وزارة التعليم العالـي والبحث العلمي

جامعة العربي التبسي– تبســــــة

كلية الحقوق والعلوم السياسية

قسم: الحقوق

مذكرة مقدمة في اطار نيل شهادة: ماستر تخصص قانون جنائي وعلوم جنائية

العنوان: الحماية الجنائية للوثائق البيومترية في التشريع الجزائري

إعداد الطالبة: عبان روميسة

إشراف الأستاذة: فرحي ربيعة

الاسم واللقب	الرتبة العلمية	الصفة في البحث
أجعود سعاد	استاذ محاضر قسم ب	رئيسا
فرحي ربيعة	استاذ محاضر قسم ب	مشرفا و مقررا
بومعزة نبيلة	استاذ محاضر قسم ا	ممتحنا

السنةالجامعية:2021/2020

شكر وعرفان

إذا عجزت اليد عن المكافأة فلا يعجز اللسان عن الشكر

أولا أشكر الله المولى عز وجل وأحمده على توفيقه لي في إنجاز هذا البحث، وأنا بصدد إتمام هذا العمل لا يسعني إلا أن أتقدم بأخلص معاني الشكر لأستاذتي الفاضلة " فرحي ربيعة " التي شرفتني بقبولها الإشراف على المذكرة وعلى دعمها وتوجيهاتها القيمة رغم مشاغلها الكبيرة فجزاها الله خير الجزاء.

كما أشكر أعضاء اللجنة الموقرة لقبولهم مناقشة هذه المذكرة.

كما يسرني أن أوجه أسمى عبارات التقدير إلى جميع أساتذة كلية الحقوق الذين منحونا يد المساعدة ومهدوا لنا سبل العلم والمعرف

الإهداء

حين قالوا لمن ستهدي هذا العمل

قلت:

إلى نور قلبي وبهجة نفسي وسيدتي الفاضلة من علمتني الحب والإخلاص، من أشعر برضا ربي حين أقبل يديها: والدتي الغالية

إلى من أبصرت عيناي من نور مكتبته، من له الفضل على ورمز التضحية والعطاء، من أدين له بكل نجاح أحققه، علمني حب العلم، إلى والدي الحبيب الأستاذ الفاضل: عبان جمال

إلى عمي العقيد لطفي الذي أعتبره قدوة لي في هذه الحياة

إلى إخوتي الذين كانوا دوما لي سندا

رضا، طه ياسين، بهاء الدين، سندس، ريتاج وسجى

إلى أختي التي لم تلدها أمي ورفيقة دربي حلوها ومرها، رمز الإيثار والوفاء

"كنزة "

إلى من ساندتني وخطت معي خطواتي ويسرت لي الصعاب " خولة "

إلى كل من أحبني بصدق فدعا لي بالتوفيق والسداد.

مقدمة:

مع التطور التكنولوجي والعلمي في عصرنا الحديث حيث أصبحت حياة الإنسان سهلة بكثير مما سبق ودلك بفضل التقنيات الحديثة والتي أصبحت ركيزة أساسية تقوم عليها جل المعاملات الأمر الذي أدى إلى الانتقال التدريجي من الخدمات التقليدية الكلاسيكية إلى الخدمات الالكترونية بغية تحسين الخدمات العمومية الموجهة للجمهور ومن بين هذه الأعمال التي قامت بها الدولة الجزائرية في هذا المجال إصدار الوثائق البيومترية الالكترونية المتمثلة في بطاقة التعريف الوطنية البيومترية وجواز السفر البيومتري الالكتروني ورخصة السياقة البيومترية الالكترونية بدلا من وثائق الهوية التقليدية.

على الرغم من المزايا الهائلة التي تحققت وتتحقق بفضل تقنية المعلومات على جميع الأصعدة وميادين الحياة المعاصرة إذ أضافت المعلوماتية الكثير من الجوانب الإيجابية في حياتنا. فإن هذه الأخيرة صاحبها في المقابل جملة من الانعكاسات السلبية والخطيرة جزاء سوء استخدام هذه التقنيات واستغلالها على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر والشيء الذي استتبعته ظهور أنماط جديدة وحديثة من الاعتداءات على تلك المعلومات المخزنة في البيئة الرقمية، مما أفرز نوعا جديدا من الجرائم عرف بالجرائم الماسة بالوثائق البيومترية الالكترونية وهو موضوع دراستنا مما استدعى المشرع الجزائري إضفاء حماية قانونية لمواجهة هذا النوع من الجرائم حفاظا على أمن معلوماتها وكبح مثل هذه السلوكات الإجرامية والتي ترتكب عن طريق الأنظمة المعلوماتية.

1. الأهمية:

إن موضوع الحماية الجنائية للوثائق البيومترية الالكترونية من أهم الموضوعات سواء على الصعيد العلمي أو العملي على حد سواء :

الناحية العلمية:

تتجلى الأهمية العلمية من خلال التطرق إلى معرفة أهم الجرائم التي تمس بهذه الوثائق والوقوف على الحماية الجنائية الإجرائية ومعرفة الإجراءات المتبعة في جمع الدليل الالكتروني التي تثبت قيام الجرائم الماسة بالوثائق البيومترية الالكترونية ومعرفة خصوصية الإثبات في هذه الجرائم.

الناحية العملية:

نلخص الأهمية العملية لهذا البحث في النقاط الآتية:

- التركيز على مناحي الحماية الجنائية من تجريم وعقاب في حالة المساس بهذه الوثائق، خاصة وإن حاملي هذا النوع من الوثائق يجهلون حقوقهم أو كيفية الحفاظ عليها، نظرا لغياب نصوص قانونية واضحة تختص بهذا الشأن.
- تبيين أهم أنماط الاعتداء على الوثائق البيومترية الالكترونية
- يمكن أن يستفيد من موضوع بحثنا رجال القانون كالمحققين ورجال التحري كونهم يمكنهم التعرف على الدليل الالكتروني الذي يختلف على الدليل المادي وتبيان أهم إجراءات التحري والتحقيق المتبعة في جمع الدليل الالكتروني الناتج عن هذه الجريمة.

2. أسباب اختيار الموضوع:

2.1 أسباب شخصية:

نظرا لقلة التطرق للموضوع من قبل، لما له من أهمية بالغة اخترت الخوض في هذا الموضوع أملا مني أن أثري المكتبة القانونية بعمل ولو بسيط

يعود سبب اختياري هذا الموضوع لحداثة هذا النوع من الجرائم كونها من أكثر الجرائم تعقيدا لارتباطها بالنظام المعلوماتي.

معرفة ما إذا كان المشرع الجزائري قد وفق في إضفاء القدر الكافي من الحماية لهذه الوثائق البيومترية الالكترونية أم أن قواعده عاجزة على تحقيق ذلك

2.2 أسباب موضوعية:

لكونه موضوع حديث التزامن مع التطور التكنولوجي لوسائل الاتصال والإعلام من جهة ومن جهة أخرى نظرا لكونه من بين الجرائم الأكثر تعقيدا فيما يخص إشكالية إتيان الأدلة المؤدية إلى إدانة المتهم أو تبرئته وأن الدليل في مثل هذه الجرائم في أغلب الأحيان دليل ذو طبيعة خاصة أي ذو

طبيعة إلكترونية بالنظر إلى المحيط الذي ترتكب فيه الجريمة الماسة بالوثائق البيومترية الالكترونية.

3. أهداف الدراسة:

تسعى دراستنا الراهنة إلى تحقيق الأهداف التالية:

- معرفة مستوى الحماية التي تحظى بها الوثائق البيومترية الالكترونية في التشريع الجزائري.

- الاطلاع على أهم الإجراءات لهذه الجريمة ومكافحتها.

- التعرف على مدى حجية الدليل الإلكتروني الناتج عن ارتكاب الجرائم الماسة بالوثائق البيومترية الإلكترونية في الإثبات الجنائي.

- إزالة الغموض والتعرف على مفهوم الوثائق البيومترية الالكترونية وبيان الجرائم الواقعة عليها

- إبراز دور المشرع الجزائري في التصدي لهذه الجريمة من خلال استحداث قواعد موضوعية وأخرى إجرائية.

4. الإشكالية:

وفي سبيل إجلاء معالم الدراسة اخترت الإشكالية التالية:

هل سن المشرع ضمانات موضوعية وإجرائية لمجابهة الجريمة الماسة بالوثائق البيومترية الإلكترونية؟

للإجابة على هذه الإشكالية الرئيسة تستلزم طرح بعض التساؤلات الفرعية والتي نوردها على النحو التالي:

- ما المقصود بالوثائق البيومترية الالكترونية؟
- ما مدى كفاية النصوص العقابية التقليدي في مكافحة الجرائم الواقعة على الوثائق البيومترية؟

- ما مدى كفاية الإجراءات الجنائية التقليدية المتبعة في التحري والتحقيق في الجرائم الماسة بالوثائق البيومترية الالكترونية؟
- ما هي الإجراءات المتبعة لإثبات هذه الجريمة الماسة بالوثائق البيومترية؟ وهل تطبيق هذه الإجراءات كافيا وفعالا لإثبات هذه الجريمة؟

5. المنهج المتبع:

اعتمدنا في دراستنا لموضوع الحماية الجنائية للوثائق البيومترية على المنهج الوصفي من خلال التطرق لمفهوم الوثائق البيومترية الالكترونية ووصف كل جريمة على حدى من الجرائم الماسة بالوثائق البيومترية الالكترونية بالإضافة إلى التطرق للإجراءات الجزائية المستحدثة في إطار مكافحة الجريمة المعلوماتية في التشريع الجزائري كما استخدمنا المنهج في التعريف بالدليل الالكتروني وبيان خصائصه وأنواعه ومشروعيته واستعنا إلى جانب المنهج الوصفي بالمنهج التحليلي وذلك من خلال العمل على تحليل مختلف النصوص العقابية والإجرامية المتبعة في مكافحة الجرائم الماسة بالوثائق البيومترية الالكترونية.

6. الدراسات السابقة:

لم يتم التطرق إلى موضوع الحماية الجنائية للوثائق البيومترية كدراسة علمية سابقة بشكل أساسي إلا أنه هناك العديد من الكتب والدراسات ذات صلة بالموضوع والتي كان تأثيرها كبيرا في دعم الموضوع أشرنا إليها في قائمة المصادر والمراجع.

7. صعوبات الدراسة:

من بين الصعوبات التي واجهتها خلال إعداد موضوعنا حول الحماية الجنائية للوثائق البيومترية هو قلة المراجع المخصصة في الموضوع

حداثة الموضوع وطابعه الفني الذي يتطلب دراية علمية بنظام المعلوماتية

لم يولي المشرع الجزائري اهتماما كبيرا لموضوع الحماية الجنائية للوثائق البيومترية الالكترونية حيث لم نجد نصوص قانونية صريحة تعنى بالوثائق البيومترية الالكترونية في هذا الموضوع.

8. تصريح بالخطة:

لقد تضمنت هذه الدراسة المقدمة من فصلين حيث خصصنا الفصل الأول من هذه الدراسة بالتعرض فيه إلى ماهية الوثائق البيومترية الالكترونية ونطاق تطبيق الحماية الجنائية الموضوعية للوثائق البيومترية الإلكترونية والفصل الثاني تعرضنا الى الحماية الجنائية الاجرائية للوثائق البيومترية الالكترونية

بينما الفصل الثاني تم تخصيصه لدراسة الحماية الجنائية الإجرائية للوثائق البيومترية الالكترونية وذلك من خلال التطرق للحماية الجنائية من خلال إجراءات المتابعة للجرائم الماسة بالوثائق البيومترية، وحجية الدليل الرقمي أمام القاضي الجزائي في الجرائم الماسة بالوثائق البيومترية.

وفي آخر دراستنا ختمنا بحثنا بخاتمة تضم أهم النتائج المتوصل إليها وبعض الاقتراحات التي تقدمنا بها على سبيل إثراء موضوع الحماية الجنائية للوثائق البيومترية الالكتروني.

الفصل الأول:

الحماية الجنائية الموضوعية للوثائق البيومترية الإلكترونية

الفصل الأول

إن الجريمة ظاهرة اجتماعية في حد ذاتها مرتبطة بتواجد الإنسان والمجتمع وبتطورهما، بحيث شغلت الفلاسفة وعلماء الاجتماع وفقهاء القانون الجنائي على حد سواء وعلى مر العصور فأولو دراستها اهتماما متزايدا لاستخلاص القوانين والنظم التي تحقق العدالة وتنشر الأمن والاطمئنان، ولهذا تعتبر جريمة المساس بالوثائق البيومترية الالكترونية من أخطر الجرائم الواقعة على الأفراد كونها تهدد الحياة الخاصة بما فيها انتهاك الخصوصية لبياناتهم ومعلوماتهم الشخصية ونظرا للتطورات العلمية أصبحت هذه الجرائم ترتكب بسلاسة وذلك لسهولة الحصول على المعلومات الشخصية مما دفع بالمشرع للتدخل من أجل كبح هذه السلوكات الإجرامية والتي ترتكب عن طريق أنظمة معلوماتية لهذا سوف يتم التطرق في هذا الفصل إلى ماهية هذه الوثائق البيومترية الالكترونية في المبحث الأول، حيث تم تخصيص المبحث الثاني للحماية الإجرائية للوثائق البيومترية الالكترونية.

المبحث الأول: ماهية الوثائق البيومترية الالكترونية كمحل للحماية.

قد فرضت تكنولوجيا المعلومات والاتصال ضرورة تطوير جميع القطاعات، وأصبح إدخال تكنولوجيا المعلومات في كافة الأعمال هدف العديد من الدول التي تسعى للتقدم والرقي ومن بين إفرازات التطور التكنولوجي الانتقال التدريجي من الخدمات الكلاسيكية التقليدية إلى الخدمات الإلكترونية حيث تم إصدار الوثائق البيومترية الإلكترونية إلا أن هذه الأخيرة رافقتها العديد من الجرائم الماسة بها، مما استلزم إضفاء حماية قانونية لذلك سنتطرق في هذا المبحث إلى مفهوم الوثائق البيومترية الإلكترونية.

المطلب الأول: مفهوم بطاقة التعريف الوطنية البيومترية الالكترونية ورخصة السياقة:

تعد الوثائق البيومترية الإلكترونية من الوثائق المستحدثة، ولغرض إعطاء صورة واضحة عن بطاقة التعريف الوطنية ورخصة السياقة لابد من تسليط الضوء على تعريفهما وهذا ما سنتطرق إليه من خلال الفرع الأول تعريف بطاقة التعريف الوطنية والفرع الثاني تعريف رخصة السياقة.

الفرع الأول: تعريف بطاقة التعريف الوطنية البيومترية الالكترونية:

لم يرد لبطاقة التعريف الوطنية البيومترية الالكترونية تعريف فقهي وإنما عرفها المشرع الجزائري طبقا للمرسوم الرئاسي 17-143 وحسب المرسوم الرئاسي تعرف على أنها وثيقة هوية فردية تسلم لكل مواطن جزائري دون شرط سن[1] 17 وتحدد صلاحيتها 10 سنوات للأشخاص البالغين 19 سنة وخمس سنوات صلاحية للأطفال ابتداء من سن الخامسة بالنسبة للقصر[2] فهي مزورة برقم سري يوضع تحت مسؤولية صاحبها أو وليه الشرعي ويستعمل هذا الرمز السري من أجل الولوج إلى الخدمات الالكترونية[3] وتكون بطاقة التعريف الوطنية من نوع بيومتري إلكتروني وتحتوي على شريحتين:

---

[1] المادة 03 من المرسوم الرئاسي رقم17-143، المؤرخ في 21رجب عام 1438، الموافق 18 أفريل 2017، المتعلق بتحديد كيفيات إعداد بطاقة التعريف الوطنية وتسليمها، الجريدة الرسمية للجمهورية الديمقراطية الشعبية، العدد25، الصادر بتاريخ، 19 أفريل 2017.

[2] المادة 05 من المرسوم الرئاسي رقم 17-143، سابق الذكر.

[3] المادة 07 من المرسوم الرئاسي رقم 17-143،سابق الذكر.

- الشريحة الأولى: معلومات إدارية ومعلومات تخص صاحبها
- الشريحة الثانية: تطبيقه من أجل التحقق من صاحبها[1]

أولا: إجراءات إعداد وتسليم بطاقة التعريف الوطنية:

1- إجراءات إعدادها:

يتم إعداد بطاقة التعريف الوطنية بإيداع ملف طلبها على مستوى بلدية المقيمين، خارج التراب الوطني يتم إيداع ملف الطلب على مستوى المراكز الدبلوماسية والقنصلية، فور إعداد بطاقة التعريف الوطني وجب على صاحبها استلامها فهذا بع إبلاغه وفي حين عدم استلامها في أجل 6 أشهر من تاريخ علمه بالسحب تلغى وتتلف ويحدد ذلك بموجب قرار من الوزير المكلف بالداخلية[2]

2- إجراءات تسليمها:

يتم إجراء تسليم بطاقة التعريف الوطنية من طرف الوالي أو أي موظف آخر مؤهل في حالة مكان المواطنين المقيمين في التراب الوطني ويرفق بملف متكون من (شهادة الجنسية وشهادة إقامة سارية المفعول وصورتان شمسيتان للهوية وبالألوان متماثلتان بخلفية موحدة بدون إطار وباللون الأبيض[3]، وتسلم بطاقة التعريف الوطنية من قبل رؤساء المراكز الدبلوماسية والقنصلية أو أي موظف قنصلي في حالة ما كان المواطن مقيم خارج التراب الوطني ويرفق بملف متكون من(شهادة الجنسية، نسخة من بطاقة التسجيل القنصلية، صورتان شمسيتان للهوية وبالألوان متماثلتان بخلفية موحدة بدون إطار وباللون الأبيض[4].

مع إجبارية حضور طالب بطاقة التعريف الوطنية لالتقاط المعطيات البيومترية في حين يعفى القصر البالغون أقل من اثنتي عشرة سنة من التقاط البصمات الإصبعية[5]. وفي حالة وفاة صاحب

[1] المادة 06 من المرسوم الرئاسي، رقم 17-143، السابق ذكره.

[2] المادة 09 من المرسوم الرئاسي، رقم 17-143، السابق ذكره.

[3] المادة 11 من المرسوم الرئاسي، رقم 17-143،لسابق ذكره

[4] المادة 12 من المرسوم الرئاسي، رقم 17-143،السابق ذكره.

[5] المادة 13 من المرسوم الرئاسي رقم 17-143، السابق ذكره.

بطاقة التعريف الوطنية تبلغ البلدية أو المركز الدبلوماسي التي سجلت لديه الوفاة بغرض جعل هذه الوثيقة غير قابلة للاستعمال[1].

ثانيا: تجديد بطاقة التعريف الوطنية:

يتم تجديد بطاقة التعريف الوطنية وفقا للحالات الآتية على سبيل الحصر: في حالة ضياع أو إتلاف أو وعند بلوغ تسعة عشرة سنة في حالة تغيير المعلومات المتعلقة بالحالة المدنية لصاحبها ويكون تجديدها أيضا خلال ثلاثة أشهر تسبق تاريخ انقضاء تاريخ صلاحيتها[2].

يتكون ملف تجديد بطاقة التعريف الوطنية من:

استمارة يملؤها ويوقعها المعني أو الولي الشرعي بالنسبة للقصر وترفق بما يأتي: (بطاقة التعريف منتهية الصلاحية أو تصريح بالضياع أو الإتلاف أو السرقة وشهادة إقامة سارية المفعول وصورة شمسية للهوية حديثة وبألوان الخلفية موحدة وبدون إطار وباللون الأبيض[3].

الفرع الثاني: مفهوم رخصة السياقة البيومترية الالكترونية:

تم انجاز رخصة السياقة الجديدة وفقا لمعيار المنظمة الدولية للتقييس رقم 18013 المتعلق بوثائق الهوية حيث تتمثل في بطاقة ذات شريحة مصنوعة من مادة البوليكاربونات ذات خلفية مؤمنة وملونة بالوردي والأخضر والأبيض ذات شكل مستطيل طولها 85.6 مم وعرضها 54 مم وسمكها 0.76 مم، كما أنها من النوع البيومتري الالكتروني المقروء آليا بواسطة شريحة الكترونية ومنطقة للقراءة الأولية وتحتوي على عناصر مؤمنة لضمان الاستعمال الأمثل لها، تحتوي هذه الوثيقة على المعلومات الخاصة بهوية السائق والمعطيات البيومتريةالمرقمنة بما فيها صورته وإمضائه وبصمات أصابعه إضافة إلى المعلومات الإدارية الخاصة برخصة السياقة ، كما تحتوي الشريحة

[1] المادة 16 من المرسوم الرئاسي رقم 17-143، السابق ذكره.

[2] المادة 17 من المرسوم الرئاسي رقم 17-143، السابق ذكره.

[3] المادة 18 من المرسوم الرئاسي رقم 17-143، السابق ذكره.

