الجريمة أو ظرف من ظروفها المادية أو الشخصية "، أو هو " الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه "[1].

وقد اعتمد الفقه على استخدام مصطلح الإثبات للتعبير بها عن الدليل ومصطلح الدليل للتعبير بها عن الإثبات، بحيث يبدو وكأنهما مصطلحان مترادفان، إلا أنه في الحقيقة لا يوجد تطابق بينهما. فمصطلح الإثبات بالمعنى العام تطلق على كل المراحل التي تمر بها العملية الإثباتية وعليه فالإثبات هو تنقيب عن الدليل وتقديمه وتقديره لاستخلاص السند القانوني للفصل في الدعوى المعروضة بينما مصطلح الدليل فهو الواقعة التي يستمد منها القاضي البرهان الذي يبني عليها اقتناعه بالحكم الذي ينتهي إليه وبعبارة أخرى الدليل هو الثمرة المستخلصة من الإثبات. وفي هذا المعنى الإثبات مصطلح أعم وأشمل من الدليل[2].

تختلف أنواع الأدلة الجنائية، باختلاف الزاوية التي استند عليها لتقسيمها فمنهم من قسمها على أساس مصدرها، ومنهم من قسمها على أساس الجهة التي يقدم إليها الدليل، ومنهم من قسمها على أساس علاقة الدليل بالواقعة المراد إثباتها، ومنهم من قسمها على أساس الأثر المترتب على الدليل[3].

مهما اختلفت زاوية نظر الفقهاء القانونيين في تقسيم الدليل الجنائي، فنحن نرى أنه يمكن تقسيمه إلى أدلة مادية وأدلة غير مادية أو غير مرئية كالدليل الإلكتروني (الدليل الرقمي) وهو موضوع بحثنا، لذا سنخصص هذا المبحث لدراسة التعريف بالدليل الإلكتروني (الفرع الأول) وبيان أنواع الأدلة الرقمية المستمدة من الجرائم الماسة بالوثائق البيومترية الإلكترونية (الفرع الثاني)، ثم نتطرق لأهم المشكلات المتعلقة بالدليل الإلكتروني (المطلب الثاني).

---

[1]– العربي شحط عبد القادر و نبيل صقر، **الإثبات في المواد الجنائية**، دار الهدى، الجزائر، 2006، ص 15.

[2]– المرجع نفسه، ص 15 –16.

[3]– أنظر بالتفصيل في هذه التقسيمات: المرجع نفسه، ص 19–21.

الفرع الأول: تـــــــعريف الدليل الرقمـــــــــي

يعتبر مصطلح الدليل الرقمي من أهم المصطلحات المتداولة في إطار القانون الجنائي لا سيما عند الحديث عن الإثبات، حيث بدونه لا يمكن إسناد الواقعة إلى المتهم.

يعرف الدليل الالكتروني المستخرج من الوثائق البيومترية الالكترونية على أنه "تلك الأدلة التي يمنك الحصول عليها من الحاسوب بإحدى وسائل الخراج".

وهو ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية، وأجهزة ومعدات وأدوات الحاسب الآلي أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور أو أشكال أو أصوات، لإثبات وقوع الجريمة و لتقرير البراءة أو الإدانة فيها.[1]

كما عرفته المنظمة العالمية لدليل الكمبيوتر IDCE في أكتوبر 2001 بأنه: (المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية).[2]

وفي نظرة أخرى موسعة تعرف الأدلة الرقمية: (بأنها جميع أنواع البيانات المخزنة أو المرسلة من خلال تكنولوجيا المعلومات والتي تعتمد عليها نظرة إثبات ارتكاب الجريمة)، بينما يعرفها دليل الشرطة للأدلة الجنائية في المملكة المتحدة " Evidence code UK Police and Criminel" بأنها (جميع المعلومات الموجودة في الحاسوب)[3].

ومن خلال استقراء هذه التعاريف، يمكن تحديد خاصيتين للدليل الرقمي هما:

---

[1]– محمود إبراهيم غازي، **الحماية الجنائية للخصوصية والتجارة الإلكترونية،مكتبة الوفاء القانونية**، مصر، الطبعة الأولى، 2014، ص 670.

[2]– شرف الدين وردة، الإثبات الجنائي بالأدلة الالكترونية، المرجع السابق، ص06.

[3]– هارون بحرية، **دور الدليل الرقمي في إثبات الجريمة المعلوماتية في التشريع الجزائري**، بحث مقدم لأعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة بسكرة، الجزائر، ما بين 16 و17 نوفمبر، 2015، ص02.

- الخاصية الأولى: أن الدليل الالكتروني عبارة عن معلومات أو بيانات الكترونية مخزنة في الحاسوب أو المنقولة بواسطته، أيا كان شكل هذا الحاسوب، سواء كان حاسوب شخصي، أو مخدم الانترنت، أو أن يكون ضمن الهاتف الجوال، أو ساعة اليد، أو الكاميرات الرقمية و غيرها.
- الخاصية الثانية: القيمة الاستدلالية أو البرهانية لهذه المعلومات في إثبات أو نفي الجرائم.

وبناءا على ما تقدم يمكن تعريف الدليل الرقمي بأنه "بيانات أو معلومات مخزنة في حاسوب أي كان شكله أو المنقولة بواسطته، يستعمل لإثبات قيام أو نفي جريمة ما، أمام الجهات القضائية المختصة".[1]

الفرع الثاني: أنـواع الدليـل الرقمـي المستمد من الجرائم الماسة بالوثائق البيومترية

عند تطرقنا للتعريف بالدليل الرقمي، يتجلى لنا أن الأدلة الالكترونية التي يجوز ضبطها في الجريمة المعلوماتية بصفة عامة والجرائم الماسة بالوثائق البيومترية الإلكترونية بصفة خاصة والتي لها قيمة خاصة في إثبات جرائم الحاسبة الالكترونية ونسبتها إلى المتهم تتمثل في أدلة ناتجة أن الكمبيوتر وملحقاته كالورق، جهاز الحاسوب وملحقاته وأنواع أخرى للأدلة الالكترونية ناتجة بواسطته استعمال الكمبيوتر.

أولا: الأدلـــــــة الورقيـــــــة

كثير من الجرائم الواقعة على المال أو على جسم الإنسان تترك خلفها درا كبيرا من الأوراق والمستندات الرسمية، إلا أن وجود أجهزة الحاسب تجعل كثيرا من المعلومات يمكن حفظها في الحاسب الآلي، مما قلل حجم الأوراق والملفات، ومع ذلك نجد أن الكثير من المستخدمين يقومون بطباعة المعلومات بهدف المراجعة، أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات موضوع الجريمة، وأجهزة الحاسوب والطابعات المتطورة ذات السرعة العالية تطبع

[1]– شرف الدين وردة، الإثبات الجنائي بالأدلة الالكترونية، المرجع السابق، ص07.

عددا كبيرا من الأوراق في وقت قصير، لذلك يعتبر الورق من الأدلة التي يجب الاهتمام بها وتفتيش مسرح الجريمة، والورق أربعة أنواع:[1]

- أوراق تحضيرية يتم إعدادها بخط اليد كمسودة أو تصوير للعملية التي يتم برمجتها.

- أوراق تالفة تتم طباعتها للتأكد، ومن ثمإلقاؤها في سلة المهملات.

- أوراق أساسية وقانونية محفوظة في الملفات العادية أو دفاتر الحسابات وتكون لها علاقة بالجريمة خاصة عند تلقيها أو تزوير بياناتها لتنفيذ جريمة الحاسوب.

ثانيا: جهاز الحاسب الآلي وملحقاته

وجود جهاز الحاسوب مهم للقول بأن الجريمة جريمة حاسب ألي وأنها مرتبطة بالمكان أو الشخص الحائز على الجهاز، ولأجهزة الحاسوب أشكال وأحجام، فان خبير الحاسب الآلي يستطيع أن يتعرف على الحاسب الآلي ومواصفاته بسرعة فائقة، كما يستطيع تمييزه عن الأجهزة الالكترونية الأخرى وتحديد طريقة التعامل معه في حالة الضبط والتحرير.

وجهاز الحاسب الآلي يتكون من المكونات المادية، وهذه المكونات وسيلة لإدخال الأوامر، والقدرة على استقبال النتائج من هذا الحاسب، وهذه المكونات هي:[2]

1- وحدات الإدخال:

وهي الوحدات التي تمكن للشخص من خلالها إدخال البيانات أو الأوامر، وبمعنى أخر لا يمكن للمجرم المعلوماتي ارتكاب جريمته عن طريق الحاسوب إلا باستخدام هذه الأدوات والتي يمكن بمقتضاها تغذية الحاسوب بالبيانات أو المعلومات التي يريد تزويدها أو تخزينها فيه، أو يعدل تلك المعلومات والبيانات المحفوظة على الجهاز أو المسجلة لدى شبكة المعلومات

[1]- محمد الأمين البشري، **التحقيق في جرائم الحاسب الآلي والانترنت**، مقال منشور ضمن المجلة العربية للدراسات الأمنية والتدريب، المجلد 15، العدد 30، تصدرها أكاديمية نايف للعلوم الأمنية، 1421هـ، ص361.

[2]- عبد الفتاح بيومي حجازي، المرجع السابق، ص18، أنظر كذلك: شرف الدين وردة، الإثبات الجنائي بالأدلة الالكترونية، المرجع السابق، ص ص11، 14.

الدولية، وهذه الوحدات هي:(الفأرة، مشغل الأقراص الممغنطة، الماسح الضوئي، مشغل الأسطوانات).

2-وحدات المعالجة المركزية:

ووظيفة هذه الوحدات تلقي الأوامر عن طريق أجزاء الإدخال ثم معالجتها وإخراجها بالكيفية التي يريدها مستعمل الجهاز، حتى ولو كان مجرما معلوماتيا، فجهاز الحاسوب يتعامل مع معلومة أو بيان بغض النظر عن الشخص الذي يتول تشغيل الجهاز أو بطلب البيان، وهذه الوحدات هي: (وحدة الذاكرة الرئيسية، وحدة الحساب والمنطق، وحدات التحكم).

3- وحدات الإخراج:

وهي الوحدات التي من خلالها يمكن للمجرم المعلوماتي أو لأي شخص إخراج النتائج وإظهارها بأشكال مختلفة (مرئية، مطبوعة، مسموعة) ومن أمثلة هذه الوحدات: (الطابعات، الشاشات، مشغل الأقراص...).

4- وحدات التخزين:

وتعد من أهم أجزاء الحاسوب، لأنها تضم المعلومات والبرامج التي يعتمد عليها المستخدم في عمله ومن خلال أجزائها، يمكن لمستخدم الجهاز تخزين الملفات التي يقوم بعملها، وذلك على برامج التشغيل المختلفة.

وهذا الجزء هام جدا لاقتراف الجريمة المعلوماتية، إذ باقتحام الملفات المخزنة يمكن الحصول على ما يريد من البيانات أو المعلومات أو تخريب هذه المعلومات أو تدميرها أو تزييفها أو تزويرها.

5- المودم:

وهو الوسيلة التي تمكن أجهزة الحاسوب من الاتصال ببعضها البعض عبر خطوط الهاتف، وقد تطورت المودم لتكون أجهزة إرسال واستقبال فاكس، والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها.

المطلب الثاني: شروط قبول القاضي الجزائي للأدلة الرقمية الناتجة عن الجرائم الماسة بالوثائق البيومترية الالكترونية

لا تقف الصعوبات التي تواجه الدليل الإلكتروني عند كيفية جمعه وحفظه، بل تمتد إلى مدى القوة الثبوتية التي يتمتع بها هذا الدليل، ومدى حرية القاضي في الاقتناع به، لبناء الحكم على أساسه بالبراءة أو الإدانة[1]، إلا أن حرية القاضي الجزائي في تقدير الأدلة الجنائية بصفة عامة والأدلة الرقمية بصفة خاصة، تختلف بحسب نظام الإثبات المتبع في الدولة، بين نظام **الإثبات المقيد أو القانوني**، وهو نظام متبنى في الدول الإنجلوسكسونية، ووفقا لهذا المذهب، فإن المشرع يحدد سلفا طرقا محددة للإثبات، لا يمكن اللجوء لغيرها لإثبات الحق، كما أن المشرع هنا يحدد قيمة كل دليل في الإثبات، ولذلك يكون دور القاضي سلبيا، فهو يكتفي بجمع الأدلة المقدمة وترجيح واحدة على الأخرى حسب القيمة القانونية لكل دليل[2]، كما أن دور القاضي في هذا النظام هو دور ثانوي، فهو يقتصر على فحص مدى توفر الأحكام القانونية المتعلقة بالإثبات والتحقق من مراعاة الشروط القانونية الممهدة للحكم، فإن لم تتوفر هذه الأحكام فإنه لا يجوز للقاضي أن يحكم بالإدانة المقررة حتى ولو كان لديه اقتناع شخصي بأن المتهم الماثل أمامه هو الشخص مقترف الجريمة[3].

و**نظام الإثبات الحر أو المعنوي:** الذي يتمثل في أن الاقتناع الشخصي هو وحده الذي يتحكم في قرار القاضي الجنائي وهذا الاقتناع لا بد أن يصدر بكل حرية من ضمير القاضي فهذا الأخير يجب أن يكون حرا من جهة في اختيار الدليل من بين الأدلة المتعددة ومن جهة أخرى حر في تقييمها أو تقديرها، وعليه فالقاضي الجزائي لا يطالب بتبيان سبب اقتناعه بدليل دون آخر، كما يستبعد كل تدخل من طرف المشرع لتقييم مسبق لهذه الأدلة[4]. أما **نظام الإثبات المختلط:** حاول هذا المذهب تجنب الانتقادات التي وجهت لكلا المذهبين السابقين،

---

[1]– محمد طارق عبد الرؤوف الحن، المرجع السابق، ص 354.