الالكترونية على عنوان الرخصة، ومعلومات أخرى متعلقة برصيد النقاط، الوضعية القانونية للرخصة.[1]

أولا: ملف طلب رخصة السياقة البيومترية الالكترونية وتجديدها:

01- الوثائق المكونة لملف الطلب تتمثل في:

- تقديم طابع جبائي طبقا لقانون الطابع (المادة 144)
- صورتان شمسيتان بخلفية بيضاء

02- ملف طلب رخصة السياقة في حال تجديدها:

- استمارة تسلم من طرف مكتب رخصة السياقة بالبلدية
- رخصة السياقة المنتهية الصلاحية أو المتلفة أو تصريح بضياع الرخصة[2]
- شهادة طبية تسلم من طرف مكتب رخصة السياقة ويتم ملؤها من طبيب مؤهل
- ثلاث صور شمسية بخلفية بيضاء
- بطاقة الإقامة
- رسم الطابع الجبائي[3]

ثانيا: إجراءات معالجة الملف وتسليمها:

01.إجراءات معالجة الملف:

- آخذ المعطيات البيومترية لطالب الرخصة
- تسليم شهادة النجاح المسلمة من طرف مفتش السياقة والأمن في الطرق للمصلحة المختصة ليتم وضعها ضمن ملف تقاعدي
- معالجة الملف عبر الشباك الالكتروني بعد التأكد من هوية المعني بالأمر

[1] رزيقة مخناش، الخدمة العمومية الالكترونية على مستوى البلدية في الجزائر، مجلة الدراسات القانونية والسياسية، العدد 02، جوان 2010، جامعة محمد لمين دباغين، سطيف 2، ص 232

[2] المنشور الوزاري رقم 06 المؤرخ في 05 نوفمبر 2018 والمتضمن الترتيبات التنظيمية المؤطرة للتحديثات المضافة للشباك الالكتروني لاسيما المتعلق بإصدار رخصة السياقة البيومترية ص 03، 04

[3] المنشور الوزاري رقم06، سابق الذكر ص 02.

- بعد أخذ جميع معلومات المعني بالأمر يتم تسليمه وصل استلام شهادة تأهيل مؤقتة وفي حالة ضياع يمكن للمعني بالأمر طلب استخراج نسخة ثانية لشهادة التأهيل المؤقتة[1]

02.إجراءات تسليم رخصة السياقة:

بعد إنجازها يتم إرسالها لمصالح البلدية وجب أن نقوم بالآتي:

- تبليغ المعني فورا للتقدم إلى مصالحها لاستلام رخصة السياقة
- يعني حضور المعني شخصيا لاستلامها مرفوقا بشهادة التأهيل المؤقتة
- التأكد من صحة المعلومات
- التأكد من هوية المتهم عن طريق مطابقة البصمات
- تفعيل رخصة السياقة قبل تسليمها للمضي[2]

المطلب الثاني: مفهوم جواز السفر البيومتري الإلكتروني.

إثر التطورات التكنولوجية وتحقيق الإجراءات الإدارية ثم إصدار شكل جديد لجوازات السفر المتمثل في جواز السفر البيومتري الالكتروني لهذا سوف نتطرق إلى تعريف جواز السفر البيومتري من خلال الفرع الأول والفرع الثاني إجراءاته والفرع الثالث أنواعه.

الفرع الأول: تعريف جواز السفر البيومتري الالكتروني.

يعد جواز السفر البيومتري الالكتروني وثيقة هوية سفر مؤمنة قابلة للقراءة آليا يحتوي بصفة خاصة على صورة رقمية وشريحة الكترونية مطابقة للمعايير المعتمدة من طرف المنظمة الدولية للطيران المدني[3].

الفرع الثاني: إجراءات استصدار جواز السفرالبيومتري في الجزائر.

[1] المنشور الوزاري رقم06، سابق الذكر ص 03.

[2] المنشور الوزاري رقم06، سابق الذكر ص 04.

[3] رزيقة مخناش، المرجع السابق، ص231.

تمر عملية استصدار جوازات السفر البيومترية في الجزائر بمجموعة من المراحل المختلفة التي تطلبها استصدار جواز السفر العادي والتي تم العمل بها وتوفير متطلباتها بشكل تدريجي ويمكن حصرها فيما يأتي:

أولا: آخذ موعد قبلي لإيداع الملف.

يمكن للمواطنين الاتصال هاتفيا أو الولوج للموقع الالكتروني المخصص من أجل الحصول على اقتراحات لحجز موعد وذلك من خلال تطبيق معلوماتي لتسيير المواعد، كما يمكن التنقل إلى الدائرة (إلى البلدية حاليا) المكلفة باستصدار الجوازات وحجز موعد بالطريقة التقليدية في حال محدودية الطلبات.[1]

ثانيا:استقبال الملفات.

يكلف أعوان استقبال الملفات الاطلاع على الملفات المقدمة للتأكد من مطابقتها للشروط المطلوبة، تزويد المتقدمين باستمارة طلب جواز السفر من أجل ملئها وإرفاقها بالملف، وأخيرا تأكيد المعد وتوجيه طالبي الجواز لقاعة الانتظار.

ثالثا: المراجعة.

يتم في هذه المرحلة مراجعة طلب جواز السفر من قبل الموظف المكلف من خلال التأكد من تطابق بيانات الملف مع البيانات المدونة في استمارة طلب جواز السفر، عرض طلب استخراج الجواز الكترونيا، تأكيد الإنشاء الآلي للملف ورقم الطلب ورقمنة الصورة وشهادة الميلاد وأخيرا إنشاء ووضع وصل إيداع الطلب وإرساله للمصادقة[2].

رابعا: المصادقة

يقوم العون المكلف بالمصادقة بمراقبة كتابة البيانات واستخراج وثيقة التحقيق بشكل إلكتروني.

خامسا: موافقة طالبي الجواز: حيث يتم المتابعة المرتبة للبيانات المرئية التي تمت كتابتها من قبل طالبي الجوازات وإدخال البيانات البيومترية.

سادسا:ضبط موعد لأخذ جواز السفر.

---

[1]كعواش رؤووف الإدارة الالكترونية لجوازات السفر البيومترية في الجزائر، مجلة تاريخ العلوم، العدد الثامن من الجزء الأول، كلية الحقوق والعلوم السياسية جامعة جيجل، ص330

[2]كعواش رؤوف، المرجع السابق، ص331.

يتم إرسال الطلب الكترونيا إلى الخلية التقنية بالولاية، والتي تتكفل بإرساله لوزارة الداخلية بالعاصمة للقيام بالتحقيقات اللازمة واستصدار الجواز في حال كانت نتائج التحقيقات سلبية، كما يتم تزويد طالبي الجوازات بأرقام تمكنهم من متابعة مسار طلب جواز سفرهم الكترونيا، وإعلامهم بموعد استلامه من خلال رسالة نصية على هواتفهم النقالة 3أيام قبل جمهوره.

سابعا: إحضار جواز السفر وتسليمه لطالبيه.

يتم التنقل مرتين في الأسبوع من قبل الموظفين على مستوى الولاية يجلب جوازات السفر إلى الولايات المعينة أين يتم تسجيلها ومن ثم إرسالها إلى البلديات المعينة لتوزيعها على المواطنين على المواطنين حسب المواعيد المتفق عليها.[1]

ولقد أضاف المشرع الجزائري مجموعة من الملاحظات التي يخص جواز السفر والتوصيات الخاصة بالمحافظة عليه من الآتي:

01 ـــــــ جواز السفر شخصي لا يمكن إعارته ولا يجوز إرساله عن طريق البريد.

02 ـــــــ يحتوي هذا الجهاز على شريحة إلكترونية ذات حساسية بالغة، يوصي صاحبه بالحفاظ عليها، كل عط يصيب الشريحة قد يجعلها غير صالحة للقراءة ويسبب إلغاء الوثيقة.

03 ـــــــ كل تزييف يعرض الوثيقة للإلغاء.

04 ـــــــ في حالة الضياع الجواز أو إصابته بعطب يجب على صاحبه إحضار السلطة الإدارية أو القنصلية المختصة فورا.

05 ـــــــ لا يجوز لأي مواطن أن يحوز في آن واحد أكثر من سند أو وثيقة سفر من نفس النوع[2]

الفرع الثالث: أنواع جواز السفر البيومتري.

[1] كعواش رؤوف، المرجع نفسه، ص331.

[2] المادة 08 من القانون رقم14-03 المصدر، المؤرخ في 2014/02/24، المتعلق بسندات ووثائق السفر، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد، 16 الصادر في 2014/03/23.

أولا: جواز السفر العادي.

يعتبر جواز السفر العادي وثيقة إدارية رسمية تصدر عن السلطات الجزائرية وتسمح للمواطنين الجزائريين بالتنقل من والي الجزائر بطريقة نظامية ويمنح جواز السفر لحاملي الجنسية الجزائرية الأصلية والمكتبة ويخضع مالكه للقوانين والأنظمة سارية المفعول، لقد تم التراجع عن العمل به تدريجيا لغاية سنة 2014، أين تم تعويضه بأخر بيومتري[1].

ثانيا: جواز السفر الاستعجالي.

يتم إصدار جواز السفر الاستعجالي بصفة استثنائية لفائدة المواطنين الجزائريين المقيمين في الخارج والمستعجلين لدى مركز دبلوماسي أو قنصلي وغير حائزين جواز سفر بيومتري الكتروني، الذين يضطرون للتنقل على عجل لأسباب عائلية أو مهنية أو إدارية أو صحية إلى خارج بلد إقامتهم[2]، أو المواطنين الجزائريين المقيمين في الخارج والمسجلين لدى مركز دبلوماسي أو قنصلي، الذين يوجدون في إقامة مؤقتة في بلد غير بلد إقامتهم وضاع منهم جواز السفر أو تلف أو سرق أو المواطنين الجزائريين غير المسجلين لدى مركز دبلوماسي أو قنصلي، الذين حظي ملف تسوية وضعيتهم الإدارية فيما يخص الإقامة بالقبول من طرف سلطات بلد الاستقبال، وهم في حاجة لجواز سفر ذي صلاحية جارية أو المواطنين الجزائريين الموجودين في إقامة مؤقتة في الخارج، الذي ضاع منهم جواز السفر أو تلف أو سرق، والمضطرين للالتحاق ببلد أجنبي أو أكثر قبل عودتهم إلى الجزائر، المواطنين الجزائريين المقيمين في الخارج والمسجلين لدى مركز دبلوماسي أو قنصلي الذين يوجدون في إقامة مؤقتة في الجزائر وضاع منهم جواز السفر أو تلف أو سرق أو انقضت مدة صلاحيته والمضطرين للعودة لبلد إقامتهم، المواطنين الجزائريين المقيمين في الجزائر وغير حائزين جواز سفر والمضطرين للتنقل على عجل لأسباب عائلية أو مهنية أو إدارية أو صحية لخارج التراب الوطني وتحدد صلاحيته بسنة واحدة (1) على الأكثر تسري ابتداء من تاريخ إعداده، ولا يمكن تمديدها[3].

---

[1] كعواش رؤوف، المرجع نفسه، ص330.

[2] المرسوم التنفيذي رقم 16 -58 المؤرخ في: 2016/02/03 المتعلق بشروط إعداد وإصدار جواز السفر الإستعجالي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 07، الصادر في: 07\02\2016.

[3] المرسوم التنفيذي رقم 16-58، سابق الذكر.

ثالثا: جواز السفر الدبلوماسي.

هو وثيقة سفر يخولها القانون لفئات معينة كالسفراء والقناصل العاملين خارج الوطن وإطارات الدولة والأعوان الدبلوماسية والشخصيات الوطنية والموظفين في إطار محدود وكذا الشخصيات التاريخية وأفراد عائلاتهم المخولين قانونا وبصفة مشروعة بحمل جواز السفر الدبلوماسي ويسلم جواز السفر الدبلوماسي من قبل السلطات المختصة لوزارة الشؤون الخارجية [1]

رابعا: جواز سفر المصلحة:

هي وثيقة تسلم من قبل السلطات المختصة لوزارة الشؤون الخارجية لأعضاء تقنيين وإداريين غير مصنفين دبلوماسيين بهدف إنجاز مهام محددة خارج التراب الوطني.[2]

[1] المادة 06 من القانون رقم 14-03، سابق الذكر.

[2] المادة 02 من القانون 14-03، سابق الذكر.

المبحث الثاني: الجرائم الواقعة على الوثائق البيومترية الالكترونية.

إن التطور الكبير الذي تشهده التقنيات من خدماتها المتنوعة والسريعة أدى إلى التغير الجذري في تنظيم الأعمال وطرق تداول المعلومات والوثائق من شكلها التقليدي، إلى شكلها الالكتروني وتعد بطرق إتاحتها وحفظها واسترجاعها، رغم هذا التطور التكنولوجي إلا أنه انعكس أثره وذلك بتمخض جرائم جديدة ذلك الشيء الذي استلزم سن نصوص قانونية تجرم هذه الأفعال لهذا سوف نتحدث في هذا المبحث عن الحماية الجنائية الموضوعية التقليدية للوثائق البيومترية الالكترونية في حيث يتناول الحماية الجنائية الموضوعية الحديثة في المطلب الثاني.

المطلب الأول: الجرائم التقليدية الواقعة على الوثائق البيومترية الالكترونية.

الجرائم التقليدية الواقعة على الوثائق البيومترية سوف نتناول في هذت المطلب إلى الحماية الجنائية الموضوعية في شكلها التقليدي وهذا من خلال التطرق لمدى خضوع الجرائم الواقعة على هذه الوثائق لكل من جريمة التزوير، في الفرع الأول والإتلاف تم تناوله في الفرع الثاني والسرقة في الفرع الثالث.

الفرع الأول: جريمة تزوير الوثائق البيومترية الالكترونية.

قبل التطرق إلى جريمة التزوير لابد من التعريج على تعريف جريمة التزوير التقليدية والإلكترونية.

أولا:تعريف جريمة التزوير التقليدية.

تناول الفقه التزوير في عديد من التعاريف حيث يعرف "إن التزوير هو عملية مادية وصورة 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].

وعرفه أيضا"أن التزوير هو تغيير الحقيقة، أي تغيير واقعة مع العلم بأنها تخالف الحقيقة، فهو تشتمل كل طريقة يستعملها شخص ليغش بها"، غير أن المشرع الجنائي لا يعاقب على جميع

[1]عبد العزيز سعد، جرائم التزوير وخيانة الأمانة واستعمال المزور. دار هومة، الجزائر، ط205، ص14.

الأعمال التي يراد بها غش الغير، بل يخير منها بعض الأفعال الخطيرة وعاقب عليها وأحاطها بسياج من الحماية عن طريق التغريم، وترك ما عداها في عداد أفعال الغش المدني التي لا يترتب عليها سوى التزام فاعلها بتعويض ما عساه ينشأ من فعله من الضرر، وعلى هذا فالتزوير إطلاقا يشمل فالنطاق الجنائي كثيرا من الجرائم التي ورد النص عليها في قانون العقوبات[1] وعليه فإن النصوص القانونية تشترط أن ينصب التزوير على محرر مكتوب، فهو محل الجريمة وهو المحل المراد حمايته قانونيا وهذا ما تفرضه النصوص التقليدية، وعليه فإن خصائص المحرر تتجلى في ثلاث نقاط:

01/ أن يتخذ المحرر شكلا كتابيا، ويجب إدراك مضمون المحرر بالنظر إليه أو لمسه، وإذا استحال قراءته فلا يصلح للإثبات ولا عقاب على ما احتواه من تغيير[2]

02/ أن تكون الكتابة منسوبة لشخص معين.

03/ أن يحدث المحرر أثارا قانونية، فيجب أن يتضمن المحرر محل الجريمة التزوير تعبيرا عن الإرادة وإثبات للحقيقة، فإذا لم تكن الكتابة صالحة لإحداث أثر قانوني فاستبدالها بغيرها أو تحريفها أو اصطناعها لا يعد تزويرا، فالحماية القانونية تنصب على المراكز القانونية المرتبطة بالمحرر.

04/ لا يشترط في المحرر الذي يحدث فيه التزوير أن يكون مكتوب بخط اليد، بل يصح أن تكون مطبوعة، فمن يغير الحقيقة في البيانات المكتوبة بخط اليد في عقد إيجار مطبوع، أو يوقع عليه بإمضاء أو ختم مزورها، يعاقب بعقوبة التزوير[3].

ثانيا: تعريف جريمة التزوير الالكترونية.

"هو تغيير الحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة، أو كانت مرسومة عن طريق الراسم، ويستوي في المحرر الالكتروني أن يكون مدونا باللغة أو لغة أخرى لها دلالتها، كذلك قد يتم في مخرجات ورقية شرط أن تكون

[1] بلحاج العربي، أبحاث ومذكرات في القانون والفقه الإسلامي، ديوان المطبوعات الجامعية بن عكنون، الجزائر، 1996، ص465.

[2] أمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، الطبقة الثانية، دار هومة، الجزائر، سنة 2010، ص136.

[3] أمال قارة، المرجع السابق ص136.

محفوظة على دعامة، كبرنامج منسوخ على اسطوانة وشرط أن يكون المحرر الالكتروني ذا أثر في إثبات حق أو أثر قانوني"[1].

كما عرف التزوير الالكتروني على "أنه تغيير الحقيقة في المسندات المعالجة آليا والمسندات المعلوماتية وذلك بغية استعمالها وبالتالي جريمة التزوير الالكتروني هي ارتكاب جريمة التزوير الالكتروني سواء بالدخول المشروع أو غير المشروع على النظام المعلوماتي والتعامل مع بياناته تزويرا بطرق التزوير المادية والمعنوية باستخدام الآلي وملحقاته للحصول على محرر أو وثيقة إلكترونية مزورة"[2].

ثالثا: أركان جريمة التزوير.

سوف يتم إبراز حماية المشرع الجزائري للوثائق البيومترية الإلكترونية ضد جرائم التزوير في ظل إقحامه عن تحديث التشريع العقابي ليتناسب مع التطور التكنولوجي والخصوصية التي تتمتع بها الوثائق البيومترية الالكترونية وبالتالي سوف نتطرق لارتكاب جريمة التزوير المتمثلة في الركن الشرعي، الركن المادي والركن المعنوي.

01/ الركن الشرعي:

نص المشرع الجزائري صراحة على فعل التزوير للوثائق البيومترية الالكترونية الآتية:

طبقا للمادة 20 من المرسوم الرئاسي رقم 17-143 نصت على:

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

[1] حجازي عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، 2002، ص170.

[2] قهوجي علي عبد القادر، الحماية الجنائية لبرامج الحاسب، بحث منشور مجلة الحقوق للبحوث القانونية والاقتصادية، كلية الحقوق جامعة الاسكندرية 1992، ص63.

وبالتالي المشرع الجزائري لم يدرج نص قانوني خاص بالتزوير الوثائق الالكتروني إنما تم ادراجها القوانين العامة أو التقليدية[1]

الركن الشرعي جرم التزوير طبقا لنص المادة "214" من قانون العقوبات على أنه تتمثل أفعال التزوير المادية في الطرق الآتية:

ـــ إما بوضع توقيعات مزورة.

إما بإحداث تغيير في المحررات أو الخطوط أو التوقيعات.

ـــ إما بانتحار شخصية الغير أو الحلول محلها.

ـــ إما بالكتابة في السجلات أو غيرها من المحررات العمومية أو بالتغيير فيها بعد إتمامها أو قفلها.

في هذه المادة اشترط المشرع الجزائري لقيام التزوير في المحررات الرسمية أو العمومية أن يقع فعل تغيير الحقيقة على المحرر الرسمي أو العمومي من طرف موظف عام أثناء تأدية وظيفته أو قاضى[2] في حين المادة 216 من قانون العقوبات الجزائري تشترط لقيام التزوير في المحررات الرسمية أو العمومية أن يقع جعل تغيير الحقيقة المحرر الرسمي أو العمومي من طرف أي شخص كان ما عدا الذين عينتهم المادة 215[3].

03/ الركن المادي:

يتكون الركن المادي في جريمة التزوير المحررات من النشاط المجرم والمتمثل في تغيير الحقيقة في المحرر بالطرق المنصوص عليها قانونا على نحو يترتب عليه ضرر محقق أو محتمل[4].

فبالرجوع لمواد قانون العقوبات الجزائري(المادة 214 إلى 216) نجد أن تغيير الحقيقة قد يتم بطرق مادية تترك أثرا يمكن إدارته بالحواس المجردة أو عن طريق الاستعانة بالخبرة الفنية، كما

---

[1] المادة 20 من المرسوم 17-143 السابق الذكر.

[2] المادة 214، من الأمر رقم 156/66 ،المتعلق بقانون العقوبات، ص75.

[3] المادة 216 ،من الأمر رقم 156/66 ،المتعلق بقانون العقوبات، ص76.

[4] رمزي بن الصديق، تزوير المحررات الالكترونية بين قابلية الخضوع للقواعد التقليدية وضرورة مراعاة الخصوصية، مجلة الاجتهاد للدراسات القانونية والاقتصادية، العد02، المركز الجامعي لتامنغست ،2018، ص205.

قد يتم بطرق معنوية لا تترك أثرا تدركه الحواس، يقع على مضمون المحرر ومعناه وملابساته دون المساس بمادته أو شكله فيما يتعلق بطرق التزوير المادية والتي تتمثل إجمالا في:

- وضع توقيعات مزورة.
- حذف أو إضافة أو تغيير مضمون المحرر.
- اصطناع محرر.

ووفقا لهذه الطرق يستطيع المزور أن يتدخل عن طريق اقتباس المعلومات من شبكة المعلومات الدولية، أو عن طريق أجهزة إدخال المعلومات المتصلة بالحواسيب خاصة ما يتعلق منها بلوحة المفاتيح، والماسح الضوئي، والقلم الضوئي[1].

وعن طريق استدعاء المعلومات من الشبكة الدولية، وعن طريق لوحة المفاتيح يستطيع المزور خلق محرر بأكمله ونسبته إلى غير محرره، وعن طريق القلم الضوئي يستطيع المزور وضع توقيعات مزورة، كما يستطيع عن طريق الماسح الضوئي حذف وإضافة [2]تغيير مضمون المحرر، وكذا وضع أختام وتوقيعات مزورة أما فيما يتعلق بطرق التزوير المعنوية، فمن الممكن عموما تصور وقوع التزوير في المحررات الالكترونية عن طريقها وتتمثل هذه الطرق في:

- تغيير إقرارات أولي الشأن.
- جعل وقائع مزورة في صورة وقائع صحيحة، ووقائع غير معترف بها في صورة وقائع معترف بها.
- انتحال شخصية الغير.[3]

فالمقصود بتغيير إقرارات أولي الشأن: تدوين اتفاقات أو أقوال غير التي صدرت من المتعاقدين أو ملؤها، ومن ذلك مثلا قيام الجاني (والغرض هنا أي موظف عمومي) بتغيير البيانات المدخلة في النظام المعلوماتي والمتعلقة بجواز السفر الالكتروني أو رخصة القيادة الالكترونية أثناء كتابتها على المحرر الإلكتروني على خلاف ما أملاه عليه وأقر به أصحاب الشأن أما بالنسبة جعل وقائع

[1] رمزي بن الصديق، المرجع السابق، ص207.

[2] شيماء عبد الغني محمد عطاالله: الحماية الجنائية للتعاملات الالكترونية، دار النهظة العربية، مصر، سنة 2013، ص91.

[3] رمزي بن الصديق، المرجع نفسه، ص208.

مزورة في صورة وقائع صحيحة، ووقائع غير معترف بها في صورة وقائع معترف بها، هذه الطريقة هي أتم وأشمل طرق التزوير المعنوي، إذا تستوعب مجمل طرق التزوير المعنوي الأخرى وتحويها[1]، ومن تطبيقاتها أن يعمل الموظف العمومي المختص بقيد المواليد والوفيات بإثبات بيانات كاذبة في محرر الالكتروني حال إنشائه قصد الإضرار بالغير،[2] كما يمكن وقوع التزوير المعنوي بانتحال شخصية الغير حال الاستيلاء على بطاقة ائتمان تخص الغير، وقيام الجاني في استخدامها للحصول على السلع والخدمات منتحلا اسم وصفة صاحب البطاقة، بقي البيان بطرق التزوير المادية منها والمعنوية أنها طرق مذكورة على سبيل الحصر[3].

1/ الركن المعنوي:

تتطلب جريمة تزوير المحررات الالكترونية منها والتقليدية توافر القصد الجنائي العام والخاص، غير أن التشريع العقابي الجزائري (شأنه في ذلك شأن بعض التشريعات المقاربة كالتشريع العقابي الفرنسي الحالي) لم ينص صراحة على ضرورة توافر هذا الركن، إلا أنه ذلك ظاهر من طبيعة الركن المادي لهذه الجريمة، وإذ يتم على نحو عمدي يتوجه فيه إرادة الفاعل لتغيير الحقيقة على نحو يحدث ضرر[4].

أولا/ القصد الجنائي العام: يقتضي القصد الجنائي العام إدراك الجاني لكافة عناصر الواقعة الإجرامية لأن العناصر ذات الأهمية القانونية في تكوين الجريمة، ومن ذلك علم الجاني بأنه يغير الحقيقة، لعدم إدراكه لها، أو لاعتقاده أن ما دونه هو الحقيقة عينها.

ومن ذلك أيضا علم الجاني المفترض بأن تغيير الحقيقة قد تقع في محرر يحظى بالحماية القانونية، وأن هذا التغيير قد حصل بالطرق المحددة قانونا، هذا إذا كان القانون قد نص عليها تحديدا وخلافا للاتجاه الحديث في التشريعات المقارنة التي تخلت عن منهج التعداد الحصري لطرق التزوير فهذا العلم ــ كما ذكر ــ علم مفترض " تعترضه طبيعة الأشياء ويتلازم مع توافر التمييز لدى المتهم"

[1] المرجع نفسه، ص209.

[2] أحمد عاصم عجيلة، الحماية الجنائية للمحررات الالكترونية، دار النهضة العربية القاهرة، مصر، سنة 2014، ص88.

[3] حجازي عبد الفتاح بيومي حجازي، المرجع السابق، ص214.

[4] رمزي بن الصديق، المرجع نفسه، 213.

كما تفترضه القواعد العامة للتجريم، فالعلم بقواعد التجريم معترض على نحو لا يقبل إثبات العكس[1].

كما يتطلب القصد الجنائي العام علم الجاني بآن من شأن تغييره للحقيقة أن يحدث ضررا، ولو على وجه الاحتمال.

فإذا كان الجاني على علم بهذه العناصر، ومع ذلك اتجهت إرادته الآثمة إلى تغيير الحقيقة وإلى اشتمال المحرر على البيانات المزورة اكتمل القصد الجنائي العام[2].

ثانيا/ القصد الجنائي الخاص:

إن القصد العام وحده غير كاف لقيام الركن المعنوي في الجريمة محل الدراسة، وإنما يتطلب إلى جانبه قصدا خاصا،(أي أن يتكون الفاعل قد ارتكب الجرم بنية خاصة)، وقد اختلف الفقهاء في تحديده، فيرى شوفو وهيلي (Chauveau et hélié) أن هذا القصد الخاص يتمثل في نية الإضرار بالغير، بينما ينتقد جارو هذا التطبيق في دائرة القصد الجنائي، ويرى أن القصد المطلوب هو نية الغش، ولا محل لاشتراط شيء غير ذلك، فالنية الخاصة التي يتطلبها القانون في نظر جارو هي نية الاحتجاج بالمحرر المزور على أمر لليس للمزور حق فيه، وهذا هو الرأي الراجح في نظر الفقه، وهو أيضا ما نصت عليه التشريعات.

فإذا اختلفت هذه النية انتفىالقصد الجنائي، ويمثل لذلك الدكتور محمود نجيب حسني بمن يريد من خلال (اصطناع كمبيالة مزورة توضيح الشكل الذي يتطلبه القانون في الكمبيالات، أو إثبات مهارته في التقليد، أو مجرد المزاح، والغرض أن نيته متطرقة عن الاحتجاج بالكمبيالة المزورة على من زورت عليه، فالقصد الجنائي منتف في هذا المثال[3]

خلاصة ما يتعلق بهذا الركن أن قواعده المطلوبة في تزوير المحررات الالكترونية لا تخرج عما تقرر في قواعده العامة المطلوبة في جريمة تزوير المحررات التقليدية.

---

[1]محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية القاهرة، مصر، الطبعة الرابعة، سنة 2012، ص309.

[2]رمزي بن الصديق، المرجع نفسه، ص،ص 213- 214.

[3]محمود نجيب حسني، المرجع السابق، ص311 .

الفرع الثاني: جريمة إتلاف الوثائق البيومترية الإلكترونية.

إن إتلاف المعطيات في المجال المعلوماتي عبر شبكة الانترنت، يتمثل بالاعتماد على سير نظام المعالجة الآلية للمعطيات وذلك بمختلف التصرفات التي يقوم بها الجاني سواء كان ذلك باستعمال الطرق الفنية أو استعمال وسائل أخرى تؤدي في كلا الحالتين إلى إتلاف المعطيات المعلوماتية، لذا سوف نتطرق إلى تعريف الإتلاف وأركان جريمة الإتلاف من خلال الآتي:

أولا: تعريف الإتلاف.

يعرف الإتلاف "على أنه الإفناء لمادة الشيء أو قيام بإحداث تغييرات عليها، بحيث تصبح غير صالحة للاستعمال في الغرض الذي أنشأ لها وبالتالي تضيع القيمة المادية لهذا الشيء على المالك"[1].

ويقصد به أيضا "التأثير على مادة الشيء مضمونه وذلك بأن يقلل أو يزيل من قيمته وفعل الإزالة يكون بالانتقال من كفاءته لأوجه الاستعمال المخصصة لها"[2].

أما الإتلاف الإلكتروني يعرف بأنه هو" إتلاف المعلومات في مجال المعلوماتية بالاعتداء على الوظائف الطبيعية للحاسب الآلي، وذلك بالتعدي على البرامج والبيانات المخزنة والمتبادلة بين الحواسيب وشبكاته، وتدخل ضمن الجرائم الماسة بسلامة المعطيات المخزنة ضمن النظام المعلوماتي، ويكون الإتلاف العمدي للبرامج والبيانات كمحوها أو تدميرها إلكترونيا، أو تشويهها على نحو يجعلها غير صالحة للاستعمال"[3].

ثانيا: أركان جريمة الإتلاف.

---

[1] عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها، د.ط، الكتاب 2، دار الفكر الجامعي الاسكندرية، 2004، ص329.

[2] محمد حماد مرهج الهيتي، جرائم الحاسوب، ماهيتها، موضوعها، أهم صورها والصور التي تواجهها، ط1، دار المناهج، عمان، 2006، ص197.

[3] أحمد بن مسعود، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، العدد الأول، جامعة الجلفة، 2017، ص486.

إن جريمة إتلاف المعطيات المعلوماتية لا تتحقق إلا بتوافر الأركان العامة لأية جريمة (الركن المادي والمعنوي) وبالتالي لا يمكن تطبيق نصوص جزائية على جريمة الإتلاف التقني إلا بتوافر شروط معينة تسمح بذلك ، وبالتالي سنتناول أركان جريمة الإتلاف المعطيات المعلوماتية.

01/ الركن الشرعي:

نصت المادة 120من قانون العقوبات: من خلال استقراء نص المادة يلاحظ في حالة ما تم إتلاف أو إزالة وثائق أو سندات أو عقود أو أموال منقولة، من طرف قاضي أو موظف أو الضابط العمومي فإنه يعاقب بالحبس من سنتين إلى عشر سنوات وغرامة من 20000.00دج إلى 100000.00دج[1].

أما بالنسبة لنص المادة 407 من قانون العقوبات فإنه في حالة ما تم تخريب أو إتلاف عمدا الأموال الغير منصوص عليها في 396 يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 20000.00 إلى 100000.00دج وهذا دون الإخلال بأحكام المادة 395 إلى غاية 404 ق العقوبات[2].

عالج المشرع أيضا هذا النط من الجرائم من خلال نص المادة 394 من قانون العقوبات التي تنص على أنه:" يعاقب بالحبس من سست (06) أشهر إلى ثلاث (03) سنوات وبغرامة مالية من 5000.00دج إلى 20.000.00دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.[3]

02/ الركن المادي:

يستخلص الركن المادي لجريمة الإتلاف للمعطيات ثلاثعناصر:

أ/ السلوك الإجرامي:

[1] المادة 120 من الأمر رقم66-156، المتعلق بقانون العقوبات، ص52.

[2] المادة 407 من الأمر رقم66-156، المتعلق بقانون العقوبات، ص144.

[3] المادة 394 مكرر من الأمر رقم66-156، المتعلق بقانون العقوبات، ص139.

إن فعل الإتلاف في المجال المعلوماتي يمكن أن يمتد إلى المكونات المادية (الشاشة، لوحة المفاتيح ...) أو يكون على المعلومات المعنوية للنظام المعلوماتي (المعطيات، البرامج، المعلومات)

وفي كلا الحالتين يتمثل السلوك الاجرامي الذي يقوم به الجاني في تخريب الأموال سواء كانت مادية أو معنوية وجعلها غير صالحة للاستخدام سواء كان الإتلاف تاما أو جزئيا[1].

ويتمثل سلوك الجاني في إتلاف المكونات المادية للنظام المعلوماتي (لوحة المفاتيح والشاشة، وحدات الإدخال) بتخريبه أو تعطيله أو بجعله غير صالح للاستعمال[2]

أما بالنسبة للسلوك الإجرامي في إتلاف المكونات المعنوية(المعطيات المعلومات البرامج) فيتمثل في ثلاث عناصر وهي المحو والتعديل غير المشروع للمعطيات أو الإدخال غير المشروع للمعطيات بحيث يكون هذا الإتلاف معيبا لكل أو لجزء من النظام المعلوماتي[3].

ب/ النتيجة:

تتطلب هذه الجريمة أن يترتب على الدخول أو البقاء في نظام المعالجة للمعطيات إحدى النتائج الثلاث وهي المحددة على سبيل الحصر بالمادة 394 مكرر من قانون العقوبات وهي:

- حذف المعطيات ويتم ذلك بإزالتها كليا عن طريق المحو والإلغاء.

- تغيير المعطيات وهو المساس بالحالة الأصلية بحيث لا تبقى على ما كانت عليه بالقيام بعمليات عشوائية غير مدروسة.

- تحديد نظام التشغيل بجعله غير قابل للاستعمال وأداء ما وضع من آجله كما ولا يؤدي وظيفته.

ج/ العلاقة السببية:

يكفي لتحقق الجريمة أن تكون هناك علاقة سببية بين الدخول والبقاء الغير الشرعي وبين النتيجة التي تحققت وهي محو النظام أو عدم قدرته على أداء وظيفته أو تعديل البيانات[1] فلابد من وجود

[1] أمين طعباش،الحماية الجنائية للمعاملات الالكترونية ط 1، مكتبة الوفاء القانونية، الإسكندرية، 2015، ص 76

[2] هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص564.

[3] أمين طعباش، المرجع السابق، ص 78

علاقة سببية فإن حدثت إحدى هذه النتائج نتيجة فعل أخر فلا تكون أمام هذه الصورة المشددة من الجريمة بل البسيطة لتحقق فعل الدخول أو البقاء فقط، فإذا أثبت الجاني انتفاء العلاقة السببية بين فعله والنتيجة التي تحققت لم تقم الجريمة كتدخل عامل أخر، حادث مفاجئ أو قوة قاهرة[2].

وبالتالي إن 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[3].

03/ الركن المعنوي:

جريمة الإتلاف المعلوماتي هي جريمة إتلاف عمديه، حيث تتطلب أغلب التشريعات لقيامها القصد العام، أي علم الجاني بأن ما يقوم بفعله من شأنه أن يؤدي إلى إتلاف المعلومات أو تعديلها مع اتجاه إرادته إلى ارتكاب هذا الفعل، أما التشريعات التي تطلبت قصدا خاصا يتمثل في نية تحقيق الربح أو الإضرار بالغير، كالتشريع البرتغالي والتركي فقد تعرضت لانتقاد بعض الفقهاء، وإذا أنه بتطبيق القصد الجنائي الخاص فإنه يؤدي لاستبعاد العديد من الأفعال الإتلاف وعدم تجريمها عندما أن تقدير الخسائر يجب ألا يقتصر على الأضرار المادية فقط التي تلاحق بالمجني عليه[4].

ثالثا: مدى انطباق النصوص الموضوعية التقليدية لجريمة الإتلاف على إتلاف الوثائق البيومترية.

لقد اختلفت الآراء الفقهية حول مسألة حماية المعطيات والمعلومات التي تتضمنها نظم المعالجة الآلية وتوفير نصوص خاصة بجريمة إتلاف المعطيات التقنية لما لها من أهمية كبيرة في حماية المال المعنوي من إفقاده المنفعة التي نص لأجلها، ففكرة وجودة جريمة إتلاف المعطيات التقنية ترتب عنها خلاف واسع حول انطباق النصوص التقليدية المتعلقة بالإتلاف بصورته المادية على الإتلاف باستخدام سلوك معنوي قوامه تقنية المعلومات وعليه فقد قام جدل فقهي لوقوع جريمة

---

[1] جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، (الجرائم الناشئة عن استخدام الحاسب الآلي)، دار النهضة العربية، القاهرة، 1992، ص20.

[2] جدي نسيمة، مذكرة ماجستير بعنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات، جامعة وهران، 2014، ص59.

[3] عبد الفتاح بيومي حجازي، المرجع نفسه، ص542.

[4] معتوق عبد اللطيف ، مذكرة ماجستير بعنوان الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن جامعة الحاج لخضر، باتنة، 2011، ص59.

الإتلاف على المعلومات مما يؤدي بنا إلى دراسة إمكانية تطبيق النصوص التقليدية على إتلاف المعلومات والبرامج المعلوماتية التي تمس الوثائق البيومترية وبالتالي فسنتكلم عن مدى إخضاع جريمة إتلاف المعطيات في المجال المعلوماتي على النصوص التقليدية.

ذهب الاتجاه المؤيد لإمكانية تطبيق النصوص التقليدية بجريمة الإتلاف على الوثائق البيومترية.

يرى صلاحية النصوص التقليدية لاستيعاب القوالب الجرمية المستحدثة الناشئة عن استغلال تقنية نظم المعلومات في إيقاع إتلاف المعطيات المعلوماتية حيث اشترط فيها شروط خاصة سوى أن تتحقق النتيجة ويقع الضرر وهم بذلك لا يرون مانعا لتطبيق النصوص التقليدية على الإتلاف المعلوماتي[1].

ومنه نستنتج أن هذا الاتجاه الذي تبناه الفقه التقليدي وفقا لنوع الأموال التي كانت عند إصدار النص التشريعي وعليه فإن عدم تبرير صلاحية المعطيات والمعلومات لأن تكون محل إتلاف المعطيات المعلوماتية بمقتضى النصوص التقليدية في قانون العقوبات[2].

في حين أن الاتجاه المعارض يرى لإمكانية تطبيق النصوص التقليدية لجريمة الإتلاف على الوثائق البيومترية الإلكترونية.

يرى الاتجاه الثاني من الفقه وهو الاتجاه المعارض آن جريمة الإتلاف المعطيات التقنية لا تصلح ولا تسري على النصوص التقليدية، حيث يعد هذا الاتجاه أكثر تفتحا وتفهما للطبيعة الخاصة لفعل الإتلاف التقني، وإدراكا أكثر لمعطيات الجريمة وبيئتها حيث أن أنصار النص التقليدي يتحدث عن المال المادي المنصوص عليه في الجرائم التقليدية[3].

[1] أسامة أحمد المناعسة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الإلكتروني، دراسة مقارنة ط1، دار الثقافة للنشر والتوزيع، عمان، 2014، ص126.

[2] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط1، منشورات الحلبي الحقوقية، بيروت، ى 2012، ص113.

[3] أسامة أحمد المناعسة، جلال محمد الزعبي، المرجع السابق ص، ص134-135.

حيث أن هذا الاتجاه ذهب إلى أن التوسع في تفسير النصوص التقليدية غير كاف بل يلزم الأمر توفر حماية المكونات المعنوية وذلك باستحداث نصوص تشريعية حديثة خاصة تراعي خصوصيتها والتي تختلف عن الأمور المادية الملموسة التي وضعت نصوص قانون العقوبات لاعتبارات عدة.[1]

إمكانية حماية نظم المعالجة الآلية بناء على النصوص التقليدية التي تجرم إتلاف الأموال تبقى محظورة في عدة حالات تتمثل في الجانب المادي لنظام المعالجة الآلية فبالرجوع لنصوص قانون العقوبات الجزائري التي نصت على جريمة الإتلاف نجد أن الاعتداء على الكيان المادي لنظام المعالجة الآلية يمكن إخضاعه على نص المادة (412) قانون العقوبات الجزائري التي قامت بتحديد الأشياء التي تصلح أن تكون محلا للإتلاف وبالتالي فإن المكونات المادية لنظم المعالجة الآلية يمكن أن يخضع لهذا النص التجريمي واعتباره محلا للإتلاف سواء بوصفها أجهزة أو بضائع[2].

ويمكن إخضاعها لنص المادة 394 مكرر 1 قانون العقوبات الجزائري والتي بدورها أحالتها إلى نص المادة 407.

وعليه فإن محاولة إخضاع الاعتداء الوارد على المكونات[3] الغير المادية لنظام المعالجة الآلية إلى النصوص التقليدية غير ممكنة نظرا لطبيعتها الخاصة الغير المادية، فتجريم الإتلاف المعطيات من خلال النصوص خاصة ضرورة تقتضيها خطورة هذه الجرائم، فالعقوبات المقررة كجزاء على جريمة الإتلاف لا تتناسب مع خطورة جريمة إتلاف المعطيات المعلوماتية وما يقتضي إقرار عقوبات خاصة بها[4].

أما بالنسبة لموقف المشرع الجزائري لمدى انطباق النصوص التقليدية الموضوعية لجريمة الإتلاف على الوثائق البيومترية فإنه لم يقرر المشرع الجزائري حماية خاصة لجريمة الإتلاف الالكتروني وإنما أشار لها عندما عرفت الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، طبقا للمادة 02 الفقرة أ منه قانون رقم 09-04 المؤرخ في 05 غشت 2009، على أنها جرائم المساس بأنظمة المساس

[1] رشيدة بوكر، المرجع السابق، ص115.

[2] المرجع نفسه، ص116.

[3] المرجع نفسه، ص155.

[4] المرجع نفسه، ص155.

المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو سهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية[1].

الفرع الثالث: جريمة سرقة الوثائق البيومترية الإلكترونية.

إن المزايا التي أخذتها الثورة التقنية للمعلومات رافقها العديد من التغيرات والإشكالات القانونية حول مقدرة وكيفية تعامل النصوص العقابية التقليدية لنشاط الوسائل الالكترونية المستحدثة وما استتبعه من عجز لمعظم النصوص الجنائية في مواجهة التطور المعلوماتي وبالتالي سوف نقوم بدراسة جريمة سرقة الوثائق البيومترية من خلال تعريفها وتبيان البنيان القانوني لهذه الجريمة ثم التطرق إلى مدى انطباق النصوص الموضوعية التقليدية لجريمة السرقة على سرقة الوثائق البيومترية.

أولا: تعريف جريمة السرقة.

01/ تعريف جريمة السرقة التقليدية:

"هي أخذ مال الغير المنقول خفية أو عنوة بقصد التملك فالسرقة هي جريمة اعتداء على مال الغير بإخراجه من حيازة المالك وإدخاله في حيازة السارق دون وجه حق، ودون رضا صاحب المال أو علمه".

وجاء في تعريفها أيضا " السرقة" الاستيلاء خلسة على شيء منقول للغير مع نية التصرف كمالك لهذا الشيء"[2].