[2]– شرايش زكريا، **الوجيز في قانون الإثبات**، دراسة مدعمة بالفقه الإسلامي، دار هومة، الجزائر، 2015، ص 30–31.

[3]– محمد مروان، **نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري**، الجزء الأول، ديوان المطبوعات الجامعية، الجزائر، ص 35.

[4]– المرجع نفسه، ص 39.

ولذلك فهو يأخذ بتحديد طرق معينة لإثبات كل حق، لكنه لا يجعل دور القاضي سلبيا بل يعطي له أحقية تقدير كل دليل يقدم[1].

ورغم اختلاف مبادئ كل نظام، إلا أن هناك ضوابط معينة تحكم الأدلة الناتجة عن الحاسوب بشكل عام يلتزم بها القضاء لتحاشي سوء التصرف ولدعم حماية حقوق الأطراف أو غيرها، فمبدأ أصل البراءة وما يتفرع عنه من نتائج وآثار، يستوجب توافر شروط معينة في المخرجات الإلكترونية حتى يمكن الحكم بالإدانة ودحض قرينة البراءة وافتراض عكسها[2]، كذلك فالأدلة الإلكترونية قد توجس منها كل من الفقه والقضاء خيفة من عدم تعبيرها عن الحقيقة لإمكانية خضوع طرق الحصول عليها للتزييف والتحريف والأخطاء المتعددة، فإنه ذلك قد تطلب لزوم توافر مجموعة من الشروط قد تضفي عليها المصداقية ومن ثم اقترابها نحو الحقيقة وقبولها كأدلة إثبات في المواد الجنائية[3]،

ويمكن إجمال الشروط الواجب توافرها في الدليل الرقمي الناتج عن الجرائم المعلوماتية منها الجرائم الماسة بالوثائق البيومترية الإلكترونية في: مشروعية وسائل جمع الأدلة الإلكترونية (الفرع الأول)، مناقشة الأدلة المستخرجة من الحاسوب والإنترنت (الفرع الثاني)، يقينية الأدلة الإلكترونية (الفرع الثالث)، وللمشرع الجزائري موقف في قبول القاضي الجزائي لأدلة المستمدة من الجرائم الماسة بالوثائق البيومترية الإلكتروني (الفرع الرابع).

[1]– شرايش زكريا، المرجع السابق، ص 31.

[2]– راشد من حمد البلوشي، **الدليل في الجريمة المعلوماتية**، ورقة عمل مقدمة إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، برعاية الجمعية الدولية لمكافحة الإجرام السيبيري بفرنسا، جمهورية مصر العربية، الفترة بين 2 إلى 4 يونيو 2008.

[3]– حسين بن سعيد الغافري، المرجع السابق، ص 605.

الفرع الأول: شرط مشروعية الحصول على الدليل الرقمي المستمد من الجرائم الماسة بالوثائق البيومترية الإلكترونية

يشترط في الدليل الرقمي الجنائي عموما لقبوله كدليل إثبات أن يتم الحصول عليه بطريقة مشروعة.[1]

ووفقا للأمانة والنزاهة ذلك أنه يستلزم على القاضي الجنائي تطبيق الدليل تطبيقا سليما وأن يستمد اقتناعه من دليل رقمي مقبول، لأن محل الحرية التي يتمتع بها القاضي الجنائي هو الأدلة المقبولة وأن لا يتحصل عليه من أدلة غير مشروعة كالإكراه المادي أو المعنوي أو الغش ضد الجاني في الجرائم المعلوماتية من أجل فك الشيفرة وهو ما ذهب إليه المشرع الجزائري، إذ عبر صراحة في نص المادة "160" من ق.إ.ج. على استبعاد الأدلة الغير مشروعة وبالتالي فان الأدلة الرقمية غير المشروعة تستبعد ولا يؤخذ بها استنادا إلى القواعد العامة[2].

وعن شروط مشروعية إجراءات جمع الأدلة الرقمية في الاتفاقيات الدولية فقد نصت المادة 03 من الإعلان العالمي لحقوق الإنسان على:

(لكل الفرد الحق في الحياة والحرية وسلامة شخصه).وأضافت المادة "12" من نفس الإعلان على أنه: (لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاه أو لمحات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات)[3].

إلا أن المادة 29-02 منه أجازت إمكانية المساس بتلك الحقوق حيث نصت على: (يخضع الفرد في ممارسة حقوقه وحرياته لتلك القيود التي يقرها القانون فقط لضمان الاعتراف

[1]- خالد عياد حيلي، المرجع السابق، ص238.

[2]- بحرية هارون، المرجع السابق، ص13.

[3]-شرف الدين وردة، الإثبات الجنائي بالأدلة الالكترونية، المرجع السابق، ص39.

بحقوق الغير وحرياته واحترامها ولتحقيق المقتضيات العادلة للنظام العام والمصلحة العامة والأخلاق في مجتمع ديمقراطي)[1].

وأشارت المادة 17 من الفقرة الأولى من العهد الدولي الخاص بالحقوق المدنية والسياسية على أنه: (لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته).

الفرع الثاني: شرط مناقشة الدليل الرقمي المستخرج من الوثائق البيومترية الالكترونية

نصت المادة 02/212 من ق.إج.ج على أنه:(ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه)[2].

ويستوي الأمر بالنسبة للأدلة الرقمية سواء كانت في شكل مخرجات ورقية أو الكترونية أو معروضة بواسطة الكمبيوتر على الشاشة الخاصة به، فيجب أن تعرض للمناقشة أثناء المحاكمة بوصفها أدلة إثبات، وللقاضي الجزائي الحرية في أن يستمد قناعته منها طالما أن لها ووقعت عليها المرافعات وناقشها أطراف الدعوى، ويترتب على هذه القاعدة شرطان أساسيان هما[3]:

أ- وجوب مناقشة الدليل الالكتروني بين أطراف الدعوى.

ب- الضوابط المتعلقة بالاقتناع القاضي: إذ أن سلطة القاضي الجزائي في تقديم الأدلة الرقمية وموازنتها وفقا لما يمليه وجدانه لا يخضع في ذلك لرقابة المحكمة العليا إلا أنه مع ذلك مقيد بضرورة تأسيس اقتناعه على الجزم واليقين من غير أن يكون هذا الاقتناع مخالفا لمقتضيات العقل والمنطق السليم.

---

[1]- شرف الدين وردة، الإثبات الجنائي بالأدلة الالكترونية، المرجع السابق، ص 39.

[2]- الأمر رقم 155-66 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، المصدر السابق.

[3]-بحرية هارون، المرجع السابق، ص ص 14، 15.

الفرع الثالث: شرط يقينية الأدلة الالكترونية الناتجة عن الجرائم الماسة بالوثائق البيومترية الإلكترونية

يشترط في الأدلة المستخرجة من الوثائق البيومترية الالكترونية أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، ذلك أنه لا يمكن دحض قرينة البراءة وافتراض عكسها إلا عندما يصل القاضي الجزائري لحد الجزم واليقين،فشرط اليقين في أحكام الإدانة هو شرط عام حيث أنه سواء كانت الأدلة التي يستنتج منها تقليدية أو مستحدثة كالدليل الرقمي، لذلك أن يكون الدليل الرقمي غير قابل للشك، إذ أن هذا الأخير يفسر لصالح المتهم استنادا إلى قاعدة أن الأصل في الإنسان البراءة، فيكفي أن يشكك القاضي من صحة إسناد التهمة إلى المتهم حتى يقضي بالبراءة[1].