02/ تعريف جريمة السرقة الإلكترونية:

تعرف "بأنها استخدام الوسائط الحاسوبية وشبكات الانترنت لأخذ مال متقوم مملوك للغير بلغ نصابا، خفية، من حرر مثله من غير شبهة ولا تأويل".

[1] القانون رقم 09-04، الصادر في 05أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائية الديمقراطية الشعبية، العدد47.

[2] ضياء مصطفى عثمان، السرقة الإلكترونية الطبعة الأولى، الاردن دار النفائس للنشر والتوزيع ص49.

فالسرقة الإلكترونية هي الاعتداء الحاصل على الكيان المعنوي للحاسب الآلي، فيخرج عن نطاق السرقة الإلكترونية الاعتداء المادي على كيان الحاسب الآلي، فالسرقة التي تقع على الكيان المادي ليس لها ميزة خاصة تميزها بها عن جرائم أخرى وتوضيح ذلك أن سرقة الجهاز الآلي أو الطابعة المرتبطة بالجهاز أو لوحة المفاتيح لا يعطي لجريمة السرقة طابعا خاصا يميزها في الأحكام كونها وقعت على الكيان المادي للحاسب الآلي[1].

ثانيا: أركان السرقة.

بالعودة إلى تعريف السرقة فإن التعريف يتضمن الإشارة إلى موضوع السرقة بأنه المال الغير المنقولثم الركن المادي وهو فعل الاختلاس أو الآخذ دون الرضا أما الركن المعنوي فيستخلص من الأحكام العامة ويتألف من القصد العام والقصد الخاص وهو نية التملك وسوف نتناول كل ركن من هذه الأركان على النحو التالي:

1/ الركن الشرعي:

بالرجوع إلى قانون العقوبات فقد خصص المشرع الجزائري للسرقة نصوص المواد من 350 إلى 369[2]

أما بخصوص السرقة الالكترونية فإنها تحمل طابعا خاصا كونها ترد على المنقولات المعنوية وبالتالي سيوضح إذا كانت هناك إمكانية إخفاء تلك الأركان على سرقة الوثائق البيومترية الالكترونية مما أثار جدلا فقهيا في هذه المسألة نطرحها كالآتي:

الرأي المؤيد: يرى أن السرقة تتجسد في فعل الاختلاس الذي يحتوي على عنصر موضوعي وآخر شخصي، فالأول يتمثل في النشاط الإرادي الذي يؤدي إلى نتيجة بينما الشخصي يتمثل في اتجاه نية الجاني إلى تملك الشيء وحيازته، إذن ففعل الاختلاس المعلوماتي يتحقق على إثر قيام الجاني بتشغيل الجهاز والحصول على البيانات والمعلومات فنتيجة الاختلاس تتحقق بمجرد حيازة المعلومة عند طريق استحواذها أو الحصول عليها بطريقة غير مشروعة، أما العنصر الشخصي في الحيازة

[1] ضياء مصطفى عثمان، المرجع السابق، ص60.

[2] المادة 350، من الأمر 156/66، المتضمن قانون العقوبات، ص123

أي عدم رضا حائز الشيء المعلوماتية والمترتبة عن الاختلاس فمالك المعلومة أو صاحب الحق الشيء المعلوماتي المعنوي لم يرضى بالاختلاس[1]

الرأي المعارض:

يرى هذا الرأي عدم وجود إمكانية وقوع جريمة السرقة المعلوماتية لارتباط فعل الاختلاس بالمحل المادي للاختلاس في السرقة[2] إذ أن الاختلاس نسخة من برنامج أو معلومة من جهاز حاسب آلي لا يحرم صاحبها منها ولا ينقل إليه حيازتها[3].

وبالتالي يمكن القول التحجج بأن المال المعلوماتي غير قابل للسرقة وهي حجة تنافي المنطق ذلك أن التسليم بها نفي تجديد المال المعلوماتي من الحماية الجنائية مما تجعله عرضة للادعاء، وبالتالي حفاظا على المصلحة العامة وخاصة 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[4].

2/ الركن المادي:

الركن المادي لجريمة السرقة هو الاختلاس أو الأخذ ويعرف على أنه نقل الشيء أو نزعه من المجني عليه بغير علمه وبغير رضاه وإدخاله إلى حيازة الجاني إذ يلزم لقيام الركن المادي في جريمة سرقة المعلومات أن يقوم الجاني بنشاط خارجي ملموس أو فعل مادي يعبر به الجاني عن انصراف إرادته في انتهاك نظام الحماية أو أخذ تلك المعلومات الموجودة على النظام الالكتروني مع علم الجاني بما يقوم به على غير رضا المجني عليه ويتضح من خلال التعريفات السابقة أن

[1] شول بن شهرة، الحماية الجنائية للتجارة الالكترونية، أطروحة دكتوراه في علوم تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم حقوق جامعة محمد خيضر، بسكرة، ص،ص 114 – 115.

[2] معتوق عبد اللطيف، مذكرة ماجستير بعنوان الإطار القانون لمكافحة الجرائم المعلوماتية في التشريع الجزائري والتشريع النقارن، جامعة الحاج لخصر، باتنة،2011، ص35.

[3] مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة 2000، ص148.

[4] محمد أمين شوابكة جرائم الحاسوب والانترنت، (الجريمة المعلوماتية) ط1 دار الثقافة للنشر والتوزيع الأردن، 2007، ص، ص102،101.

هناك شرطين يجب توفرهما لتحقيق الاختلاس، يتلخص الشرط الأول بفعل الآخذ أي أخذ الشيء بغير رضا حائزه والشرط الآخر هو انعدام رضا المجني عليه[1]

3/الركن المعنوي:

في الجريمة الالكترونية شأنها شأن أية جريمة من الجرائم التقليدية فهي جريمة مقصودة يتخذ ركنها المعنوي صورة القصد العام والخاص فلا بد من أن ترتكب من شخص قادر على تحمل تبعة أفعاله مدرك لها ويتحقق القصد الجنائي للعام بتوفر عنصرية العلم والإرادة ويتخذ القصد الخاص نية التملك.[2]

[1] حابس يوسف ريدات، مدى استيعاب النصوص التقليدية للسرقة الالكترونية، دراسة مقارنة مجلة مركز حكم القانون ومكافحة الفساد العدد 9، دار جامعة حمد بن خليفة للنشر، 2019 ص 5

[2] حابس يوسف زيدات، المرجع السابق، ص06.

ثالثا: موقف المشرع الجزائري من سرقة الوثائق البيومترية الالكترونية:

رجوعا إلى قانون العقوبات يتضح جليا من خلال نص المادة 350 منه ليس هناك ما يمنع تطبيق تلك النصوص على الأشياء المعنوية وكون مصطلح الشيء لا يقتصر على دلالة الشيء المادي فقط بل على المعنوي ولأن المشرع الجزائري لم يحدد لنا الأشياء المعنوية هي قابلة للتملك والحيازة والنقل فهي تصلح لأن تكون محل لجريمة السرقة لأن نصوص السرقة لا تحدد صيغة الشيء محل الجريمة (مادي أو معنوي)[1]

المطلب الثاني: الجرائم المستحدثة الواقفة على الوثائق البيومترية الإلكترونية.

نظرا لخصوصية الجرائم المعلوماتية فإن القواعد التقليدية للحماية لن تجدي نفعا وذلك لا يتماشى مع التطور المستمر مما استدعى المشرع الجزائري بإعادة النظر في النصوص القانونية وذلك بإدراج الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في نصوص المواد 394 قانون العقوبات إلى 394 مكرر 7 ومن هنا سوف نقوم بدراسة في الفرع الأول في حين يتم دراسة قانون حماية المعطيات الشخصية في الفرع الثاني.

الفرع الأول: في إطار قانون العقوبات.

من أجل التصدي لظاهرة الإجرام الالكتروني ومحاولة المشرع الجزائري تدارك الفراغ التشريعي القائم في هذا المجال وعمد إلى تعديل العديد من القوانين الوطنية على رأسها قانون العقوبات تجاوبا مع التطورات الإجرامية في مجال المعلوماتية فقام بتعديل قانون العقوبات مستحدثا جملة من النصوص جرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات وهذا ما سوف يتم بيانه من خلال الآتي:

أولا: جريمة الدخول أو البقاء غير المصرح له.

01/ الركن الشرعي:

إن مبدأ الشرعية الجنائية يلزم وجود نص قانوني سابق للعمل بجرمه ويعاقب عليه حتى يتم وصفه بغير مشروع وهو مبدأ مكرس دستوريا وبالتالي فإن جريمة الدخول والبقاء غير المصرح به نصت

[1] المادة 350، من الأمر 66-156، المتضمن قانون العقوبات ص123.

عليه المادة 394[1] مكرر، وتتجسد في صورتين الأولى بسيطة وتتمثل في الدخول والبقاء بطريقة غير شرعية والصورة الثانية مشددة، وهذه الصورة هي النتيجة المحققة عن فعلا الدخول والبقاء لذلك يجب التمييز بين فعل الدخول وفعل البقاء من خلال الركن المادي[2]

2/ الركن المادي:

يقوم الركن المادي للجريمة على ثلاثة عناصر هي: السلوك أو الفعل الإجرامي والنتيجة الجرمية والعلاقة السببية بينهما فإذا اكتملت هذه العناصر أطلق عليها جريمة مادية[3].

1- النشاط الإجرامي:

يعرف السلوك الإجرامي في الجرائم التقليدية أنه فعل الجاني الذي يحدث أثر في العالم الخارجي[4].

أ) الدخول غير المصرح به (Accés non autorisé l frauduleux) يقصد به الولوج غير المشروع لنظام المعالجة الآلية للمعطيات ضد إدارة المسؤول عن النظام[5].

وتستعمل العديد من التقنيات لارتكاب جريمة الدخول غير المشروع كاستخدام البرامج الظاهرة المخصصة لتخطي أنظمة الحماية الفنية في الحالات الطارئة[6].

ولم يشترط المشرع صفة معينة في الجاني فيكفي أن يقوم أي شخص مهما كانت صفته بالولوج إلى النظام دون إذن المسؤول عن النظام، سواء كان في حالة عدم وجود تصريح أو حالة تجاوز حدود التصريح وتجدر الإشارة هنا إلى أن التجاوز المقصود هو التجاوز في المكان (المجال المكاني)[7].

---

[1] المادة 394 مكرر من الأمر 156/66، المتضمن قانون العقوبات ص139.

[2] أمال قارة، المرجع السابق، ص43.

[3] طلال آبو عفيفة، شرح قانون العقوبات، القسم العام، الطبعة الأولى، دار الثقافة، الأردن، ص242.

[4] منصور رحماني، الوجيز في القانون الجنائي العام، د.ط، دار العلوم للنشر والتوزيع، عنابة، 2006، ص94.

[5] رشيدة بوكر، المرجع نفسه، ص177.

[6] أمال قارة، المرجع نفسه، ص43.

[7] رشيدة بوكر، المرجع نفسه، ص،ص 191- 194.

ب) البقاء غير المصرح به Maintient non autorisé: يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق البقاء المعاقب عليه مستقلا عن الدخول للنظام وقد يجتمعان معا[1].

2- محل النشاط :

ما يلاحظ أن المشرع الجزائري قد اتجه نحو التشديد في حماية نظام المعالجة الآلية ومن مظاهر ذلك التوسع بالركن المادي للدخول أو البقاء بغير تصريح، حيث ينصب سلوك الجاني على المعلومات في نظام المعالجة الآلية خلال المعالجة والتخزين والاسترجاع، النظام الذي يتضمنها، فضلا عن الشبكات ذاتها أو المعلومات المنقولة عبرها[2].

3- النتيجة الإجرامية:

تنقسم الجرائم تبعا للنتيجة الإجرامية المترتبة عنها إلى جرائم مادية وجرائم شكلية يرد انتماء جريمتي الدخول والبقاء بغير تصريح إلى هذه أو تلك حسب ما إذا كانت بسيطة أو مشددة.

أ) الدخول أو البقاء المجردان إلى نظام المعالجة الآلية (الصورة البسيطة) بالرجوع إلى نص المادة (394 مكرر) من قانون العقوبات الجزائري[3]، نجد أن المشرع يعاقب على جريمة الدخول والبقاء عن طريق الغش بمجرد الدخول أو البقاء داخل النظام[4].

ب) الدخول أو البقاء المرتبان للنتيجة الجرمية (الصورة المشددة) تشدد العقوبة إذا ما ترتب عبى الدخول والبقاء إحدى النتائج التالية:

- إما حذف أو تغير المعلومات التي يحتويها النظام.

- تخريب نظام اشتغال المنظومة[1]

[1] أمال قارة، المرجع نفسه، ص46.

[2] رشيدة بوكر، المرجع نفسه، ص224.

[3] المادة 394 مكرر 01 من الأمر 66-156، المتضمن قانون العقوبات ص139.

[4] رشيدة بوكر، المرجع نفسه ص 228.

3/ الركن المعنوي.

لقيام القصد الجرمي لابد أن ينصرف علم الجاني إلى الواقعة ذات أهمية قانونية في تكوين الجريمة، والتكييف الذي تتصف به واتجاه إرادته لتحقيقها[2].

ونص القانون صراحة على كون جريمتي الدخول والبقاء جرائم عمدية بنصه في المادة (394مكرر) كل من يدخل أو يبقى عن طريق الغش[3].

ثانيا: جريمة التلاعب بمعطيات الحاسب الآلي.

هي جريمة مستقلة تضمنتها المادة 394 مكرر 1 من قانون العقوبات، وتتمثل هذه الجريمة في القيام بجملة من الأفعال التي تعتبر اعتداءات عمدية على المعطيات وهذا ما سنبينه في الآتي:

01/ الركن الشرعي:

جرم المشرع الجزائري التلاعب غير المصرح به بمعلومات النظام بموجب المادة(394 مكرر1) قانون العقوبات حيث نصت " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500000دج إلى 2000000دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات أو أزال أو عدل بطريق الغش المعطيات التي تتضمنها[4].

02/ الركن المادي:

[1]محمد خليفة، الحماية الجنائية بمعطيات الحاسب الآلي في القانون الجزائي المقارن د.ط، دار الجامعة الجديدة الإسكندرية 2007، ص161.

[2]محمود نجيب حسني، النظرية العامة للقصد الجنائي،د.ط، دار النهضة العربية القاهرة 1988 ص51.

[3]المادة 394 مكرر من الأمر 66-156 المتضمن قانون العقوبات ص139.

[4]المادة 394 مكرر1 من الأمر 66-156، المتضمن قانون العقوبات ص139.

أ/ النشاط الإجرامي: يتحقق النشاط الإجرامي في جريمة التلاعب بارتكاب واحد من الأفعال المنصوص عليها في المادة (394 مكرر1) ويكفي لقيام الجريمة أن يرتكب الجاني أحد هاته الأفعال، الإدخال، التعديل، الإزالة[1].

ب/ محل النشاط: يقتصر محل النشاط الجرمي على المعلومات الموجودة داخل النظام، أو التي يحتويها النظام وتشكل جزاء منه، ومنه فإن الحماية الجزائية تشمل المعلومات المعالجة آليا أو المعلومات في طريقها للمعالجة أو المعالجة المنفصلة عن النظام والتي أعيد إدخالها فيه، والمعلومات المسجلة في دائرة نظام المعالجة الآلية.

ج/ النتيجة الجرمية: يعتبر المشرع الجزائري جرائم الاعتداء على نظم المعالجة الآلية جرائم خطر، أي أن المشرع يستشعر خطورة الجاني من السلوك المجرد، ومنه لم يشترط تحقق نتيجة مادية محسوسة وضارة[2].

02/ الركن المعنوي:

تعد هذه الجريمة من الجرائم العمدية التي تقوم على القصد الجنائي العام بحيث يجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، مع علمه بأن هذا الفعل غير مشروع ورغما عن صاحب الحق في المعطيات أو من له السيطرة عليها مع توافر نية الغش– القصد–[3]

– القصد الجنائي العام:

جريمة التلاعب بالمعلومات من الجرائم العمدية، تتطلب القصد الجنائي العام الذي يقوم على علم الجاني بأنه يقوم بإحدى الأفعال التي جرمها النص القانوني وأن من شأن أفعاله أن تؤدي إلى النتيجة المجرمة المتمثلة في التعديل أو الإزالة أو المحو أو أن يقبل بحدوثها، وذلك تطبيقا للقواعد

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلي الحقوقية لبنان 2005 ص437.

[2] رشيدة بوكر، المرجع نفسه، ص257.

[3] صالح شنين، الحماية الجنائية للتجارة الإلكترونية – دراسة مقارنة، أطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بلقايد تلمسان، 2012، ص91.

العامة دون الحاجة للنص عليها، غير أن الفقه في غياب النص الصريح أثار جدلا واسعا بخصوص مدى وجوب توفر قصد جنائي خاص متى تقوم هذه الجريمة.

- القصد الجنائي الخاص:

بناء على المادة 394 مكرر1 ومن خلال مصطلح الغش الذي استعمله المشرع نستنتج أن الأخير اشترط أن تكون الجريمة عمدية، وهو ذات الوضع في نص المادة 323-3 من تقنين العقوبات الفرنسي، وما استقر عليه القضاء الفرنسي وكرسه في العديد من أحكامه، منها النقض الجنائي في: 08-12-1999 وبالتالي هذا الجريمة لا تتطلب أي قصد خاص[1]، لكن هناك قوانين أخرى مثل القانون البرتغالي والفنلندي والتركي تشترط قصدا خاصا لهذه الجريمة وهو نية تحقيق الربح، الأمر الذي كان محل انتقادات فقهية كبيرة كما يهمنا أن المشرع الجزائري لم يشترط صراحة القصد الجنائي الخاص[2].

ثالثا: جريمة التعامل في معطيات غير مشروعة.

قام المشرع الجزائري بتجريم جملة من الأفعال التي تتعرض لها المعلومات أيضا من خلال جريمة التعامل في معطيات غير مشروعة، حيث نصت أو عاقبت المادة 394 مكرر 2 من قانون العقوبات الجزائري وبالتالي سوف نفصل في أركان هذه الجريمة من خلال ما يلي:

01/ الركن الشرعي:

من خلال استقراء نص المادة 394 مكرر2 فقرة 1 من قانون العقوبات تم استنتاج أن كل من يقوم عمدا أو عن طريق الغش بما يأتي:

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

[1] حمودي ناصر، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الأكاديمية للبحث القانوني، العدد الثاني، جامعة أكلي محند أوحاج، البويرة، 2016، ص81.

[2] نائلة عادل محمد فريد قورة، مرجع سابق، ص223.

– حيازة أو إفشاء أو نشر او استعمال لأي غرض كان، للمعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم وبالتالي تقوم جريمة التعامل في معطيات غير مشروعة في حالة ما تم استخدام إحدى النقاط المبينة أعلاه[1].

[1] المادة 394 مكرر02 من الأمر رقم 66–156 المتعلق بقانون العقوبات، ص 139.

02/ الركن المادي:

أ/ النشاط الإجرامي:

تقوم هذه الجريمة في معلومات صالحة لارتكاب جريمة من الجرائم التي سبقت دراستها، أو التعامل في معلومات متحصلة منها، وهي كلها صورا شكلية تقع وتكتمل بمجرد اكتمال الفعل دون تطلب نتيجة معينة، لكنهما صورتان تنطويان على العديد من الأفعال وهي كالآتي:

أولا: التعامل في معلومات صالحة لارتكاب جريمة: التعامل في معطيات فعل ينطوي على العديد من الأفعال والأعمال والعمليات السابقة على المعلومات، مثل تصميمها وبحثها وتجميعها، وصولا إلى توفيرها أو نشرها أو الاتجار فيها، ويكفي أيا منها لقيام السلوك المادي للجريمة وسنبين معنى هذه الأفعال فيما يلي:

1/ تصميم: هو إعداد معلومات صالحة لارتكاب الجريمة، في العادة ما يقوم به أشخاص مختصين كمصممي البرامج، مثل تصميم الفيروسات أو برامج تمكن من الوصول لنظم المعالجة الآلية للمعطيات[1].

2/ البحث: فعل يقصد به البحث عن كيفية تصميم المعلومات وإعدادها وليس مجرد البحث عنها، أي البحث عن المعلومات من أجل تصميمها لأغراض تجريميه، مثل البحث عن الشفرات والبيانات التي تمكن من الاستيلاء على التوقيع الإلكتروني للشخص أو فك شفرات تعاملاته المالية الإلكترونية.

3/ التجميع: فعل يتمثل في القيام بجمع قدر كبير من المعلومات، يمكن أن ترتكب بها إحدى جرائم الاعتداء على نظم المعالجة الآلية للمعطيات.

4/ يقصد به عرض المعلومات وإتاحتها وجعلها في متناول الغير وتحت تصرفه وحيازته، مثل كلمات أو شفرات المرور التي تسمح بالولوج لجزء من النظام أو كله.

[1] بوكر رشيدة، مرجع نفسه، ص206.

5/ النشر: هو إذاعة المعلومات محل الجريمة وتمكين الغير من الاطلاع عليها، مهما كانت طبيعة هذه المعلومات[1] ويرى البعض أن النشر يعد من أخطر الأفعال كونه يعني نقل هذه المعلومات إلى أكبر قدر ممكن من الأشخاص.

6/ الاتجار: يعني تقديم المعلومات للغير مقابل أيا كان نوع هذا المقابل على عكس التوفير الذي قد يكون بدون مقابل، غير أنه للاتجار في مجالنامعنى يستوعب مختلف التعاملات التي يمكن تصور وقوعها على المعلومات، سواء كان ذلك بمقال أو بدون مقابل وهو ما يمكن من القضاء على الجرائم في المهد[2].

ثانيا: التعامل في معلومات متحصلة من جريمة.

أفرد المشرع الجزائري صورة ثانية من صور التعامل في معلومات غير مشروعة، تتمثل في التعامل في معلومات متحصلة من جريمة، وذلك بفعل من الأفعال التي حصرتها الفقرة الثانية من المادة 394 مكرر2 وهي الحيازة، الإفشاء، النشر والاستعمال، وهو ما لم يتضمنه لا القانون الفرنسي ولا اتفاقية بودابست، وتقوم الجريمة بأي فعل من الأفعال التي يتناول تبيان معناها باختصار:

– الحيازة: حيازة المعلومات المتحصلة من إحدى الجرائم السابقة فعل غير مشروع يعاقب من يحوزها، سواء كان ذلك بصفة دائمة أو بصفة مؤقتة، ويمكن تشبيه هذه الجريمة بجريمة حيازة أشياء متحصل عليها من جنحة أو جناية أو جنحة إخفاء أشياء مسروقة المعروفة في النصوص التقليدية لجرائم الأموال.

– الإفشاء: وهو إفشاء معلومات يكون قد تم الحصول عليها بارتكاب جريمة من جرائم الاعتداء على نظم المعالجة الآلية للمعطيات السابق تبيانها وهو فعل يفترض انتقال المعلومات من حيازة الجاني إلى غيره من الأشخاص.

[1] حمودي ناصر، مرجع نفسه، ص83.

[2] بوكر رشيدة، مرجع نفسه، ص،ص 206– 207.

– النشر: النشر شأنه شأن الإفشاء يعني اختراق النظم المعلوماتية والحصول على المعلومات منها ومن ثم القيام بإفشائها، أيا كانت وسيلة هذا الإفشاء.

– الاستعمال: استعمال المعلومات المتحصل عليها بطريق غير مشروع فعل مجرم، أيا كانت نوعية هذا الاستعمال والغرض منه، رغبة من المشرع غلق الباب أمام أي استعمال معلومات متحصل عليها بطرق مجرمة[1].

محل النشاط الإجرامي:

بموجب المادة 394 مكرر2 من تقنين العقوبات الجزائري، تم تجريم التلاعب في معلومات غير مشروعة، وبذلك تم إضفاء حماية جنائية واسعة للبيانات والمعطيات سواء كانت في طور المعالجة، أو التخزين أو الإرسال، وهو حال غالبية البيانات والمعطيات التي تتم عبر النظم المعلوماتية[2].

النتيجة الجرمية:

تنقسم الجرائم كما سبقت الإشارة إلى جرائم مادية وجرائم شكلية وتنتمي جرائم التعامل في معلومات غير مشروعة للجرائم الشكلية حيث أن المشرع الجزائري لم يتطلب لقيامها حدوث نتيجة مادية منفصلة عن النشاط الإجرامي الصادر عن الجاني[3].

الركن المعنوي:

– القصد الجنائي العام:

تقوم جريمة التعامل في معلومات غير مشروعة على القصد الجنائي العام بعنصرية العلم والإرادة، فالجاني يجب أن يكون يحيط علما بكافة العناصر التي تدخل في تكوين الجريمة أهمها علمه بأنه يتعامل في معلومات غير مشروعة، وأن هذا التعامل قد تستخدم في ارتكاب الجريمة، يتضمن وجود اتجاه إرادة الجاني إلى إثبات وتحقيق أحد الأفعال السلوكية المجرمة في نص المادة 394 مكرر2، وأن تنصرف هذه الإرادة إلى النشاط الجرمي فحسب دون إرادة أي نتيجة.

[1] مرجع السابق، ص 208.

[2] حمودي ناصر، مرجع نفسه، ص84.

[3] رشيدة بوكر، مرجع نفسه، ص294.

- القصد الجنائي الخاص:

بحث البعض، فيما إن كانت جريمة التعامل في المعلومات غير مشروعة، تشترط بالإضافة للقصد الجنائي العام السابق قصدا جنائيا خاصا، سواء في صورة الجريمة الأولى أو في صورتها الثانية، فبخصوص الصورة الأولى، ذهب هذا الاتجاه للقول بوجوب توفر قصد خاص إلى جانب القصد العام حتى تقوم جريمة التعامل في معلومات صالحة لارتكاب جريمة ويشمل هذا القصد الخاص في اتجاه إرادة الجاني إلى الإعداد والتمهيد لاستعمال هذه المعلومات في ارتكاب جريمة من جرائم الاعتداء على نظم المعالجة الآلية للمعلومات، غير أن المشرع الجزائري صراحة لم يشترط هذا القصد في نص المادة 394 مكرر2.

أما بخصوص الصورة الثانية لهذه الجريمة فإن القصد العام كاف لوحد لقيامها[1].

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

تعتبر حماية المعطيات الشخصية ذات أهمية قصوى في المجتمع الرقمي المتغير الأمر الذي أدى بالمشرع الجزائري لإضفاء حماية خاصة للأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي من خلال القانون رقم 18-01[2]

أولا: التعريف بالمعطيات ذات الطابع الشخصي:

لقد عرف المشرع الجزائري المعطيات ذات الطابع الشخصي من خلال المادة 3 من القانون 18-07 كل معلومة بغض النظر عن دعامتهاالمتعلقة لشخص المعني بصفة مباشرة أو غير مباشرة لاسيما لربوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهوية البدنية أو الفيزيولوجية أو الجينية أو البيومترية.

يحتوي هذا التعريف على خاصيتين:

[1] حمودي ناصر،المرجع نفسه ص،ص 84-85.

[2] عز الدين عثماني، عفاف خذيري، الحماية القانونية للمعطيات ذات الطابع الشخصي في التشريع الجزائري، دراسة في ظل القانون رقم 18-07. المجلة الدولية للبحوث القانونية والسياسية العدد 01، جامعة العربي التبسي تبسة 2020 ص،ص 86-88.

- الأولى تتعلق بالمعطيات ذات الطابع الشخصي متعلقة بالشخص الطبيعي وليس بالشخص المعنوي.
- الثانية هي تلك المعطيات التي تمكن من عريف والتعرف على الشخص الطبيعي[1]

ثانيا: الاعتداء على المعطيات ذات الطابع الشخصي

يمكن لكل شخص يدعي أنه تم المساس بحقوقه المتمثلة بالمعطيات ذات الطابع الشخصي، أن يطلب من الجهة القضائية المختصة اتخاذ أي إجراءات تحفظية لوضع حد لهذا التعدي أو الحصول على التعويض اللازم. تختص الجهات القضائية الجزائرية بمتابعة هذه الجرائم وفقا لقواعد الاختصاص المنصوص عليها في المادة 588 من قانون الإجراءات الجزائية وقد جرم القانون الجزائري من خلال القانون سابق الذكر الأفعال الماسة بالمعطيات ذات الطابع الشخصي وأقر لها عقوبات متفاوتة ويتم إدراجها كالآتي[2]

01- تجريم الجمع غير المشروع للمعطيات الشخصية تتضمن هذه الجريم عدة صور مخالفة لأحكام جمع المعطيات الشخصية وذلك باستعمال الوسائل التدليسية أو غير النزيهة أو غير المشروعة وكما قد تتعلق بطبيعة المعطيات التي قام المسؤول عن المعالجة بجمعها عندما ترتبط خصوصا بالمعطيات الحساسة.

02- تجريم المخالفات المرتكبة أثناء إنشاء المعالجة وهذه المرحلة تعد الأكثر تعرضا لارتكاب مخالفات كثيرة تشكل جرائم معاقب عليها بمقتضى القانون 07/18 والتي تقوم أما بسبب مخالفة الشروط المسبقة للمعالجة، أو بسبب خرق للالتزامات الملقاة على عاتق المسؤول عن المعالجة أثناء القيام بعملية المعالجة

03- تجريم الاستغلال غير المشروع للمعطيات الشخصية:

تتضمن هذه الجريمة في أن الجاني يفترض فيه أنه قد استوفى كل الشروط المسبقة لانجاز المعالجة إلا أنه أثناء استعمالها لبلوغ الأهداف التي أنجزت من أجلها قد يرتكب مخالفات قدر المشرع أنها

[1] تومي يحيى، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون رقم 8-07 دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 4 جامعة يحيى فارس، المدية، 2019 ص،ص 25-26

[2] عز الدين عثماني. عفاف خذيري، المرجع السابق ص 103.

ستؤدي إلى الإضرار بالمعطيات الشخصية فمنها ما يتعلق بمخالفة بعض بنود التصريح بالمعالجة، وأخرى ما يتعلق بإفساد المعطيات إلى غير المؤهلين لذلك.[1]

ثالثا: العقوبات الجزائية الردعية لحماية المعطيات ذات الطابع الشخصي:

نص عليها المشرع الجزائري في القانون 18-07 في الفصل بعنوان " الأحكام الجزائية" وهي العقوبات الناتجة عن مخالفة أحكام هذا القانون وأقر لها عقوبات متفاوتة تتراوح بين الحبس من شهرين إلى خمس سنوات والغرامات التي تتراوح بين 20.000 دج إلى مليون دينار جزائري، وتختلف الجزاءات بحسب اختلاف المخالفات التي يرتكبها الشخص المعالج أو المعالج من الباطن أو أي شخص آخر أدى تصرفه للمساس بسلامة وأمن المعطيات ذات الطابع الشخصي[2]

من بين العقوبات المنصوص عليها:

- يعاقب كل من يقوم بمعالجة المعطيات ذات الطابع الشخصي دون الحصول على الموافقة الصريحة للشخص المعني أو تطلع الغير المعطيات ذات الطابع الشخصي الخاضعة للمعالجة خارج إطار أدائه لمهامه إلا من أجل الغايات المرتبطة مباشرة بمهام المسؤول عن المعالجة والمرسل إليه وبعد الموافقة المسبقة للشخص المعني بالحبس من سنة إلى ثلاث سنوات وبغرامة من 100.000 دج إلى 300.000 دج لكل من يقوم بجمع البيانات الشخصية بأية وسيلة غير مشروعة كالغش والتدليس.

- يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 200.000 دج إلى 500.000 لكل من يسمح بالولوج إلى معطيات ذات طابع شخصي لأشخاص غير مؤهلين لذلك[3].

---

[1] طعباش عز الدين، الحماية الجزائرية للمعطيات الشخصية في التشريع الجزائري، دراسة في ظل قانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المجلة الأكاديمية للبحث القانوني العدد 02/ 2018، ص،ص 29- 34-53.

[2] عز الدين عثماني، عفاف خذيري، المرجع السابق ص 104.

[3] المرجع نفسه ص 105.

ملخص الفصل الأول

إلى هنا أنهيت الفصل الأول تحت عنوان ماهية الوثائق البيومترية الإلكترونية من خلال المبحث الأول، الذي تطرقنا من خلاله مفهوم هذه الوثائق البيومترية الإلكترونية، رخصة السياقة البيومترية الإلكترونية، جواز السفر البيومتري الإلكتروني، أما بالنسبة للمبحث الثاني تم رصد الآليات الموضوعية لمواجهة جريمة المساس بهذه الوثائق البيومترية الإلكترونية تعتبر هذه الجريمة وطرق ارتكابها مستحدثة، يختلف عن تلك التي كانت ترتكب بها الجريمة التقليدية، التي تتسم قوانينها الموضوعية بطابع تقليدي مفرط يميل للثبات والاستقراء مما ترتب على ذلك خطورة هذه القواعد عن مواكبة التطور العلمي والتكنولوجي الذي طرأ على كافة مناخي الحياة المعاصرة بصفة عامة، مما أدى هذه الأخيرة إلى إفراز العديد من الجرائم المستحدثة ذات الطبيعة الخاصة، إلا أنه مكافحة هذه الجرائم مازال يتم في إطار النصوص التقليدية ومن أمثلة ذلك جريمة الاعتداء أو المساس بالوثائق البيومترية الإلكترونية، حيث لا توجد نصوص عقابية صريحة في هذا الشأن، ونظرا لهذا العجز، حاول المشرع الجزائري سن تشريع جديد يتجاوب مع الطبيعة الخاصة لهذه الجرائم الحديثة حيث قام بتعديل قانون العقوبات بموجب القانون رقم 04-05 مستحدثا فيه جملة من النصوص جرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات ذات الطابع الشخصي للأشخاص الطبيعيين، لننتقل للفصل الثاني الذي يعالج الجانب الإجرائي يتناول الآليات القانونية التي تبناها المشرع الجزائي لمواجهة الجرائم الماسة بالوثائق البيومترية.

الفصل الثاني:

الحماية الجنائية الإجرائية للوثائق البيومترية الإلكترونية.

الفصل الثاني

إذا كانت ظاهرة الإجرام الالكتروني قد أثارت بعض المشكلات فيما يتعلق القانون الجنائي الموضوعي، بحثا عن إمكانية تطبيق نصوصه التقليدية على هذا النوع من الجرائم واحترام مبدأ الشرعية والتفسير الضيق للنصوص الجزائية، فقد أثارت في الوقت نفسه مشكلات أكثر في نطاق القانون الجزائي الإجرائي،وتزويد المشكلات الإجرائية في مجال الجرائم الإلكترونية لتعلقها في العديد من الأحيان ببيانات المعالجة الآلية وكيانات معنوية، ومن ثم يصعب الكشف عنها وإثباتها نظرا للسرعة الفائقة والدقة غير المتناهية في تنفيذها، ناهيك عن إمكانية محوها وتمويه أثارها وإخفاء الأدلة المتحصل منها بسهولة عق تنفيذها باستعمال تقنيات تكنولوجية عالية عكس الإجراءات المتعلقة بجرائم تقليدية، تركب في عالم محسوس وملموس يؤدي فيه السلوك المادي الدول الأكبر والأهم وأمام هذا الوضع أثير التساؤل حول مدى صلاحية تطيق إجراءات المتابعة التقليدية على جرائم إلكترونية ارتكبت في عالم افتراضي غير ملموس، وهذا ما سوف تقوم بدراسته من خلال هذا الفصل حيث تناولنا مبحثين المبحث الأول: إجراءات المتابعة للجرائم الماسة بالوثائق البيومترية الإلكترونية أما المبحث الثاني تناولنا حجية الدليل الرقمي أمام القاضي الجزائي في الجرائم الماسة بالوثائق البيومترية.

المبحث الأول: إجراءات المتابعة للجرائم الماسة بالوثائق البيومترية.

لقد أدرك المشرع الجزائري جيدا بان المواجهة الفعالة لجرائم الماسة بالوثائق البيومترية الالكترونية لا تكون بإرساء قواعد قانونية موضوعية فقط، وإنما لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية من اجل الكشف عن هذه الجريمة نظرا لطبيعتها الخاصة كونها تتعلق بمحل غير مادي حيث اعتمد المشرع مجموعة مجموعة من الأساليب في متابعة الجريمة الماسة بالوثائق البيومترية الالكترونية و المتمثلة في القواعد العامة و الخاصة في التحري و التحقيق و هذا ما سنعرضه كالآتي:

المطلب الأول: القواعد العامة في التحري والتحقيق.

إن الجريمة الماسة بالوثائق البيومترية الإلكترونية تعتبر كأي جريمة من الجرائم المنصوص عليها في قانون العقوبات والقوانين الأخرى فلذلك تتبع الجريمة الإلكترونية دعوى عمومية وهذه الدعوى تتم مراحل سنوضحها من خلال الفروع الآتية.

الفرع الأول: الإجراءات المادية.

سنتناول في هذا الفرع الإجراءات المادية لتحري والتحقيق في الجرائم الماسة بالوثائق البيومترية الالكترونية تتمثل فالآتي

أولا: المعاينة:

تعتبر المعاينة من المراحل الأولى للاستدلال على ملابسات الجريمة ومن أهم إجراءات التحقيق على الإطلاق، نظرا لما يمكن أن توفره من أدلة إثبات، وتزداد أهميتها أكثر إذا تعلق الأمر بالجرائم الإلكترونية، باعتبارها من الجرائم المستحدثة وغير المألوفة النظر للطبيعة الخاصة للسلوك الإجرامي فيها[1]ولهذا يمكننا تعريفها كالآتي: "حيث يقصد بالمعاينة العمل الذي يقوم به المحقق والذي يتطلب منه الانتقال لمكان وقوع الجريمة لمعاينة حالة الأمكنة والأشياء والأشخاص ووجود

[1]براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل درجة دكتوراه، في القانون، جامعة مولود معمري – تيزي وزو 2018 ص56.

الجريمة ماديا وكل ما يلزم إثبات حالته قبل أن يكون أي منها عرضة لمؤثرات خارجية"[1] وللمعاينة أهمية بارزة في مجال التحقيق الجنائي لكونها مصدر أصيلا من مصادر الأدلة المادية والفنية الراسخة والثابتة التي تكون دائما محل ثقة سلطات التحقيق والقضاء ومرآة صادقة تعكس بأمانة وقائع وملابسات الجريمة[2].

وتتم المعاينة في الجرائم الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة، غير أن الانتقال هنا يختلف حسب طبيعة الجريمة الإلكترونية المرتكبة، وإذا كانت الجريمة واقفة على المكونات المادية للأجهزة الإلكترونية كجرائم الاعتداء على الحاسب الآلي أو الأشرطة أو الأقراص الممغنطة، فالانتقال في هذه الحالة يكون ماديا لمسرح الجريمة الذي يحوي هذه المكونات لمعاينته والتحفظ على الأشياء التي تعد أدلة مادية تدل على وقوع الجريمة وانتسابها لشخص معين تم ضبطها وضمها في أحراز مختومة تقدم للنيابة العامة[3] أما إذا كانت الجريمة واقعة على المكونات الغير المادية للأجهزة الإلكترونية أو بواسطتها، كتلك الواقعة على برامج الحاسب وبياناته بواسطة الانترنت فيكون الانتقال للمعاينة هنا افتراضيا أو إلكترونيا، ويمكن للمحقق إجراء المعاينة الافتراضية أو الالكترونية بالولوج أو الانتقال لمسرح الجريمة عبر الانترنت انطلاقا من مكتبة بواسطة الحاسب الموضوع تحت تصرفه، أو من خلال مقهى الانترنت أو إحدى مقرات مزود خدمات الانترنت[4].

ويلتزم المحقق عادة قبل البدء في المعاينة الالكترونية بجملة من التدابير الفنية والتحفظية التي تساعده في القيام بمهامه على أحسن وجه وهي كالآتي:

---

[1] عبدالله اوهايبية، شرح قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، 2004 ص164.

[2] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دار النهضة العربية، القاهرة 2013، ص44.

[3] ياسر محمد الكومي محمود أبو حطب، الحماية الجنائية والأمنية للتوقيع الإلكتروني، منشأة المعارف، الاسكندرية 2014 ص243.

[4] براهيمي جمال،المرجع السابق ص58.

1/ الاستعلام المسبق عن مكان وقوع الجريمة، ونوع وعدد ومواقع الأجهزة الإلكترونية وشبكاتها وسائر ملاحقاتها والنهايات المتصلة بها المتوقع مداهمتها[1].

2/ توفير الوسائل والإمكانات اللازمة من أجهزة وبرامج وأقراص صلبة ولينة التي يمكن الاستعانة بها في الفحص، التشغيل، الضبط والتأمين و حفظ المعلومات.

3/ تأمين التيار الكهربائي بشكل لا يتم التلاعب أو التخريب عن طريق قطع التيار أو تعديل الطاقة الكهربائية.

4/ التأكد من خلو المحيط الخارجي لمسرح الجريمة الإلكترونية من أية مجالات لقوى مغناطيسية أو ممرات اتصالات التي يمكن أن تتسبب في محو البيانات المسجلة أو إتلاف الآثار الأخرى للجريمة.

5/ التحفظ على محتويات سلة المهملات ومستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليها من بصمات.

6/ إعداد فريق من المختصين وأهل الخبرة في مجال تكنولوجيا الإعلان الآلي للاستعانة بهم عند الحاجة[2].

ثانيا: التفتيش.

إذا كان تفتيش مسرح الجريمة التقليدية يخضع للإجراءات المنصوص عليها في قانون الإجراءات الجزائية فإن التفتيش عن الجريمة الإلكترونية سؤال يطرح نفسه هل يخضع أيضا إلى نفس إجراءات التفتيش في الجريمة التقليدية وللإجابة عن هذا السؤال وجب تقديم تعريف التفتيش:

1/ التعريف التفتيش الإلكتروني:

يعرف التفتيش بأنه هو "البحث في مستودع سر عن أدلة الجريمة التي وقعت وكل ما يفيد في الكشف عن الحقيقة ويتمثل السر في شخص المتهم أو في المكان الذي يعمل فيه أو يقيم فيه"[1].

[1] ياسر محمد الكومي محمود أبو حطب، مرجع سابق، ص245.

[2] براهيمي جمال، المرجع نفسه، ص، ص 58- 59.

أما تعريف التفتيش في منظومة إلكترونية: "هوالاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو نظمه أو الانترنت"[2] والجدير بالذكر أن الإجراءات التي يخضع لها المحقق الجنائي في عملية التفتيش في الجريمة التقليدية سواء ما تعلق منها بالاختصاص المحلي أو الزماني، تختلف عن تلك التي أقرها له المشرع في الجريمة المعلوماتية، بحيث إذا كان المحقق أو ضابط الشرطة القضائية بصدد البحث والتحري أو التحقيق في الجريمة المعلوماتية فإن مواعيد التفتيش تكون مفتوحة بحيث يمكنه التفتيش في أية ساعة ليلا أو نهارا، كما يمكنه تمديد اختصاصه المحلي بحيث يصبح وطنيا كل ذلك تحت سلطة النيابة العامة وهذا ما نصت عليه المادة 47 من قانون الإجراءات الجزائية في فقرتها3[3].