والقاضي لكي يصل إلى يقينية الأدلة الرقمية المجسدة، بمخرجات الكمبيوتر لابد من تطلب نوعين من المعرفة، أولهما المعرفة الحسية التي تدركها الحواس من خلال معاينة هذه المخرجات وتفحصها وثانيهما المعرفة العقلية عن طريق التحليل والاستنتاج من خلال الربط بين هذه المخرجات و الملابسات التي أحالت بها.

وهذا خاصة مع التحديات المحلية التي تواجه مكافحة الجريمة المعلوماتية و التي من بينها:

- زيادة عدد المشتركين في شبكة الانترنت (أكثر من 10 ملايين مشترك بالجزائر)، انتشار تكنولوجيا الانترنت فائق السرعة APSL. SDSL. VSAT .

- التطور التكنولوجي وظهور الانترنت اللاسلكي 3G , 4G,Wifi .[2]

[1]- عائشة بن قارة مصطفى، المرجع السابق، ص277.

[2]- بحرية هارون، المرجع السابق، ص16.

الفرع الرابع: موقف المشرع الجزائري من الدليل الرقمي المستمد من الجرائم الماسة بالوثائق البيومترية الإلكترونية

سنتناول بالحديث عن موقف المشرع الجزائري من النص على الأدلة الرقمية ثم موقفه من قبول هذه الأدلة غير المرئيةفي إثبات الجرائم الماسة بالوثائق البيومترية الإلكترونية وذلك من خلال ما يلي:

أولا: موقف المشرع الجزائري من النص على الدليل الرقمي الناتج عن الجرائم البيومترية الإلكترونية

تناول المشرع الجزائري في القانون 04/09، طرق حديثة لاستخلاص الأدلة الرقمية منها المراقبة الالكترونية والتفتيش المعلوماتي ثم الضبط المعلوماتي، وهي إجراءات ذات بعدين أولاها للوقاية من الجرائم المعلوماتية وثانيها لمكافحة الجريمة وذلك بضبط الأدلة الرقمية.فبعد الاطلاع على نص المادة 06 من القانون رقم 04/09 نجد أن المشرع الجزائري تحدث عن حجز المعطيات المفيدة في كشف الجرائم أو مرتكبيها بعد أن يتم نسخ المعطيات على دعامة تخزين وحرزها وهي شكل من أشكال الأدلة الرقمية، كما سبق بيانه، فالمشرع هنا يقصد الأدلة الرقمية.ولو أنه لم يسميها إلا أنه يحرص على تحريز الدليل الرقمي لإثبات أنه أصيل وموثوق به ويقع ضمن سلسلة الأدلة المقدمة في الدعوى.[1]

وأيضا بالرجوع إلى نص المادة 341 ق.ع الجزائري وبالضبط في مصطلح الرسالة أو الوثيقة هل المقصود بهما ما ورد على الشكل التقليدي أي على الكتابة المحمولة على الدعامة الورقية فقط؟.

من المعلوم بأن الرسالة قد تكون رسالة الكترونية كما أن مصطلح الوثائق البيومترية الالكترونية قد يحمل صور على دعامة رقمية، وبما أن المشرع لم يقيد مصطلحي الرسالة والوثائق البيومترية الالكترونية بالدعامة الورقية فلماذا لا يعتد بالدليل الرقمي الذي يكون مثلا

[1]– ناني لحسن، المرجع سابق، ص116.

عبارة عن رسالة رقمية وجدت في البريد الالكتروني للمتهم أو شريكه، يضاف إلى هذا أن التطور الحاصل جعل المجتمع بصفة عامة والمجرمين بصفة خاصة يتفادون الكتابة كونها وسيلة سهلة الاكتشاف عن طريق مضاهاة الخطوط .[1]

مما يعني أن المشرع الجزائري تبنى الأدلة الرقمية لكن بدون تسمية صريحة، وصفوة القول أن مبدأ قبول الأدلة الرقمية يجد له أساس في قانون الإجراءات الجزائية في باب طرق الإثبات أين ترك المجال مفتوحا لقبول أي دليل من شأنه إثبات الجريمة تطبيقا لمبدأ حرية الإثبات لذلك لم يجد المشرع حرجا لما وضع نصوص القانون 09-04 وجاءت خالية من ذكر الدليل الرقمي شأنه في ذلك شأن الأدلة العلمية الأخرى مثل الADN ...الخ[2].

ثانيا: موقف المشرع الجزائري من قبول الدليل الرقمي في إثبات الجرائم الماسة بالوثائق البيومترية الإلكترونية

لم يخص المشرع الجزائري نصوص صريحة تتناول كيفية قبول الدليل الرقمي مما يحيلنا إلى طرق الإثبات العامة المطبقة في قبول الأدلة والتي تخضع إلى السلطة التقديرية للقاضي عملا بنص المادة 212 ق.إ.ج. ما يجعلها مقبولة نظريا.ومنه تبقى مسألة تقييم الدليل الجنائي في إثبات الواقعة الجرمية هي مسألة موضوعية محضة، ولهذا يترك للقاضي الجنائي حرية تقدير الأدلة الجنائية وتكوين قناعته، ويبني حكمه على أي دليل متى أطمأن إليه ولو كان مستمد من محاضر الاستدلالات.[3]

وعليه يمكن القول أن المشرع سلك ما سلكه المشرع الفرنسي من خلال اعتبار الدليل الجنائي الرقمي مثل باقي الأدلة الجنائية الأخرى، وأن السلطة التقديرية التي يتمتع بها القاضي تمتد لتشمل جميع الأدلة الجنائية بما فيها الأدلة الرقمية، وبالتالي فان هذا النوع من الأدلة لا يثير إشكالا بالنسبة للمشرع الجزائري ما دام يعتنق حرية الإثبات، وللقاضي مطالب فقط باحترام

[1] – بن فردية محمد، المرجع السابق، ص281.

[2] – بحرية هارون، المرجع السابق، ص11.

[3] – سعيد أني نعيم، المرجع سابق، ص214.