2/ شروط التفتيش: حتى يكون التفتيش صحيحا لابد من توفر مجموعة من الشروط الشكلية والموضوعية:

أ/ الشروط الشكلية:

اوجب المشرع الجزائري شروطا شكلية محددة لإجراء عملية التفتيش وهذه الشروط هي أن يصدر إذن التفتيش من طرف لجهة القضائية مختصة (النيابة العامة) وان يقوم بإجراء التفتيش شخص مختص من رجال الضبطية أو قاضي التحقيق وان يحرر محضر يضم جميع إجراءات التفتيش ونتائجه[4]

ب/ الشروط الموضوعية:

تتمثل في المحل والسبب والسلطة المختصة للقيام به، فالمحل عادة في الجريمة المعلوماتية مكان التفتيش هو الحاسب الآلي وهو نوعان مادي ومعنوي، والسبب أن تكون هناك شبهة متعلقة بشخص

---

[1]عبدالله اوهايبية، المرجع السابق، ص25.

[2]علي حسن الطوالبة، التفتيش الجنائي على نظام الحاسوب والانترنت ودراسة مقارنة في عالم الكتب الحديث، الأردن: 2004، ص13.

[3]علي حسن الطوالبة، المرجع السابق،ص60.

[4] ياسر محمد الكومي محمود أبو حطب، مرجع سابق، ص245.

تقود إلى دليل الإثبات وقوع الجريمة ونسبتها لمرتكبها، والسلطة المختصة بالتفتيش هي الضبطية القضائية أو قاضي التحقيق تحت سلطة النيابة العامة[1].

3/ التحديات التي تواجه عملية التفتيش في النظام المعلوماتي:

سبق وأن ذكرنا أن هذا النوع من الجرائم لا يترك أي أثر مادي في مسرح الجريمة فضلا على أن مرتكبيها يملكون القدرة على إتلاف أو تشويه الدليل في فترة وجيزة أما بالنسبة لإجراءات التفتيش فهذا النوع من الجرائم يتم عادة على شبكات المعلومات وقد يتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة وهذا هو الغالب في شبكات الاتصال الداخلية أو الدولية مما يستوجب امتداد نطاق إجراءات التفتيش إلى نظم غير النظام محل الاشتباه مما يشكل تحديات كبيرة، أو لها مدى قانونية هذا الإجراء، ومدى مساسه بحقوق أصحاب النظم التي يمتد إليها التفتيش ولكن هذه التحديات قد تمت معالجتها وبالنسبة لقانونية إجراء تمديد التفتيش وبسرعة إلى نظم أخرى،[2] إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وآن هذه المعطيات يمكن الدخول إليها من المنظومة الأولى، لكن بشرط إعلام السلطة القضائية المختصة مسبقا.

وما يكن استنتاجه هو الاختلاف القائم بين التفتيش في الجريمة التقليدية وبين التفتيش في الجريمة المعلوماتية، ففي الأولى يقع التفتيش على الأشياء المادية المتعلقة بالجريمة وملبساتها، بينما في الثانية التفتيش يقع على الأشياء المادية والمعنوية معا[3].

ثالثا: ضبط الأدلة.

يعتبر الضبط من إجراءات جمع الأدلة وهو النتيجة الطبيعية التي ينتهي إليها التفتيش والأثر المباشر الذي يسفر عنه، ويقصد به وضع اليد على الأشياء المتعلقة بجريمة وقعت والتي تفيد في

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، ط1، دار الفكر الجامعي مصر، 2007، ص234.

[2] زبيحة زيدان، الجرية المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر 2011، ص138.

[3] زبيحة زيدان، المرجع السابق، ص138.

كشف الحقيقة عنها وعن مرتكبها ووضعها في أحراز مختومة وتتقدم إلى الجهة القضائية المختصة كدليل إثبات[1].

وتحصيل الأدلة في الجرام الإلكترونية قد يرتبط بعناصر مادية كجهاز الحاسب الآلي وملحقاته، الأقراص الصلبة والأشرطة الممغنطة، الطباعة، البرامج اللينة والمراشد البطاقات الممغنطة وبطاقات الائتمان والمعدات المستعملة في شبكة الانترنت مثل المودم ففي هذه الحالة فلا يطرح ضبط هذه المكونات المادية أي إشكال قانوني أو عملي لإمكانية إخضاعها لإجراءات الضبط والتحرير التقليدية[2]، لقد نصت المادة 03/19 من الاتفاقية الأوروبية على مجموعة من التدابير الخاصة لضمان تحرير هذه الأدلة ذات الطبيعة الخاصة وحمايتها فنيا وصيانتها من أي تغيير أو إتلاف أو عبث يمكن أن يصيبها والتي نلاحظها فيما يلي:[3]

- استخراج نسخ احتياطية من دعائم البيانات والمعطيات المضبوطة والعمل عليها لتفادي المساس بالدليل الأصلي.

- عدم طوي القرص لتفادي تلفه وتحطيمه وفقدان المعلومات المسجلة فيه.

- تأمين البرامج المعلوماتية المضبوطة فنيا قبل تشغيلها.

- مراعاة ظروف الحرارة والرطوبة المناسبة في أماكن تخزين الأقراص والأشرطة الممغنطة المحرزة، والتي يجب لأن تتراوح درجة الحرارة فيها بين (4-32 درجة) وتكون درجة الرطوبة فيها ما بين (20-80%) مع تفادي تعريضها للأضواء أو لأي سائل من السوائل مع العلم أنه في مثل هذه الظروف يمكن أن تصل مدة صلاحية تخزين هذه الأقراص إلى ثلاث سنوات دون أن يصيبها تلف أو تعديل أو تحول[4].

---

[1] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، 2011 ص170.

[2] براهيمي جمال، المرجع نفسه، ص 47.

[3] حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، دراسة تطبيقية مقارنة جرائم لاعتداء على التوقيع الإلكتروني دار الكتب القانونية، القاهرة 2013 ص525.

[4] .حسام محمد نبيل الشنراقي، المرجع السابق، ص526.

– اقتداء بالاتفاقية الأوروبية حول الجرائم المعلوماتية، تدخلت عدة دول لتعديل قوانينها واستكمال مالها من فراغ تشريعي في مجال ضبط الأدلة الإلكترونية الرقمية وقواعد تحريرها، في مقدمتها فرنسا وعلى غرار المشرع الفرنسي تنبه المشرع الجزائري بدوره لهذا القصور، وتبنى في القانون رقم (09-04) المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في 2009/08/05، إجراءات مستحدثة خاصة لضبط وتحرير المعطيات والبيانات المعلوماتية وغيرها من الأدلة الرقمية ما يتناسب وطبيعتها اللامادية تحت عنوان "حجز المعطيات المعلوماتية"[1].

[1] براهيمي جمال، المرجع نفسه، ص،ص 51-52.

الفرع الثاني: الإجراءات في مواجهة الأشخاص.

أولا: الشهادة

الشهادة في مجال الجريمة الإلكترونية لا تختلف من حيث ماهيتها عن الجريمة التقليدية، وأمر سماع الشهود متروك لفطنة المحقق ومرتبط بظروف التحقيق، والأصل أن يطلب من الخصوم سماع من يرون من الشهود، وللمحقق أن يدعو للشهادة من يقدر أن لشهادته أهمية، وله أن يسمع أي شاهد يتقدم من تلقاء نفسه والشاهد في الجريمة المعلوماتية هو ذلك الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي، والذي تكون لديه معلومات جوهرية أو هامة لازمة للدخول في نظام المعالجة الآلية للبيانات، إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، وذلك تمييزا له عن الشاهد التقليدي[1].

1/ طوائف الشاهد المعلوماتي:

أ/ مشغلو الحاسب الآلي: وهم الخبراء الذي تكون لهم الدراية التامة بتشغيل جهاز الحاسب الألي والمعدات المتصلة به، واستخدام لوحة المفاتيح في إدخال البيانات، وتكون لديهم معلومات عن قواعد كتابة البرامج[2].

ب/ المحللون: والمحلل هو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين وتحليلها إلى وحدات منفصلة، واستنتاج العلاقات الوظيفية منها، كما يقوم كذلك بتتبع البيانات داخل لنظام عن طريق ما يسمى بمخطط تدفق البيانات، واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب.

ج/ المبرمجون: وهم الأشخاص المتخصصون في كتابة أوامر البرامج ويمكن تقسيمهم إلى قسمين:

*الفئة الأولى: هم مخططو برامج التطبيقات، ويقومون بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم، ثم يقومون بتحويلها إلى برامج دقيقة وموثوقة لتحقيق هذه المواصفات.

[1] عبد الإله هلالي، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، (د.ط)، دار النهضة العربية، القاهرة، 2000، ص23.

[2] محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، (د.ط)، مطابع المكتب المصري الحديث، القاهرة، 1991، ص23.

* الفئة الثانية: هم مخططو برامج النظم ويقومون باختيار وتعديل وتصحيح برامج نظام الحاسب الداخلية وإدخال أية تعديلات أو إضافات لها[1].

د/ مهندسو الصيانة والاتصالات: وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب وبمكوناته وشبكات الاتصال المتعلقة به[2].

ثانيا: الخبرة.

من أهم التعريفات التي وردت بخصوص الخبرة القضائية أنها عبارة عن إجراءات من إجراءات التحقيق يعهد به القاضي إلى شخص مختص ينعت بالخبير وتتعلق بواقعة يستلزم بحثها أو تقديرها إبداء رأي يتعلق بها علما أو فنا لا يتوافر في الشخص العادي ليقدم له بيانا أو رأيا فنيا لا يستطيع المحقق الوصول إليه وحده[3].

وتعتبر الخبرة من المسائل الأساسية التي يعتمد عليها رجل القضاء أو ضابط الشرطة القضائية عندما يتعلق الأمر بالأمور الفنية التي قد يقف أمامها عاجزا، ونظرا لعدم درايته بهذه الأمور فهو إن علم أشياء غابت عنه أشياء أخرى، لذلك لابد له من الاستعانة بذوي الخبرة لحل المسائل الفنية العالقة والخبرة قد يستعان بها في مرحلة جمع الاستدلالات من طرف الضبطية القضائية أو أثناء مرحلة المحاكمة[4].

1/ طرق إجراء الخبرة في الجريمة المعلوماتية:

يعتمد عمل الخبير المعلوماتي في سبيل تحري الحقيقة في مجال الجرائم الماسة بالوثائق البيومترية الإلكترونية على جمع مجموعة من الأدلة الرقمية وتحصيلها من خوادم المواقع (Les serveurs) ومن جهاز المعتدي بعد التوصيل إلى تحديده، ثم يقوم بعملية تحليل رقمي بها لمعرفة كيفية إعدادها

[1] عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، محور القانون الجنائي، دبي، من 26 إلى 28أفريل، 2003، ص616.

[2] خالد محمد المهيدي، التحقيق الجنائي العملي في الجريمة التقليدية والمعلوماتية، (ط.2)، دار الغرير للطباعة والنشر، دبي، (د، د، ن)، ص508

[3] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائي، مذكرة مقدمة لنيل الماجستير، في العلوم القانونية تخصص جنائي، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2012، ص170.

[4] الحلبي محمد علي سالم، الوجيز في أصول المحاكمات الجزائية ،ط1، دار الثقافة للنشر، الأردن، ص 135.

البرمجي ونسبها إلى مسارها الذي أعدت فيها وتحديد عناصر حركتها، ومن ثم التوصل في النهاية إلى معرفة بروتوكول الانترنت (Ip) للحاسوب الذي صدرت منه الرسائل والنبضات الإلكترونية.

ويرى بعض المتخصصين أن عمل الخبير المعلوماتي في اشتقاق وتجميع الأدلة الرقمية يتم عبر ثلاث مراحل:

* المرحلة الأولى: تجميع المعلومة المخزنة لدى الطرف مقدم الخدمة من خلال تتبع الحاسبات الخادمة التي دخل منها المجرم المعلوماتي ومحاولة إيجاد أثر له.

* المرحلة الثانية: مرحلة المراقبة ويتم ذلك بطرق مختلفة أهمها استخدام برمج مراقبة يمكن تحميلها للبحث عن المعلومات المشبه فيها، وحضر وتسجيل بيانات كل دخول وخروج بالموقع.

* المرحلة الثالثة: فحص النظام المعلوماتي المشتبه فيه بعد ضبطه من طرف جهات التحقيق بمكوناته المادية والمعنوية لانشقاق الدليل وتقديمه لجهات التحقيق وتقرير مدى وقوع الجريمة باستخدام النظام المضبوط من عدمه[1].

2/ الوسائل العلمية لإنجاز الخبرة الإلكترونية:

يعتمد الخبير في شرح ملابسات الجريمة الإلكترونية واستخلاص الدليل الرقمي الذي يساعده على الكشف عن المجرم الإلكتروني على جملة من الوسائل العلمية، والتي تمثل في الغالب أدوات فنية تستخدم في بنية نظام المعلومات، ونذكر منها مايلي:

- بروتوكول الانترنت (IP).
- نظام البروكسي (Proxy).
- برنامج (Trace route).
- أنظمة كشف الاختراق (I D S)[2].
- برامج مراجعة العمليات الحاسوبية واسترجاعها (Auditingtools).

[1] سعيداني نعيم، المرجع السابق، ص171.

[2] براهيمي جمال، المرجع نفسه، ص،ص 78-79.

- برنامج الدمج وفك الدمج (Pkzip).

- الذكاء الصناعي[1].

3/ تقنيات إنجاز الخبرة الإلكترونية:

لقد وضعت وزارة العدل الأمريكية إطارا عمليا نموذجيا يحدد التقنيات الأساسية التي يتعين على الخبير الإلكتروني إتباعها لجمع الأدلة الرقمية، فحصها وتحليلها، ومن ثم كتابة النتائج المتوصل إليها في التقرير، والتي يمكن تلخيصها فيما يلي:

أ/ التقنيات ما قبل التشغيل والفحص وتتمثل في:

- التأكد من صلاحية وحدات نظام الأجهزة الإلكترونية المتعلقة بالجريمة للتشغيل.

- التحقق من مطابقة محتويات إحراز المضبوطات لما هو مدون عليها.

- تسجيل وتوثيق وحدات المكونات المضبوطة، كالنوع والطراز والرقم التسلسلي[2].

ب/ تقنيات التشغيل والفحص وهي كالتالي:

- استكمال تسجيل باقي معطيات الوحدات من خلال قراءة الجهاز.

- وضع نسخة لكل دعائم التخزين المضبوطة بما فيها القرص الصلب وإجراء الفحوصات المبدئية عليها لحماية الأصل من أي فقدان أو تلف أو تدمير يكون سببه سوء الاستخدام أو برامج القراءة المدمرة أو ما يدعى (أقراص القراءة المدمرة) فيروسات أو قنابل برمجية.

- تحديد أسماء وأنواع المجموعات البرمجية ذات دلالة بالجريمة كبرامج النظام، برامج التطبيقات وبرامج الاتصالات... إلخ.

- إظهار الملفات المخبأة والنصوص المخفية داخل الصور واسترجاع الملفات التي تم محوها من الأصل باستعمال برامج استعادة المعلومات وإصلاح الملفات المعطلة أو التالفة، مع العلم أنه في

[1] براهيمي جمال، المرجع نفسه، ص،ص 80-81.

[2] المرجع نفسه، ص81.

حالة محو معطيات المجرمة من طرف المجرم فإنها لا تحذف ماديا وإنما " الرابط بين هذه المعطيات هو من يمحى، فالمعطيات تبقى في ذاكرة الدعامة وبالتالي يمكن إيجاد الملفات المحذوفة عن طريق فحص الهوامش العلوية (les en-tetes) ومن ثم استعادة[1].

تخزين هذه الملفات، أو البيانات وعمل نسخ طبق الأصل أخرى من الأسطوانة أو القرص المحتوي لها من أجل فحصها.

إعداد قائمة يجرد منه الخبير كل الأدلة المتحصل عليها مع إجراء مرافقة لكل نسخة أو صورة محتفظ بها في جهاز أخر للتأكد من سلامة القائمة.

- تحديد الخصائص المميزة لكل جزء من الأدلة الرقمية مثل المستند الرقمي، البرامج والتطبيقات، النصوص، الصور، الأصوات وتحويلها إلى هيئة مادية كل حسب طبيعته[2].

ثالثا: الاستجواب.

إن الاستجواب يعتبر مرحلة مهمة في إجراءات التحقيق، حيث يتم الحصول على اعترافات أو معلومات تمكن القائمين على الاستجواب من التأكد من ارتكاب الجريمة من الشخص المستوجب أو عدم وجود أي علاقة بينه وبين الجريمة المرتكبة.

إذ تتم مناقشة الشخص المستوجب حول وقائع الجريمة وتفاصيلها ومطالبته له بإبداء رأيه في الأدلة القائمة ضده إما تقنيا أو تسليما، وذلك قصد الكشف عن الحقيقة واستظهارها بالطرق القانونية.

إن الإجراءات المقررة للاستجواب في الجريمة المعلوماتية تحكمها نفس الضوابط المقررة لاستجواب المتهم في الجريمة التقليدية، لكن الفرق يكمن في ضرورة تأهيل السلطة المختصة التي تتولى إجراءات الاستجواب ذلك، أن جهات التحقيق لابد أن تكون مؤهلة للتحقيق في جرائم

[1] براهيمي جمال، المرجع السابق ص78.

[2] رابح وهيبة، الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث،للدراسات الأكاديمية، العدد 4، جامعة عبد الحميد بن باديس، مستغانم، 2014، ص28.

المعلوماتية، حتى تمكن استيعاب واقعة التحقيق والتعامل مع مفردات الجريمة سيما وأن المجرم الذي ارتكب الجريمة والذي يحقق معه ليس بمجرم عادي[1].

المطلب الثاني: الإجراءات المستحدثة لجمع الدليل.

نظرا للتطور الكبير في أساليب ارتكاب الجرائم، مما يجعل اكتشافها معقدا من طرف الجهات المختصة، كان لازما العمل على تطوير القواعد الإجرائية خاصة في سبيل مكافحة الجرائم المعلوماتية بصفة عامة والجريمة الماسة بالوثائق البيومترية الإلكترونية خاصة، وهذا من خلال القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بهذا سنحاول تفصيل ذلك من خلال الآتي:

الفرع الأول: إجراءات المتابعة من خلال قانون الإجراءات الجزائية.

نص قانون الإجراءات الجزائية على مجموعة من إجراءات التحري والتحقيق في الجرائم الإلكترونية والتي تنطبق على الجرائم المرتكبة على الوثائق البيومترية كما يلي:

أولا: التسرب.

يعد التسرب من إجراءات البحث والتحقيق الجديدة التي أرستها معظم تشريعات العالم الحديثة بمواجهة الجرائم الإلكترونية و لهذا سوف يتم تحديد معالم إجراء التسرب من خلال الآتي:

1/ تعريف التسرب:

تعرف المادة (65 مكرر12) من قانون الإجراءات الجزائية الجزائري التسرب على أنه "قيام ضابط في عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف"[2] 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"[3].

---

[1] رابح وهيبة، المرجع السابق، ص 328.

[2] براهيمي جمال، المرجع نفسه، ص83.

[3] عبد الرحمن خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، ط2، دار بلقيس، الجزائر، 2016 ص105.

الملاحظ أن إجراء التسرب يبدو غريبا وغير مستساغ نظرا لما يمثله من خطورة على الحريات وحقوق الإنسان لذلك نجد أن المشرع لم يطلق يد الضبطية القضائية في ممارسة هذا الإجراء بل خصه بضوابط وشروط تضعه في إطاره القانوني: وتتمثل هذه الشروط فيما يلي،[1] حيث وردت في نص المادة 65 مكرر 11 من قانون الإجراءات الجزائية حيث نستخلص منها الآتي:

- أن يصدر الإذن من وكيل الجمهورية أو قاضي التحقيق.

- أن يوجه هذا الإذن لضابط الشرطة القضائية.

- أن تكون الجريمة المتسرب فيها تشكل إحدى الجرائم المذكورة في المادة 65 مكرر5.

- عدم تحريض المتسرب للمشتبه فيهم لارتكاب الجرائم من أجل القبض عليهم تحت طائلة البطلان وفقا لنص المادة 65 مكرر 2/12.

- أن يكون التسرب وفق إذن مكتوب يحدد فيه بدقة نوع العملية المتسرب من أجلها وصفة ضابط الشرطة القضائية المسؤول عن عملية التسرب، وأسباب اتخاذ هذا الإجراء.

- أن تكون مدة عملية التسرب محددة فلا يجب أن تتجاوز 4أشهر إلا إذا دعت مقتضيات التحري ذلك، ويجب أن يكون التمديد من إذن وكيل الجمهورية.

- وجوب إعداد تقرير يتضمن جميع ما قام به العضو المسرب من إجراءات[2].

2/ خصائص التسرب.

دور التسرب يتمثل في مجرد مطابقة خصائصه بخصائص الجريمة المقصودة بها وهي نفس الخصائص الضامنة لفعالية العلمية والتي يمكن حصرها فيما يلي:

[1] زيبحة زيدان، المرجع نفسه، ص169.

[2] هنوني نصرالدين ويقدح دارين، الضبطية القضائية في القانون الجزائري ط2. دار هومة الجزائر 2011 ص81.