القواعد العامة المتعلقة بقبول الأدلة الجنائية أمام القضاء، التي قد تأخذ شكل محاضر على اثر القيام بإجراء التفتيش أو اعتراض المراسلات مثلا، أو تأخذ أيضا شكل تقرير خبرة فنية بمناسبة معاينة أو فحص أو تحليل الأدلة الجنائية الرقمية الناتجة عن أجهزة الحاسب الآلي و ملحقاته.[1]

وعليه فإذا تعلق الأمر بالمحاضر فالمشرع الجزائري اعتبرها كقاعدة عامة مجرد الاستدلالات ما لم ينص القانون على خلاف ذلك وهو ما أوردته المادة 215 من قانون الإجراءات الجزائية بقولها: "لا تعتبر المحاضر والتقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك".[2]

كما نصت المادة 214 من نفس القانون على أنه: "لا يكون للمحضر أو التقرير قوة الإثبات إلا إذا كان صحيحا في الشكل ويكون قد حرره واضعه أثناء مباشرة أعمال وظيفته وأورد فيه عن موضوع داخل في نطاق اختصامه ما قد رآه أو سمعه أو عاينه بنفسه". إلا إن المحاضر التي يخول القانون فيها لضباط الشرطة القضائية إعدادها بنص خاص لإثبات بحجة معينة، فان هذه المحاضر تتميز بحجية ما لم يدحضها دليل عكسي، وذلك وفقا لما نصت عليه المادة 216 من نفس القانون والتي جاء فيها: "في الأحوال التي يخول القانون فيها بنص خاص لضباط الشرطة القضائية أو أعوانهم أو للموظفين وأعوانهم الموكلة إليهم بعض مهام الضبط القضائي سلطة إثبات جنح في محاضر أو تقارير، تكون لهذه الحاضر أو التقارير حجيتها ما لم يدحضها دليل عكسي بالكتابة أو شهادة شهود".[3]

وأما بالنسبة لتقارير الخبرة الفنية فان المشرع الجزائري اعتبرها كذلك مثل باقي أدلة الإثبات من خلال خضوعها للسلطة التقديرية للقاضي، وهو ما أكدته المادة 215المذكورة أعلاه.

[1]– سعيد أني نعيم، المرجع السابق، ص214

[2]– المرجع نفسه، ص 2016.

[3] المرجع نفسه، ص217.

الخاتمـــــــــة:

الخاتمـــــــــــــــــة:

تعد الحماية الجنائية الموضوعية للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية من المواضيع الحديثة وهي نوع من الدراسات المتعلقة بالمحررات والوثائق الإلكترونية، هذه الأخيرة التي عملت على تحويل الوثائق الورقية إلى وثائق الكترونية.

وللإجابة عن الإشكالية المطروحة فقد توصلنا إلى مجموعة من النتائج:

1- عملت الجزائر على الأخذ بفكرة الإدارة الإلكترونية كوسيلة لتطوير وتسيير الإدارات الجزائرية لتسهيل استخرج مختلف الوثائق والمحررات الإلكترونية لتوفير الوقت والجهد على المواطن جراء ما كان يتكبده من عناء ومشقة في ظل البيوقراطية ونظام استخراج الوثائق التقليدية الورقية، وقد تجسدت تلك الفكرة على مستوى الجماعات المحلية من خلال استصدار الوثائق البيومترية الإلكترونية والمتمثلة في بطاقات التعريف البيومترية الإلكترونية، جواز السفر البيومتري الإلكتروني وفي الطريق بطاقة السياقة الإلكترونية.

2- استحدثت وزارة الداخلية والجماعات المحلية والتهيئة العمرانية الشباك الإلكتروني كآلية تقنية تعمل على استقبال طلبات مختلف الوثائق البيومترية الالكترونية التي تعتبر وثائق لإثبات الهوية، وفقا لإجراءات قانونية وتقنية تحكمها.

3- بالنسبة للحماية الجزائية الموضوعية فقد اختلفت الدول في إمكانية تطبيق النصوص الموضوعية العقابية للجرائم التقليدية كالسرقة والإتلاف والتزوير ... على الجرائم الإلكترونية- منها جرائم الماسة بالوثائق البيومترية الإلكترونية-، فمنهم من أنكر إمكانية تطبيق هذه النصوص على هذه الجرائم، كونها تنطبق على الأموال والأشياء المادية المرئية وليست الأشياء المعنوية غير الملموسة مما أدى إلى إفلات المجرم المعلوماتي من العقاب لدى هذه الدول عملا بمبدأ الشرعية لعدم وجود نصوص عقابية صريحة تحكمها، ومنهم من عمل على التوسيع في تطبيق هذه النصوص التقليدية العقابية على الجرائم المعلوماتية لكون أن الأدلة الناتجة عنها يمكن إفراغها في وسائط تخزين وبالتالي تتحول إلى أشياء مادية يمكن لمسها،

ومن الدول من عمل على النص صراحة على إمكانية تطبيق النصوص العقابية الموضوعية التقليدية على الجرائم المعلوماتية بإضافة للركن المادي لهذه الجرائم التقليدية شرط أن ترتكب الجرائم المعلوماتية بواسطة نظم معلوماتية أو شبكة اتصالات الكترونية فنصوا على التزوير الإلكتروني والسرقة الإلكترونية والإتلاف الإلكتروني... كما فعل المشرع الإماراتي وغيرهم.

بالنسبة لموقف المشرع الجزائري فقد نص على إمكانية تطبيق النصوص العقابية التقليدية على الجرائم المعلوماتية بشرط أن تكون وسيلة ارتكابها نظم معلوماتية أو نظام اتصالات الكترونية كما جاء في المادة 2-أ من قانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تنص: على أنه يقصد بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية.

4- عنى المشرع الجزائري بتوفير حماية جنائية موضوعية فعالة للجرائم الواقعة على الوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية من خلال النصوص العقابية التقليدية المجرمة لجريمة التزوير والسرقة والإتلاف المنصوص عليها في قانون العقوبات، ومن خلال نصوص عقابية مستحدثة منصوص عليها في المواد من 394 مكرر 1 إلى 394 مكرر 7 ق.ع الخاصة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات وكذا من خلال القانون رقم 18-07 المؤرخ في 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي،

5- فيما يخص إمكانية تطبيق النصوص الإجرائية التقليدية على الجرائم المعلوماتية، فقد ثبت عمليا عدم كفاية هذه الإجراءات في التحري والتحقيق في الجرائم المعلوماتية -منها الجرائم الواقعة على الوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية-، كالتفتيش

للإمكانية تواجد الدليل الرقمي بحاسوب شخص آخر متصل بحاسوب المتهم أو وجود الدليل الرقمي المثبت لقيام الجريمة المعلوماتية بحاسوب شخص آخر خارج الدولة متصل بحاسوب المتهم وهذا المشكل لم يتطرق له قانون الإجراءات الجزائية مما يترك رجال التحري والتحقيق يقفون عاجزين عن الولوج والتفتيش في حاسوب آخر غير المذكور في إذن التفتيش أو الولوج إلى حاسوب خارج الوطن مما يمس بسيادة وأمن دولة أخرى، هذا الإشكال يؤدي بالتالي إلى ضياع الدليل الرقمي المثبت لقيام الجرائم المعلوماتية.

كما يوجد إشكال يتعلق بإجراء الضبط حيث ثبت عمليا عدم إمكانية ضبط الأدلة الرقمية بنفس طريقة ضبط الأدلة المادية وفقا لأحكام قانون الإجراءات الجزائية، وإنما تحتاج هذه الأدلة المادية طرق مختلفة للضبط عن طريق إفراغها في وسائط تخزين والحفاظ عليها من التلف وفقا لدرجة حرارة معينة ومكان خاص وإلا ضاع الدليل الرقمي المثبت لقيام الجرائم المعلوماتية – منها الجرائم الماسة بالوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية–.