أ/ السرية:

والمقصود بها إئتمان سر ما يتعلق بالعملية، وتكون السرية عاملا يضمن عدم الترصد بالنسبة للمتسرب من جهة ويضمن إبقاء النشاط الإجرامي للشبكة في سريان عادي، دون أن يشك المجرم بأنه تمت مراقبته كما أن لها دور فعال في ضمان أمن وسلامة المتسرب وحسن سير العملية[1].

ب/ الحيلة:

تعتبر الحيلة من أهم خصائص التسرب والتي نجد لها نص في المادة 65 مكرر12 "... بإيهامهم وعلى القائم بإجراء التسرب مراعاة هذا الأمر وذلك بالقضاء على كل الشكوك التي تبادر إلى ذهن المشتبه فيه، فالحيلة في ميدان الإجرام متبادلة وتكون في هذا المجال خالية من الضوابط التي تحكمها، ما عددا قاعدتي البقاء والنجاح كما أن الحيلة تخضع لمبدأ الإخلاص في ضبط الأدلة.

ج/ الخطورة:

يعتبر إجراء التسرب من أخطر الإجراءات التحقيق القضائي ويعود ذلك لعدة عوامل منها:

– ما يتعلق بالإجرام فهي كل الأعمال التي يؤديها المتسرب المتعلقة بتغطية صفته القضائية وعليه تعد من الأعمال الإجرامية المرتبة بخطورة بعد اعتداء على حقوق الأخرين وهذا قد يعرض المتسرب إلى الدفاع الشرعي من الضحايا.[2]

– ومنها ما يتعلق بمكان تواجد المتسرب فواجبه المهني يحتم عليها التواجد بأماكن أكثر أمنا للمجرمين والأخطر على حياته كتلك المتعلقة بالجغرافيا مثال على ذلك عمليات التسرب في الشبكات الإرهابية التي تعتمد على الأوتار والمخابئ في أعلى الجبال وأعماق الغابات والتي قد تعرضه لأخطار متعددة[3].

---

[1] أسماء عنتر مكافحة الجرائم المستحدثة في التشريع الجزائري، (التسرب نموذجا) مجلة القانون العام الجزائري والمقارن، العدد6، 2007، جامعة عبد الحميد بن باديس، مستغانم، ص79

[2] أسماء عنتر، المرجع السابق، ص80.

[3] المرجع نفسه، ص 81.

3/ مراحل وإجراءات تنفيذ عملية التسرب:

على المتسرب وقبل الشروع في المهمة التي أوكلت إليه أن يقوم ببعض الأمور الأولية التي تسهل عليه عملية الدخول والتوغل حسب نشاطه وهذا ما سنوضحه من خلال الآتي:

1/ مراحل تنفيذ عملية التسرب:

أ/ أخذ صورة لازمة للوسط المراد اختراقه وهذا حسب طبيعة الوسط المتسرب فيه وحسب نشاط المتسرب فيه.

ب/ حسن اختيار القائم بعملية التسرب، وذلك من خلال إخضاعه لجملة من الاختبارات قصد التأكد من مدى قدرته على التحمل لأن هذا الاختبارات قد تصادفه أمام العملية.

ج/ تقديم طلب ترخيص من الجهات المختصة (وكيل الجمهورية، قاضي التحقيق)[1].

2/ الإجراءات المستعملة في عملية التسرب.

إجراءات التحقيق تنقسم إلى قسمين مادية وأخرى خاصة متضمنة إجراء التسرب وسنحاول ذكر العلاقة العملية بينهما فيما يلي:

أ/ إجراءات التحقيق الخاصة:

قصد الوصول للنتيجة المنتظرة من عملية التسرب، أجاز المشرع الاعتماد على طرق وأساليب خاصة ولكن وردت جملة من الاستثناءات باعتبار أن الجريمة ليست مطلقة وأنها قد تكون نسبية، ومن بين هذه الأساليب الخاصة نعود لنص المادة 65 مكرر2 في فقرتها التالية من قانون الإجراءات الجزائية وهي: اعتراض المراسلات السلكية واللاسلكية، التنصت على المحادثات السرية والمكالمات الهاتفية، تسجيل الأصوات والتقاط الصور وهذه ما تكون عادة في مرحلة الإعداد والتحضير لتنفيذ العملية[2].

[1] أسماء عنتر، المرجع نفسه، ص84.

[2] أحمد غازي، ضمانات المشتبه في أثناء التحريات الأولية، دار هومة، الطبعة الثانية، الجزائر 2011 ص211.

ب/ إجراءات التحقيق العادية: وهي الإجراءات المعتادة لتفتيش التوقيف للنظر[1].

– التفتيش: لم يعد ضباط الشرطة القضائية ملزمين بمراعاة حضور المتهم أثناء عملية التفتيش إذا تعلق الأمر بالجرائم الخطيرة، كما نص المشرع في هذه الحالة على إمكانية التفتيش خارج الأوقات القانونية[2] مما يمكن من ضبط الأدلة والحصول على نتيجة متكاملة في حالة التسرب.

– التوقيف للنظر: يمكن تمديد التوقيف للنظر على النحو التالي:

3 مرات إذا تعلق الأمر بالجريمة المنظمة، تبييض الأموال، جرائم الماسة بالتشريع الخاص والصرف، مرتان بالنسبة لجرائم الاعتداء على آمن الدولة، مرة واحدة إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[3].

ثانيا: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

لقدر أقرا المشرع الجزائري إمكانية اعتراض مراسلة الأشخاص ولذلك في إطار متابعة بعض الجرائم أو ما اصطلح عليه بالجرائم المستحدثة وقد ذكرت على سبيل الحصر في المادة 65 مكرر5، لذلك وجب معرفة هذا الإجراء وطرق تطبيقه في الجرائم الإلكترونية عامة والجرائم الماسة بالوثائق البيومترية خاصة لأنها موضوع البحث.

1/ تعريف اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

أ/ تعريف اعتراض المراسلات:

هو "عملية مراقبة سرية المراسلات السلكية واللاسلكية، وذلك في إطار البحث عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم أو في مشاركتهم في ارتكاب الجرائم"[4].

وقد اقتبس المشرع الجزائري هذا التعريف بشيء من التفصيل في المادة 65 مكرر5 من قانون الإجراءات الجزائية، إذا اعتبر عملية مراقبة المراسلات بأنها اعتراض أو تسجيل أو نسخ

[1] أسماء عنتر، المرجع نفسه، ص85.

[2] أسماء عنتر، المرجع نفسه، ص86.

[3] المرجع نفسه، ص84.

[4] براهيمي جمال، المرجع نفسه، ص88.

المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهذه المراسلات عبارة عن بيانات قابلة للانتهاج والتوزيع، التخزين، الاستقبال والعرض فبالرجوع لنص المادة، نلاحظ أن المشرع الجزائري حدد المراسلات التي تصلح أن تكون للاعتراض بتلك المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية دون أن يشير إلى طبيعة هذه المراسلات، مما يفتح المجال لمختلف الرسائل المكتوبة بغض النظر عن شكلها أو الدعامة أو الوسيلة المستعملة باستثناء الكتب والمجلات والرسائل والحوليات التي تعد مراسلات خاصة [1].

ب/ تسجيل الأصوات.

تسجيل الأصوات المقصود به تسجيل المتهم وشركائه عن واقعة معينة من الوقائع المنصوص عليها في المادة (65 مكرر5 ق إ.ج.ج) خلسة.

فبعدما أعطى المشرع للمتهم الحق في الصمت، فإنه وبشكل غير مباشر أورد استثناء عن هذا الحق بموجب المادة 65 مكرر السابق الذكر، أن أصبح من الممكن أخذ اعتراف الشخص ضد نفسه بشكل خفي ودون رضاه وموافقته عن طريق تسجيل كل ما يتفوه به من كلام بصفة خاصة أو سرية[2].

ج/ التقاط الصور:

لم يكتف المشرع بالسماح لقاضي التحقيق تسجيل الأصوات، بل مكنه أيضا من إمكانية التقاط الصور، فعدسة الكاميرا التي أصبحت من أفضل الأساليب لإثبات الحالة، بما تنقله من صور حية وكاملة صادقة لمكان معين أو لحدث معين أو واقعة معينة رأى المشرع توظيفها كعين من العيون التي لا تغفل في خدمته القضاء وكشف الحقيقة، فبموجب المادة 65 مكرر 5 السابقة الذكر سمح قانون الإجراءات الجزائرية الجزائري لقاضي التحقيق أن يمد عين الكاميرا إلى الأماكن الخاصة التي تعد مستودعات أسرار المعنيين بالمراقبة[3].

---

[1] المرجع نفسه، ص89.

[2] فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجزائية، مجلة العلوم الانسانية، عدد 33، جوان2010، كلية الحقوق والعلوم السياسية، جامعة منتوري قسنطينة، ص 237.

[3] فوزي عمارة، المرجع السابق، ص238.

فبموجب المادة 65 مكرر5 يسمح المشرع الجزائري لسلطات التحقيق والاستدلال إذا استدعت ضرورة التحري في الجريمة المتلبس بها، أو التحقيق في الجريمة الإلكترونية، اللجوء إلى إجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات والأصوات والتقاط الصور، والاستعانة بكل الترتيبات التقنية اللازمة لذلك من أجل الوصول إلى الكشف عن ملابسات الجريمة وإثباتها دون أن يتقيدوا بقواعد التفتيش والضبط المألوفة[1]

2/ شروط إجراء اعتراض المراسلات:

أوج المشرع الجزائري شروطا محددة لإجراء عملية اعتراض المراسلات وذلك تحت طائلة البطلان، وهذه الشروط هي:

أ- أن يصدر الأمر من وكيل الجمهورية أو قاضي التحقيق المختصين.

ب- أن يوجه الإذن لضابط الشرطة القضائية لا إلى الأعوان رغم أن الضباط يمكنهم تسخير الأعوان للقيام بهذه الإجراءات.

ج- أن تكون الجريمة المعنية بهذه الإجراءات من الجرائم المذكورة في المادة 65 مكرر5 دون سواها.

د- أن يكون هذا الإذن مكتوب وأن يتضمن بدقة المهام التي يقوم بها الضابط.

ه- أن يكون هذا الإذن محدد المدة فلا يجوز أن تتعدى المدة 4 أشهر مع إمكانية تمديدها وفق نفس الشروط.

و- تحرير محضر يتضمن كافة الأعمال والإجراءات التي قام بها.

[1] براهيمي جمال، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، ص140.

هذا بالنسبة للشروط الشكلية أما بالنسبة للشروط الموضوعية أن تكون الجريمة الواقعة على إحدى الجرائم المذكورة في نص المادة 65 مكرر5 بصفة عامة وبصفة خاصة الجرائم الماسة بالوثائق البيومترية الإلكترونية كونها محل دراسة[1].

3/ القيود الواردة على عملية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

تمت إحاطة عملية الاعتراض بعدد من القيود القانونية التي تضمن عدم تعسف السلطات العامة وتصون الحرية الفردية والتي نلاحظها فيما يلي:

أ/ الحصول على إذن من السلطة القضائية المختصة.

ب/ بسبب اللجوء إلى اعتراض أو مراقبة المراسلات ويقصد به المبرر البشري والضرورة الملحة التي تستدعي القيام بعملية اعتراض أو مراقبة المراسلات.[2]

ج/ تحديد الجرائم محل الاعتراض والمراقبة أن يكون مجال تطبيقها متوفرا على نوع محدد فقط وهو ما حددته المادة (64 مكرر 5) من قانون الإجراءات الجزائية.

د/ سرية الإجراءات وكتمان السر المهني أن تنفذ عملية الاعتراض في سرية تامة ودون علم أو رضا المشتبه فيه أو صاحب الأماكن، مع مراعاة عدم المساس بالسر المهني المقرر بنص المادة (45 فقرة4) ق.إج ج[3].

الفرع الثاني: إجراءات المتابعة من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

نص قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال أيضا على جملة من الإجراءات المستحدثة والخاصة بالتحري والتحقيق عن الجرائم الماسة بالتوقيع الإلكتروني والجرائم الماسة بالوثائق البيومترية الإلكترونية، كمراقبة الاتصالات الإلكترونية، حجز المعطيات

[1] نصرالدين هنوني ودارين يقدح،المرجع السابق، ص75.

[2] براهيمي جمال، المرجع نفسه، ص، ص،ص 94، 95، 96.

[3] المرجع نفسه، ص، ص 97-98.

المعلوماتية، جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وسنتكلم بمزيد من التفصيل عن كل إجراء فيما يلي[1].

أولا: مراقبة الاتصالات الإلكترونية.

تم النص على مراقبة الاتصالات الإلكترونية بموجب المادة الرابعة من الفصل الثاني من القانون 09-04 المذكور آنفا[2] في حين يفصل بالاتصالات الإلكترونية حسب المادة2 ومن نفس القانون سابق الذكر، أي تراسل او إرسال أو استقبال علامات أو إشارات أو كتابات إلكترونية، وبالتالي فإن المشرع الجزائري لم يحدد المقصود بمراقبة الاتصالات الإلكترونية وإنما اكتفى بتحديد مفهوم الاتصالات الإلكترونية[3].

1/ أسباب إباحة مراقبة الاتصالات الإلكترونية:

لم ينص المشرع الجزائري على إمكانية اللجوء إلى المراقبة بعد ارتكاب الجريمة والبحث عن حقيقة الوصول إلى مرتكبها فقط، بل أقر أيضا اللجوء إلى استعمال هذه التدابير كوسيلة وقائية للحماية من وقوع جرائم معينة هي الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة أو الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني ومن جهة ثالثة تهدف هذه الإجراءات إلى تعزيز التعاون الدولي في مجال مكافحة الإجرام المنظم في مجال المعلوماتية ذلك أن هذه الجرائم تعد من الجرائم العابرة للحدود الوطنية ولا ترتبط في كثير من الأحيان بمكان معين، ويكون ذلك في إطار المساعدة الدولية المتبادلة وفقا لما نص عليه القانون في هذا الشأن[4]

2/ الضمانات المقررة لتنفيذ مراقبة الاتصالات الإلكترونية تتم عملية تنفيذ باتخاذ الإجراءات التالية:

---

[1] شرف الدين وردة، بلجراف سامية، الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري، مجلة المنار للبحوث والدراسات القانونية والسياسية، العدد الثالث، ديسمبر 2017، جامعة محمد خيضر بسكرة، ص48.

[2] زبيحة زيدان، المرجع نفسه، ص127

[3] جبار فطيمة، مراقبة الاتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري بمجلة الدراسات القانونية المقارنة العدد الثالث، ديسمبر 2016 ص14.

[4] دنيا ثابت زاد، مراقبة الاتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والإنسانية، العدد السادس، جامعة تبسة، ص،ص 209-210.

* سرية الإجراءات: تتم العملية بسرية تامة سواء في مواجهة الأشخاص حيث تتم بدون علمهم، ودون رضاهم كما أنها تتم بسرية في مواجهة الكافة احتراما لمبدأ السر المهني المقرر في المادة 45 فقرة4 من ق إج.

* التسخير: حيث أنه يجوز لوكيل الجمهورية، أو لقاضي التحقيق، أو لضابط الشرطة القضائية أن يسخر عون مؤهل لدى هيئة مكلفة بالاتصالات سواء كانت عامة أو خاصة للقيام بهذا الإجراء.

* المحاضر: يحرر الشخص المكلف بالعملية محضرا يحوي العناصر الأساسية للعملية "التاريخ الساعة نسخ المراسلات أو الصور.... إلخ، ويودع المحضر لدى الجهة القضائية المكلفة، بمعنى وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق[1].

* حماية المعطيات المتحصل عليها: حيث جاء في المادة التاسعة 09 من القانون ى04/09 أنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق[2] عمليات المراقبة المنصوص عليها في هذا القانون وإلا في حدود الضرورية للتحريات أو التحقيقات القضائية، وهذا تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، في حال استعمال هذه المعطيات خارج هذه الحدود أي التحريات، أو التحقيقات القضائية[3].

* الإذن: أشار المشرع الجزائري في نص المادة 04 من القانون 04/09 أنه في حالة ما إذا تعلق الأمر بوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة يختص النائب العام لدى مجلس القضاء الجزائري يمنح ضباط الشرطة القضائية المنتمين للتهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته إذن لمدة (6) أشهر قابلة للتجديد، وذلك على أساس تقرير يبنن طبيعة الترتيبات المستعملة، والأغراض المنصوص عليها في الإجراءات الجزائية.[4]

ثانيا: تفتيش المنظومة المعلوماتية وحجز المعطيات المعلوماتية.

---

[1] جبار فطيمة، المرجع السابق، ص، ص، ص16-18-19.

[2] المرجع نفسه ص، ص 16- 18.

[3] المرجع نفسه، ص19.

[4] المرجع نفسه ، ص20.

1/ تفتيش المنظومة المعلوماتية:

تفتيش الأنظمة المعلوماتية وهو البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه أو هو البحث الدقيق والاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه سواء كان مسكنا أو جهاز حاسوب أو أنظمة أو الانترنت، وتفتيش النظم المعلوماتية هو إجراء يسمح بجمع الأدلة المخزنة او المسجلة بشكل إلكتروني ويستهدف ضبط أدلة الجريمة مثل البرامج غير المشروعة والملفات المخزنة في الحواسيب والمعطيات المعلوماتية والاتصالات الإلكترونية.[1]

ويقصد بالمنظومة المعلوماتية في التشريع الجزائري أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذ برنامج معين.[2]

أ/ سبب تفتيش منظومة معلوماتية:

يفترض أن التفتيش يجب أن يستند عند إجراءاته إلى مبررات توضح السبب والهدف منه، وتتمثل هذه المبررات فيما يأتي:

– وقوع جريمة معلوماتية:

يتعين لإجراء تفتيش المنظومات المعلوماتية أن تكون الجرائم قد وقعت فعلا يتعين أن تكون قد وقعت فعلا جريمة معلوماتية معينة فلا يمكن إجراء التفتيش من أجل جريمة محتملة الوقوع حتى ولو كانت هناك مؤشرات على جدية احتمال وقوعها[3] وهو شرط مستقى من طبيعة التفتيش باعتباره عملا من أعمال التحقيق الابتدائي وفي مفهوم القانون الجزائري فإننا نكون بصدد جريمة معلوماتية أو إحدى الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال، جرائم المساس بأنظمة المعالجة الآلية للمعطيات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام

[1] رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، جوان 2012، جامعة ورقلة، ص160

[2] رضا هميسي، المرجع السابق، ص161.

[3] علي حسن طوالبة، المرجع نفسه، ص62.

للاتصالات الإلكترونية، أو أي جريمة ترتكب عن طريق وسائل الإعلام الإلكترونية أو أية وسيلة اتصال أخرى كالهاتف النقال أو آلة تصوير رقمية، أو جهاز تسجيل[1].

– توجيه التهمة إلى شخص وإسنادها إليه:

يتعين للقيام بإجراء التفتيش بالإضافة لوقوع الجريمة أن يكون هناك اتهام موجه إلى شخص أو عدة أشخاص سواء بصفته فاعلا أو شريكا أو حائز الأشياء تتعلق بالجريمة من جرائم تكنولوجيا الإعلام والاتصال، معنى ذلك أن تتوفر في حق المراد تفتيشه دلائل قوية وكافية تدعو للاعتقاد بأنه ساهم في ارتكاب الجريمة المعلوماتية، ولا يقتصر الأمر على مجرد تجميع القرائن والأدلة التي تفيد وقوع الجريمة ونسبتها إلى فاعلها، بل يجب أن تتضمن كذلك المعلومات والقرائن التي تعزز موقف المشتبه فيه وتنفي عنه ارتكاب الجريمة[2].

ب/ خصوصية تفتيش نظم المعلوماتية:

ينصب التفتيش في الجريمة التقليدية على شخص المتهم أو غير المتهم وكذلك على مسكن المتهم وما في حكمه وملحقاته، أو على مسكن غير المتهم وما في حكم وملحقاته، لكن في الجريمة المعلوماتية فإن محل التفتيش هي كل مكونات الحاسوب سواء كانت مادية أو معنوية، وكذلك شبكات الاتصال الخاصة به،[3] ويقصد بالمكونات المادية للحاسوب " الأشياء الملموسة من أجزائه وأدواته التي تعمل بشكل متكامل لأداء مهمة في معالجة البيانات آليا"، في حين يقصد "بالمكونات المعنوية للحاسوب حيث يطلق عليها بالبرمجيات وهي بمثابة عصب الكمبيوتر إذ توفر إمكانات وسرعة فائقة في إنجاز المهام المطلوبة وتتمثل في نظم التشغيل وبرامج التطبيقات"[4]

ثالثا: جمع وتسجيل المعطيات لمحتوى الاتصالات في حينها:

---

[1] رضا هميسي، المرجع نفسه، ص164.

[2] المرجع نفسه، ص165.

[3] ليندا بن طالب، التفتيش في المنظومة المعلوماتية، مجلة العلوم القانونية والسياسية، العدد 16، جامعة مولود معمري تيزي وزو، 2017، ص492.

[4] يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، العدد48، جامعة باجي مختار عنابة، 2016، ص،ص84-85.

ينظم المشرع الجزائري ضمن قانون 09-04 سابق الذكر إجراء جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وجعله من التزامات مقدمي الخدمات في مساعدة السلطات، حيث لنص المادة 16 على أنه في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها.... ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزوها بطلب من المحققين، وكذلك المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

وأضافت المادة 12 على أنه زيادة على الالتزامات المنصوص عليها في المادة 11 من قانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، يتعين على مقدمي خدمات الانترنت ما يلي:

1/ التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة لمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

2/ وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها[1].

[1] شرف الدين وردة، بلجراف سامية، المرجع السابق، ص52.