لذا عمل المشرع الجزائري على إضفاء تطوير أحكام التحري والتحقيق في هذه الجرائم المستحدثة وذلك من خلال التعديل في قانون الإجراءات الجزائية بإضافة أحكام جديدة تضاف إلى الأحكام العامة للتفتيش تنطبق على جرائم الماسة بأنظمة المعالجة الآلية للمعطيات فيما يتعلق بميقات التفتيش وحضور المتهم أو غير المتهم أو من ينوبهما عملية التفتيش، وكذا عمل المشرع الجزائري على إضافة إجراءات جديدة للتحري والتحقيق تتمثل في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وإجراء التسرب، ومن خلال إصدار القانون رقم 09-04 السابق ذكره بإضافة إجراء تفتيش النظم المعلوماتية، حجز المعطيات الإلكترونية، مراقبة الاتصالات الإلكترونية، حفظ المعطيات المتعلقة بحركة المرور، جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها.

6- بالرغم من علمية الوسائل المستعملة في التحري والتحقيق للحصول على الدليل الرقمي المثبت لقيام الجرائم المعلوماتية -منها الجرائم الماسة بالوثائق البيومترية الالكترونية-، والتي تقترب إلى درجة الدقة العلمية القطعية، إلا أن تقدير هذه الطرق في الإثبات يخضع للإقناع الشخصي للقاضي الجنائي وهذا ما نصت عليه المادة 1/212 إ م.ق.إ.ج.

كما أن المشرع الجزائري لم يخص نصوص صريحة تتناول كيفية قبول الدليل الرقمي عند القاضي الجزائي مما يحيلنا إلى المادة 2/212 م.ق.إ.ج بحيث لا يسوغ للقاضي أن يبني حكمه إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه، وهو نفس الحكم الذي ينطبق على كل الجرائم مهما كان نوعها. طبعا يضاف كما هو معروف في الإثبات الجنائي من ضرورة الحصول على الأدلة بطرق مشروعة دون إكراه أو غش أو تعذيب.

7- إن البعد الإجرائي للجرائم المعلوماتية، ينطوي على تحديات ومشكلات جمة، عناوينها الرئيسية الحاجة إلى سرعة الكشف خشية ضياع الدليل وقانونية وحجية الأدلة المستقاة من بيئة معلوماتية، وهذه المشكلات كانت ولا تزال محل اهتمام الصعيدين الوطني و الدولي.

بعد أن تطرقنا إلى أبرز النتائج التي توصلنا إليها نقترح بعض التوصيات والمتمثلة في:

1- سن المشرع الجزائري على غرار غيره من التشريعات لقانون خاص بالجرائم المعلوماتية -والتي تندرج تحتها الجرائم الماسة بالوثائق البيومترية الالكترونية- يجمع كل النصوص المتفرقة المنظمة في القوانين المختلفة.

2-ضرورة التعاون الدولي لمواجهة صور سلوك المنحرف في البيئة المعلوماتية، وذلك نظرا لخطورة هذه الجرائم العابرة للحدود الوطنية، ونظرا لأن الدليل الرقمي قد يتواجد بإقليم دولة أخرى مما يصعب الحصول عليه وبالتالي ضياعه و إفلات المجرمين من العقاب.

3- التطوير المستمر في النصوص الجزائية الموضوعية والإجرائية بشكل يتناسب مع التطور السريع للجريمة المعلوماتية.

4- إدراج موضوع الجريمة المعلوماتية في المقررات الدراسية سواء في الجامعات أو معاهد التكوين الخاصة بالقضاة والمحامين لإزالة الغموض الذي يكتنف هذه الجرائم من جميع نواحيها.

ويبقى مجال البحث في هذا النوع من الدراسات مفتوحا على الدوام نظرا للوتيرة المتسارعة لتطور الجريمة المعلوماتية.

قائمة المراجع والمصادر

أولا: المصادر

أ) القوانين و الأوامر :

1- القانون رقم 03-14 المؤرخ في 2014/02/24، **المتعلق بسندات ووثائق السفر**، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 16، الصادرة في 2014/03/23.

2- القانون رقم 01-16 المؤرخ في 2016/03/06، **المتضمن التعديل الدستوري**، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 14، الصادرة في 2016/03/07.

3- القانون رقم 16-02، المؤرخ في 19 يونيو 2016، **المعدل والمتمم للقانون رقم 66-156، المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات**، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 37، الصادرة في 22 يونيو 2016.

4- القانون رقم 09-04، الصادر في 05 أوت 2009، **المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها**، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، المؤرخة في 16 أوت 2009.

5- القانون رقم 18-07 المؤرخ في 10 يونيو سنة 2018، **يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي**، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 34، المؤرخة في: 10 يونيو سنة 2018.

ب) المراسيم:

1- المرسوم الرئاسي رقم 143-17 المؤرخ في 21 رجب 1483 الموافق ل 18 أفريل 2017، **المتعلق بتحديد كيفيات إعداد بطاقة التعريف الوطنية وتسليمها**، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 25، الصادرة بتاريخ 19أفر يل 2017.

2- المرسوم التنفيذي رقم 58-16 المؤرخ في 2016/02/03، **المتعلق بشروط إعداد وا إصدار جواز السفر الاستعجالي**، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 07، الصادرة في 2016/02/07.

3- المرسوم الرئاسي رقم 02-97 المؤرخ في 1997/01/04، **يحدد شروط منح وثائق السفر الرسمية التي تسلمها وزارة الشؤون الخارجية**، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 01، الصادرة في 1997/01/05.

ج) القرارات:

القرار المؤرخ في 2011/11/26، **يحدد المواصفات التقنية لجواز السفر البيومتري الالكتروني**، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 01، الصادرة في 2012/01/14.

د) المناشير:

1- المنشور الوزاري رقم 02، المؤرخ في 21 مارس 2018، **المتضمن تأطير مسار الشباك الالكتروني الخاص بالوثائق البيومترية وطرق استغلاله.**

2- المنشور الوزاري رقم 06، المؤرخ في 05 نوفمبر 2018، **المتضمن الترتيبات التنظيمية المؤطرة للتحديثات المضافة للشباك الالكتروني لاسيما المتعلقة بإصدار رخصة السياقة البيومترية الالكترونية.**

ثانيا: المراجع

أ) الكتب :

1- أمير فرج يوسف، **الجريمة الالكترونية والمعلومات والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت**، مكتبة الوفاء القانونية، مصر، الطبعة الأولى، سنة 2011.

2- أمال قارة، **الحماية الجزائية المعلوماتية في التشريع الجزائري**، الطبعة الأولى، دار هومة للنشر والتوزيع، الجزائر، سنة 2006.

3- أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، دار النهضة، مصر، سنة 1981.

4- جعفر حسن جاسم الطائي، **جرائم تكنولوجيا المعلومات**، رؤية جديدة للجريمة الحديثة، الطبعة الأولى، دار البلدية، عمان، سنة 2007.

5- حسام محمد نبيل الشراقي، **الجريمة المعلوماتية**، دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، مصر، سنة 2003.

6- خالد ممدوح إبراهيم، **أمن الجريمة الالكترونية**، الدار الجامعية، مصر، سنة 2008.

7- خيثر مسعود، **الحماية الجنائية لبرامج الكمبيوتر**، دار الهدى، الجزائر، سنة 2010.

8- ضياء مصطفي عثمان، **السرقة الالكترونية**، الطبعة الأولى، الأردن.

9- عبد الصبور عبد القوي علي مصري، **الجريمة الالكترونية**، دار العلوم للنشر و التوزيع، مصر، الطبعة الأولى، سنة 2008.

10- عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر و الانترنت**، دار الكتب القانونية، المجلة الكبرى، سنة 2005.

11- علي عبد القادر القزهجي، **الحماية الجنائية لبرامج الحاسب الآلي**، دار الجامعة الجديدة، مصر، سنة 2011.

12- عبد الرحمان خلفي، **الإجراءات الجزائية في التشريع الجزائري والمقارن**، الطبعة الثانية، دار بلقيس، الجزائر، سنة 2016.

13- فتوح الشاذلي، عفيفي كامل عفيفي، **جرائم الكمبيوتر و حقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون**، منشورات حلبي الحقوقية، لبنان، سنة 2003.

14- محمد محمد شتا، **فكرة الحماية الجنائية لبرامج الحاسب**، دار الجناية الجديدة للنشر، مصر، سنة 2001.

15- محمود نجيب ححسني، **شرح قانون العقوبات**، القسم الخامس، دار النهضة العربية، مصر.

16- محمد أمين الشوابكة، **جرائم الحاسوب والانترنت (الجريمة المعلوماتية)**، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، سنة 2007.

17- محمد أمين الرومي، **المستند الالكتروني**، الطبعة الأولى، دار الفكر الجامعي، مصر، سنة 2007.

18- محمد خليفة، **الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن**، دار الجامعة الجديدة، مصر سنة 2007.

19- محمد مروان، **نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري**، الجزء الثاني، ديوان المطبوعات الجامعية، الجزائر، سنة 1999.

20- مبروك نصر الدين، **محاضرات في الإثبات الجنائي**، الجزء الأول، دار هومة، الجزائر، سنة 2014.

21- نهلا عبد القادر المومني، **الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع، الأردن، سنة 2008.

22- نائلة عادل محمد فريد قورة، **جرائم الحاسب الآلي الاقتصادية**، دراسة نظرية و تطبيقية، منشورات الحلبي الحقوقية، الأردن، سنة 2005.

23- نائي لحسن، **التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية (بين النصوص التشريعية و الخصوصية التقنية)**، النشر الجامعي الجديد، الجزائر، سنة 2017.

24- يونس عرب،**جر ائم الكمبيوتر والانترنت**، الجزء الأول، منشورات اتحاد المصارف العربية، الطبعة الأولى، سنة 2002.

ب) الرسائل الجامعية:

- أطروحات الدكتوراه :

1- الهام بن خليفة، **الحماية الجنائية للمحررات الالكترونية من التزوير**، أطروحة لنيل شهادة الدكتوراه في العلوم القانونية والإدارية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة باتنة، سنة 2016.

2- حنان براهيمي، **جريمة التزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة محمد خيضر بسكرة، سنة 2015.

3- شرف الدين وردة، **الإثبات الجنائي بالأدلة الإلكترونية (دراسة مقارنة)**، أطروحة لنيل شهادة الدكتوراه، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق، جامعة محمد خيضر بسكرة، سنة 2017.

4- صالح شنين، **الحماية الجنائية للتجارة الالكترونية**، دراسة مقارنة، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة تلمسان، سنة 2013.

5- عباس حفصي، **جرائم التزوير الالكتروني**، دراسة مقارنة، أطروحة لنيل شهادة الدكتوراه، جامعة أحمد بن بلة وهران 01، سنة 2015.

- **رسائل الماجستير :**

1- أمغار خديجة، **جريمة التزوير في المحررات الرسمية (دراسة تحليلية مقارنة)**، مذكرة لنيل شهادة الماجستير، كلية الحقوق، جامعة الجزائر، سنة 2014.

2- رصاص فتيحة، **الحماية الجنائية للمعلومات على شبكة الانترنت**، مذكرة لنيل شهادة الماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2011-2012.

3- سوير سفيان، **جرائم المعلومات**، مذكرة لنيل شهادة الماجستير في العلوم الجنائية و علوم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، ، 2010-2011.

4- عيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة لحاج لخضر باتنة، سنة 2013.

5- طرشي نورة، **مكافحة الجريمة المعلوماتية**، مذكرة لنيل شهادة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة يوسف بن خدة الجزائر، سنة 2007.

6- طعباش أمين، **الحماية الجنائية للمعاملات الالكترونية**، مذكرة ماجستير في القانون، تخصص قانون دولي للأعمال، كلية الحقوق، جامعة مولود معمري تيزي وزو، سنة 2011.

7- ميساء مصطفى بركات، **جرائم التعدي على المعلوماتية (الإتلاف و التزوير)**، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة لبنان، سنة 2011.

8- معتوق عبد اللطيف، **الإطار القانوني لمكافحة الجرائم المعلوماتية في التشريع الجزائري والتشريع المقارن**، مذكرة ماجستير في العلوم القانونية، تخصص قانون جنائي، جامعة باتنة، سنة 2012.

ج) المجلات :

1- بومعيزة جابر، **الاعتداء على المعطيات الآلية في الحكومة الالكترونية**، مجلة البحوث للدراسات القانونية والسياسية، العدد الثاني عشر، كلية الحقوق والعلوم السياسية، جامعة البليدة 02.

2- شرف الدين وردة، **مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية في التشيع الجزائري**، مجلة المفكر، العدد الخامس عشر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 15 جوان 2017.

3- يوسف زروق، **حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07**، مجلة معالم للدراسات القانونية والسياسية، العدد 05.

د) مواقع الانترنت :

www.interieur.gov.dz بتاريخ 2019/05/20، على الساعة 10:00.

Posts<https://m.facebook.com، بتاريخ 2019/05/23، على الساعة 11:42.

www.tribunal.dg.com، بتاريخ 2019/05/23 على الساعة 10:49.

الفهرس

المحتوى	الصفحة
شكر وعرفان	
إهداء	
مقدمة	أ-ط
المبحث التمهيدي: الإطار المفاهيمي للوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية	
المطلب الأول: مفهوم الوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية.	02
الفرع الأول: مبررات لجوء الجماعات المحلية للأخذ بفكرة الوثائق البيومترية الالكترونية.	02
الفرع الثاني: مفهوم بطاقة التعريف الوطنية البيومترية الالكترونية.	03
الفرع الثالث: مفهوم رخصة السياقة البيومترية الالكترونية.	07
الفرع الرابع: مفهوم جواز السفر البيومتري الالكتروني.	10
المطلب الثاني: مفهوم الشباك الالكتروني.	16
الفرع الأول: تعريف الشباك الالكتروني.	16
الفرع الثاني: أهداف إنشاء الشباك الالكتروني.	17
الفرع الثالث: دور مقدم طلب الحصول على الوثيقة.	18
الفرع الرابع: مهام الشباك الإلكتروني.	19

الفصل الأول: الحماية الجنائية الموضوعية للوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية في الجزائر	
المبحث الأول: مفهوم الجرائم الالكترونية المرتكبة على الوثائق البيومترية الالكترونية.	28
المطلب الأول: تعريف الجريمة الالكترونية.	28
الفرع الأول: طائفة التعريفات التي تقوم على معيار واحد.	29
الفرع الثاني: طائفة التعريفات القائمة على تعدد المعايير.	31
المطلب الثاني: خصائص الجريمة الالكترونية.	33
الفرع الأول: الطابع الدولي للجريمة المعلوماتية.	33
الفرع الثاني: صعوبة إثبات الجريمة المعلوماتية.	34
الفرع الثالث: وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات.	35
الفرع الرابع: الجريمة المعلوماتية جريمة مستحدثة.	36
المبحث الثاني: نطاق تطبيق الحماية الجنائية الموضوعية للوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية في الجزائر.	38
المطلب الأول: الحماية الجنائية الموضوعية التقليدية للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر.	38
الفرع الأول: الحماية الجنائية الموضوعية للوثائق البيومترية الإلكترونية من خلال تجريم التزوير.	39
الفرع الثاني: الحماية الجنائية الموضوعية التقليدية للوثائق البيومترية من خلال تجريم الإتلاف.	43
الفرع الثالث: الحماية الجنائية الموضوعية التقليدية للوثائق البيومترية الإلكترونية من خلال تجريم السرقة.	50
المطلب الثاني: الحماية الجنائية الموضوعية الحديثة للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر.	55

الفرع الأول: الحماية الجنائية الموضوعية الحديثة للوثائق البيومترية الالكترونية في إطار قانون العقوبات.	55
الفرع الثاني: الحماية الجنائية الموضوعية الحديثة للوثائق البيومترية الالكترونية في إطار قانون حماية المعطيات ذات الطابع الشخصي.	65
الفصل الثاني: الحماية الجنائية الإجرائية للوثائق البيومترية الإلكترونية الصادرة عن الجماعات المحلية في الجزائر	
المبحث الأول: الحماية الجنائية الإجرائية التقليدية للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر.	71
المطلب الأول: حماية الوثائق البيومترية الإلكترونية من خلال الإجراءات الجنائية التقليدية المستنبطة من الواقع أو الأشياء.	72
الفرع الأول: الانتقـــال والمعاينـــــــة.	72
الفرع الثاني: التفتيـــش والضبـــــــط.	75
المطلب الثاني: حماية الوثائق البيومترية الإلكترونية من خلال الإجراءات الجنائية التقليدية المستنبطة من تصريحات الأشخاص.	78
الفرع الأول: الشـــــــــهادة.	79
الفرع الثاني: الخبـــــــــرة.	81
الفرع الثالث: الاستجـــــــواب.	83
المبحث الثاني :الحماية الجنائية الإجرائية الحديثة للوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر.	84
المطلب الأول: حماية الوثائق البيومترية الإلكترونية من خلال الإجراءات الجنائية الحديثة المستنبطة من الوقائع أو الأشياء.	85
الفرع الأول: اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور.	85
الفرع الثاني: مراقبـــة الاتصـــالات الالكترونيـــــة.	89

الفرع الثالث: جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها.	90
المطلب الثاني: الإجراءات الحديثة المستنبطة من تصريحات الأشخاص.	90
الفرع الأول: التســــــــرب.	91
الفرع الثاني: جمع وتسجيل المعطيات المتعلقة بحركة السير.	93
الفرع الثالث: الأمر بإنتاج بيانات معلوماتية.	95
المبحث الثالث :تقدير القاضي الجزائي للأدلة الرقمية الناتجة عن الجرائم الماسة بالوثائق البيومترية الالكترونية الصادرة عن الجماعات المحلية في الجزائر.	97
المطلب الأول: مفـــهوم الـــدليل الرقمـــــي.	98
الفرع الأول: تـــــعريف الدليل الرقمـــــي.	99
الفرع الثاني: أنواع الدليل الرقمي المستمد من الجرائم الماسة بالوثائق البيومترية.	100
المطلب الثاني: شروط قبول القاضي الجزائي للأدلة الرقمية الناتجة عن الجرائم الماسة بالوثائق البيومترية الالكترونية.	103
الفرع الأول: شرط مشروعية الحصول على الدليل الرقمي المستمد من الجرائم الماسة بالوثائق البيومترية الإلكترونية.	105
الفرع الثاني: شرط مناقشة الدليل الرقمي المستخرج من الوثائق البيومترية الالكترونية.	106
الفرع الثالث: شرط يقينية الأدلة الالكترونية الناتجة عن الجرائم الماسة بالوثائق البيومترية الإلكترونية.	107
الفرع الرابع: موقف المشرع الجزائري من الدليل الرقمي المستمد من الجرائم الماسة بالوثائق البيومترية الإلكترونية.	108
الخاتمة.	112
قائمة المصادر والمراجع.	118

الفهرس.	126
الملخص.	

ملخـــــــــــــص:

إن التطور الذي تعرفه تكنولوجيا الاتصالات في الآونة الأخيرة أدى إلى قيام وزارة الداخلية و الجماعات المخلية و التهيئة العمرانية باتخاذ العديد من الإجراءات الهادفة للقضاء على الاختلالات المتسببة في تعطيل بعض مصالح المواطنين بفعل المعالجة الكلاسيكية اليدوية للملفات الإدارية و عدم الشفافية في التسيير و البيروقراطية و كثرة الوثائق المكونة للملفات و غيرها، و من جملة هذه الإجراءات استحدثت الوثائق البيومترية الالكترونية و التي تعتبر وسيلة للاتصال التدريجي من مرحلة التسيير الكلاسيكي إلى مرحلة التسيير الآلي، حيث أصبحت هذه الوثائق تحل أهمية كبيرة في إصلاح مرافق الإدارة المركزية و إدارة الجماعات المحلية.

و ترتب عن هذه الأهمية المتزايدة للوثائق البيومترية الالكترونية عدة مخاطر تقع عليها كالقيام بتزويرها مثلا، على نحو يهدد الثقة العامة فيها، مما جعل المشرع الجزائري يتجه نحو توفير حماية جزائية موضوعية و إجرائية للوثائق البيومترية الالكترونية سواء في إطار نصوص عامة في قانون العقوبات أو في إطار نصوص خاصة.

و طالما أن المشرع الجزائري، ما زال لم يضع قواعد قانونية تنظم الوثائق البيومترية الالكترونية، بشكل مستقل و قائم بذاته فان الحماية الجنائية للوثائق البيومترية الالكترونية في هذا الإطار تبقى قاصرة و غير كافية.