المبحث الثاني: حجية الدليل الرقمي أمام القاضي الجزائي في الجرائم الماسة بالوثائق البيومترية.

يعد الدليل الرقمي دليلا مستحدثا وذو طبيعة معقدة وصعبة، حيث ترتكز عملية الإثبات الجنائي للجرائم المعلوماتية على الدليل الجنائي الرقمي باعتباره الوسيلة الوحيدة والرئيسية لإثبات هذا النوع من الجرائم لذلك يعد الإثبات الجنائي بالأدلة الرقمية من أبرز تطورات العصر الحديث في كافة النظم القانونية، تلك التطورات التي جاءت لتلائم الثورة العلمية والتكنولوجية والتقنية في عصرنا الحالي وهذا ما سوف سنتناوله في هذا المبحث: حجية الدليل الرقي أمام القاضي الجزائي في الجرائم الماسة بالوثائق البيومترية حيث تم التطرق لماهية الدليل الرقمي في المطلب الأول في حين المطلب الثاني مشكلة الدليل الرقمي وأثارها على الاقتناع الشخصي للقاضي الجزائي.

المطلب الأول: ماهية الدليل الرقمي:

أثرت الثورة المعلوماتية بشكل كبير خاصة على طرق الإثبات، حيث أصبحت الطرق التقليدية لا تتناسب مع الجرائم المعلوماتية لذلك ظهر نوع خاص من الأدلة يمكن الاعتماد عليها في إثبات الجريمة الإلكترونية وانطباقها على الجرائم الماسة بالوثائق البيومترية وهو ما يسمى بالدليل الإلكتروني لذا سنخصص في هذا المطلب تعريف الدليل الإلكتروني مع تبيان أنواعه وشروطه ومشروعيته.

الفرع الأول: مفهومه.

نظرا لكون الدليل الإلكتروني الوسيلة الوحيدة لإثبات الجرائم الإلكترونية، فكان من اللزوم تحديد تعريف وأنواع وشروط الدليل الإلكتروني

أولا: تعريفه.

يعرف الدليل الرقمي بأنه "الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة،[1] وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور والأصوات

[1] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2006، ص88.

والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه بشكل قانوني ويمكن الأخذ بالدليل الرقمي أمام أجهزة إنفاذ وتطبيق القانون[1]"

ثانيا: أنواعه.

تختلف الأدلة الرقمية باختلاف الوسائل التقنية المستعملة في الجريمة،فهذا ما سوف نتطرق إله من خلال الآتي:

1/ الأشرطة المغناطيسي:

إن الشريط المغناطيسي هو عبارة عن شريط بلاستيكي مغطاة بمادة قابلة للمغنطة قد يكون ملفوفا على بكرة، مثل تلك المستخدمة في أجهزة التسجيل الصوتي كالأسطوانة، وقد يكون داخل علبة على هيئة شريط الفيديو بها رأسي القراءة الكتابة، بحيث يسجل البيانات بها على شكل نقطة مغناطيسية على الشريط بشفرة خاصة تدل على البيانات المستخرجة من الحاسوب، ويستخدم هذا الشريط بشفرة خاصة تدل على البيانات المستخرجة من الحاسوب، ويستخدم هذا الشريط في تخزين البرامج والملفات المتتالية وتنظم المعلومات على الشريط على شكل وحدات خاصة تسمى كل وحدة منها حزمة وحجم الحزمة يحدده مستخدم الجهاز.[2]

2/ الأقراص المغناطيسية:

تعتبر الأقراص المغناطيسية المرنة من أشهر وسائط تخزين البيانات، نظرا لتميزها بالعديد من الخصائص المتعلقة بالاستخدام والأمان والسرعة لأن هذه الأخيرة تستخدم في حفظ البيانات الصغيرة والمتوسطة والضخمة، بسبب سهولة استخدامها وتداولها وهي نوعين قرص مرن وقرص صلب[3].

3/ الفيلم المصغر:

[1] ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص88

[2] المرجع نفسه، ص89.

[3] المرجع نفسه، ص89.

تعتبر هذه الأدلة شكلا مختلفا عن تكنولوجيا المخرجات التي تسجل فيها المعلومات والبيانات بدلا من تسجيلها على الورق، والمصغرات الفيلمية عبارة عن أفلام فوتوغرافية يتم استخدامها في تصوير صفحات البيانات مع تصغيرها لدرجة متناهية في الصغر عن طريق جهاز تحويل البيانات المسجلة على الأشرطة، والأقراص الممغنطة تتراوح سرعتها من عشرة ألاف إلى أربعين ألف سطر في الدقيقة الواحدة[1]

ثالثا: شروطه.

يتعين على القاضي لقبول هذه الأدلة كأساس تستند إليه الحقيقة في الدعوى العمومية سواء كان الحكم فيها بالإدانة أو البراءة توافر بعض الشروط أهمها:[2]

1/ أن تكون هذه الأدلة يقينية وهذا يستوجب أن تقترب نحو الحقيقة الواقعية قدر المستطاع وأن تبتعد عن الظنون والتخمينات.

2/ يتعين مناقشة الدليل الرقمي تطبيقا لمبدأ شفوية المرافعة، فإذا كانت مخرجات الرسائل الإلكترونية تعد أدلة إثبات قائمة في أوراق الدعوى في الجريمة المعلوماتية فإنه يجب مناقشتها أمام الخصوم إذ تنص المادة 212 من قانون الإجراءات الجزائية الجزائري في فقرتها الثانية على أنه: لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي فصلت المناقشة فيها حضوريا أمامه، فهذا يعني أنه للقاضي الاجتهاد في الحكم في الجرائم المعلوماتية وعدم الاعتماد على رأي الغير، إلا إذا كان الغير من الخبراء.

3/ يجب أن يكون الدليل الرقمي مشروعا ويقصد بذلك أن إجراءات جمع الأدلة الرقمية المتحصلة من الحاسب الآلي إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها، فإنها تكون باطلة ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجزائية[3].

---

[1] بلهادي حميد، حجية الدليل الرقمي في الإثبات الجنائي، مجلة البحوث والدراسات القانونية والسياسية، المجلد التاسع، العدد الأول، جامعة البليدة2، 2019، ص،ص، 17-18-19.

[2] نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، العدد11، جامعة باتنة،2017، ص919.

[3] نور الهدى محمودي، المرجع السابق، ص،ص 919- 920.

الفرع الثاني: مشروعيته.

لقد اختلفت الآراء حول مسألة مشروعية الدليل الجنائي الرقمي، وحول مدى إمكانية الأخذ به على إطلاقه أو أن تعتمد نسبيا، بمعنى هل القاضي حر في الأخذ بما يشاء من الأدلة الرقمية، أم أنه مقيد فيما قيده المشرع بالنص عن هذه الأدلة وذلك نظرا لوجود عدة اختلافات في النظم الإجرائية للإثبات الجنائي، فمنها ما تعرف بنظام الحر، ومنها ما تعرف بنظام الإثبات المقيد ومنها ما يأخذنا بالنظامين معا وسوف نحاول التطرق إلى هذه الأنظمة الإجرائية وإسقاطها على الدليل الرقمي على النحو الآتي بيانه:

أولا: حجية الدليل الرقمي في نظام الإثبات المقيد.

يقوم نظام الإثبات المقيد على مبدأ أساسا يتمثل في أن المشرع الجنائي يعد سلفا الوسائل ومختلف الطرق التي يعتمدها في إقامة الدليل الجنائي على مرتكبي الجرائم، فوفقا لهذا الاتجاه فإن المشرع هو الذي يحدد الأدلة التي يجوز للقاضي اللجوء إليها ويقدر قيمتها الإقناعية، بحيث يقتصر دور القاضي في هذا النظام على مجرد فحص الدليل والتأكد من توافر[1] الشروط التي حددها القانون، فلا سبيل للإسناد على دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات، كما لا دور للقاضي في تقدير القيمة الاستدلالية للدليل، حيث أن القانون يفيد القاضي بقائمة الأدلة التي حددت قيمتها الإثباتية[2].

ثانيا: حجية الدليل الرقمي في نظام الإثبات الحر:

يسود نظام الإثبات الحر في القوانين الإجرائية اللاتينية بحيث يتمتع القاضي بموجب هذا النظام بالحرية المطلقة في إثبات الوقائع المعروضة عليه ولا يلزمه القانون بأدلة معينة للاستناد عليها في تكوين قناعته الشخصية، وأن حجية الأدلة الإلكترونية لا تثير أي صعوبات متعلقة بمدى حرية تقديم الأداة لإثبات جرائم الحاسوب والانترنت، ولا بمدى حرية القاضي الجنائي في تقدير هذه الأدلة ذات الطبيعة الخاصة باعتبارها أدلة إثبات في المواد الجنائية أم لا، بل إن العنصر الأساسي وفق هذا المذهب هو مدى حرية قاضي الموضوع في تقدير هذه الأدلة، ومدى قبول الأدلة الناشئة عن الأدلة

[1] هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية، الطبعة الأولى، دار النهضة العربية، القاهرة 1997 ص22.

[2] هلالي عبد الإله أحمد، المرجع السابق، ص23.

أو الأدلة العلمية مثل أجهزة التصوير وأجهزة التنصت والتسجيل وغيرها من الوسائط الرقمية، كدليل قائم بذاته كاف لإثبات الإدانة أو البراءة وفي هذا الاتجاه لا تثور مشكلة مشروعية الدليل الرقمي من حيث الوجود باعتبار أن المشرع لم يعهد إليه مهمة تحديد قائمة أدلة إثبات، ولذلك فمسألة قبول الدليل لا ينال منها سوى مدى اقتناع القاضي به[1].

ثالثا:حجية الدليل الرقمي في نظام الإثبات المختلط.

يقوم النظام المختلط على أساس الجمع بين خصائص النظام المقيد ونظام الإثبات الحر ، إذ يعتمد أساسا أن القانون يحدد أدلة معينة لإثبات وقائع دون بعضها الأخر، وقد يحدد قبول الدليل شروط معينة في بعض الحالات، كما يعطي للقاضي الحرية في تقرير الأدلة القانونية أما بالنسبة للأدلة الرقمية فيرى الفقه بأن السجلات الإلكترومغناطيسية تكون غير مرئية، لذلك لا يمكن أن تطرح كدليل أمام جهات القضاء إلا إذا تم تحويلها إلى صورة مرئية عن طريق الطباعة وبالتالي يمكن قبول الدليل[2].

رابعا: موقف المشرع الجزائري من النص على الدليل الرقمي.

لم ينص المشرع الجزائري صراحة بخصوص الدليل الرقمي إلا أنه تم الاستناد في هذا الموضوع للمادة 212 من قانون الإجراءات الجزائية والتي طبق من خلالها مبدأ حرية الإثبات، لكن المشرع الجزائري أن هذا لا يكفي لوحده، ويواكب التطور الحاصل فيما بعد وضع القانون رقم 04/15 المؤرخ في 10 نوفمبر سنة 2004 المتمم والمعدل للأمر 156/66 المتضمن قانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ""ولقد جاء في عرض أسباب هذا التعديل مواكبة التطور التكنولوجي وانتشار وسائل الاتصال الحديثة التي أدت بدورها إلى ظهور أشكال جديدة للإجرام كجرائم المساس بالوثائق البيومترية الإلكترونية، وكان هذا القانون كنتيجة حتمية لما أفرزته ثورة تقنية المعلومات التي مست مصالح جديدة غير تلك التي يحميها قانون العقوبات، بعدها تدخل المشرع الجزائري لحماية التعاملات الرقمية حيث وضع القانون رقم: 09\04 المؤرخ في 5اوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم

[1] المرجع نفسه، ص24.

[2] المرجع نفسه، ص 25.

المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ومن خلال هذا القانون أدرج المشرع طريقة ضبط الأدلة الرقمية والتي تتخذ صورتين.[1]

1/ الصورة الأولى:تكمن في نسخ المعطيات محل البحث عن تخزين المعلومات الرقمية على أن تكون هذه المعطيات مهيأة بشكل يجعلها قابلة لحجزها ووضعها في أحراز حسب ما هو مقرر في قواعد تحريز الدليل المنصوص عليها في ق.إ. الجزائية.

2/ الصورة الثانية: تتمثل في الاستعانة بالتقنيات المناسبة لمنع الأشخاص المرخص لهن باستعمال المنظومة المعلوماتية من الوصول إلى المعطيات التي تحويها هذه المنظومة أو القيام بنسخها، ويكون ذلك في حالة صعوبة الحصول على هذه الأدلة وفقا للصورة الأولى.

وهذا يعني أن الدليل الرقمي يخضع في ضبطه وتحريزه إلى قواعد تحريز الأدلة الجنائية عموما، إلا أنه ونظرا إلى الطبيعة الخاصة له فإن عملية الحصول عليه تحتاج لبعض الإجراءات الخاصة التي تحافظ عليه وتحميه من العبث به وتغييره وهذا ما أشارت إليه المادة (06) في فقرتها الثالثة (ج) من القانون رقم 04/09.[2]

المطلب الثاني: مشكلات الدليل الرقمي وأثرها على الاقتناع الشخصي للقاضي الجزائي.

إن الدليل الإلكتروني يثير العديد من المشكلات، وهذه المشكلات تتعلق بطبيعته التكوينية من جهة وبإجراءات الحصول عليه من جهة أخرى فهذه المشكلات تنقص من حجيته في مجال الإثبات الجنائي إن لم يتم إيجاد حلول لها.

الفرع الأول: المشكلات الموضوعية للدليل الإلكتروني.

وهي في الغالب تتعلق بطبيعة الدليل في حد ذاته وهذا بسبب الخصائص التي يتميز بها هذا الدليل وهي كالآتي[3]:

---

[1] نور الهدي محمودي، المرجع نفسه، ص922.

[2] المرجع نفسه، ص 923.

[3] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة الاسكندرية، 2010، ص 251.

أولا/ الدليل الإلكتروني غير المرئي: فهذا الدليل عبارة عن سجل كهرومغناطيسي مخزن في نظام حاسوبي في شكل ثنائي، وبطريقة غير منظمة، فمثلا تتضمن الأقراص الصلبة مزيجا من بيانات مختلطة فيما بينها، والتي لا تكون كلها ذات صلة بالمسألة المطروحة بمعنى اختلاط الملفات البريئة مع الملفات المجرمة وبالتالي فالدليل الإلكتروني يختلف عن الآثار المادية الناتجة عن الجرائم التقليدية التي يسهل على رجال العدالة إثباتها، بعكس الجرائم الإلكترونية، حيث أن الدليل فيها عبارة عن نبضات إلكترونية كما أن هذا الدليل غالبا ما يكون مستقرا ويمكن تعديله والتلاعب فيه، مما يقطع الصلة بين المجرم وجريمته، كما أنه يشكل عائقا أمام رجال التحري والتحقيق، خاصة أنهم معتادون على الإثبات المادي للجرائم[1].

ثانيا/ مشكلة الأصالة في الدليل الإلكتروني: الأصالة في الدليل الإلكتروني لها طابع افتراضي لا يرتقي لمستوى الأصالة في الدليل المادي، باعتبار أن الدليل المادي ملموس، وهذه الأصالة أثارت العديد من المشكلات فيما يتعلق بالاعتداد بالنسخة التي تشكل دليلا كاملا.

ونجد أن موضوع الأصالة على المستوى القانوني جعل المشرع يعتمد على منطق افتراض أصالة الدليل الإلكتروني، حيث أن قانون الإجراءات الجنائية الفدرالي في الولايات المتحدة الأمريكية نص صراحة على قبول الدليل الإلكتروني على أنه مستند أصلي وهذا كاستثناء، ما دام أن البيانات قد صدرت من كمبيوتر أو جهاز مماثل له، وهذا سواء كانت هذه البيانات مطبوعة أو مسجلة على دعامة أخرى تعبر عن البيانات الأصلية بشكل دقيق، وبهذا تتساوى الكتابة المادية من حيث الأصالة مع الكتابة عبر الحاسوب رغم أن هذه الأخيرة مجرد نسخ للأصل الموجود رقميا في الحاسوب أو عبر الانترنت[2].

ثالثا/ الدليل الإلكتروني له طبيعة ديناميكية: معناه أن الدليل الإلكتروني ينتقل عبر شبكات الاتصال بسرعة فائقة، ومنه إمكانية تخزين المعلومات أو البيانات في الخارج بواسطة شبكة الاتصال عن بعد، وينتج عن هذا الأمر صعوبة تعقب الأدلة الإلكترونية وضبطها لأن هذا المشكل يستوجب القيام بإجراءات خارج حدود الدولة التي ارتكبت فيها الجريمة، كتفتيش نظام الحاسوب، وهذا كله يعيقه مشكل الحدود والولايات القضائية باعتبار أن هذا النوع من الإجراءات فيه مساس لسيادة الدولة

[1] عائشة بن قارة مصطفى، المرجع السابق، ص 252.

[2] المرجع نفسه، ص 253.

المقصودة، وهذا ما ترفضه غالبية الدول ما تأتى عنه إبرام العديد من الاتفاقيات والمعاهدات الدولية في مجال التعاون الدولي، الذي يهدف إلى التقريب بين القوانين الجنائية، بغرض تسهيل عملية جمع هذا النوع من الأدلة العابرة للحدود لمكافحة الجرائم الإلكترونية.[1]

الفرع الثاني: المشكلات الإجرائية للدليل الإلكتروني.

تتمثل في ما يلي:

أولا: ارتفاع تكاليف الحصول على الدليل الإلكتروني: في مجال الدليل الإلكتروني في أغلب الأحيان يتم الاعتماد على الخبرة للتعامل مع هذا الدليل الفني المتوفر في مجال تكنولوجيا المعلومات والانترنت، فالخبرة لها دور لا يستهان به خاصة مع نقص معرفة رجال القانون بالجوانب التقنية فيما تتعلق بالجرائم الإلكترونية، ولكن هذه الخبرة في المقابل تشكل عبئا بسبب حجم وضخامة المصاريف المتعلقة بها بغرض الحصول على الدليل الإلكتروني فالإشكال الأساسي هنا يتعلق بطبيعة الدليل الإلكتروني وما يتطلب إثباته من تكاليف باهظة، خاصة مع غياب مؤسسات متخصصة في هذا الشأن خصوصا في الدولة العربية التي تضطر للجوء لمؤسسات أجنبية، مما فعل التكاليف الخاضعة للسعر العالمي المقرر في اللوائح المالية لهذه المؤسسات.[2]

ثانيا: نقص المعرفة التقنية عند رجال القانون: إن الطبيعة الخاصة التي يتمتع بها الدليل الإلكتروني كان لها أثر على عمل رجال القانون سواء على مستوى التحقيق أو المحاكمة، وهذا راجع إلى أن الكشف عن الجرائم الإلكترونية وإثباتها يستلزم استراتيجيات خاصة، حيث أنه يترتب عليهم اكتساب مهارات خاصة في سبيل مواجهة تقنيات الحاسوب وشبكاته، لما يكتسي هذه التقنيات المعلقة بارتكاب هذه الجرائم من تعقيد الأمر الذي يستوجب معه الاعتماد على تقنيات جديدة تتماشى مع طبيعة هذه الجرائم، وهذا بغرض معرفة نوع الجريمة المرتكبة وشخصية مرتكبها، وكيفية ارتكابها، وكذلك ضبط الجاني والحصول على الأدلة التي تدينه[3].

[1] المرجع نفسه، ص 253.

[2] المرجع نفسه، ص 253.

[3] المرجع نفسه، ص254.

ملخص الفصل الثاني.

نستخلص من خلال هذه الدراسة أنه لمعالجة الجرائم الإلكترونية بصفة عامة والجريمة الماسة بالوثائق البيومترية بصفة خاصة لابد من اتباع مجموعة من إجراءات التحري والتحقيق إلى أن القوانين القائمة لا تكفي، مي حيث المبدأ لمجابهة هذا الشكل الجديد من الإجرام، ولا يقتصر هذا الأمر على القوانين العقابية الموضوعية فحسب، بل يشمل كذلك التشريعات الإجرائية، لأن معظم إجراءات التحقيق والمتابعة الجزائية التي تتضمنها التشريعات التقليدية لا تتلائم مع طبيعة هذه الجرائم ولا مع تقنيات ووسائل ارتكابها وهذا الأمر يشكل عقبة كبيرة أمام رجال الضبطية القضائية من عدة نواحي من بينها صعوبة إخضاع المكونات المنطقية للحاسوب الآلي للتفتيش والضبط وصعوبة معاينة الجرائم الإلكترونية.

الخاتمة

في ختام الدراسة المتعلقة بالحماية الجنائية للوثائق البيومترية اتضح لنا أن موضوع هذه الدراسة من المواضيع الحديثة وتعتبر ذات طابع خاص كونها تتعلق بالكيانات المعنوية الغير المادية وارتباطها بالتقنيات المعلوماتية، وينصب محل هذه الجريمة حول الوثائق البيومترية المتمثلة (بطاقة التعريف الوطنية البيومترية، رخصة السياقة البيومترية الإلكترونية، وكذا جواز السفر البيومتري الإلكتروني) حيث تمتاز هذه الأخير بخصائص تجعلها صعبة التتبع والرصد والإثبات زيادة على ذلك عجز النصوص القانونية التقليدية على متابعة والتحري في الجريمة الماسة بالوثائق البيومترية الإلكترونية ومن خلال دراستنا توصلنا للنتائج التالية:

1. محل الجريمة الماسة بالوثائق البيومترية الالكترونية ينصب على الكيان المعنوي.
2. رغم اجتهاد وتدارك المشرع الجزائري الفراغ القانوني في مجال الاجرام المعلوماتي، إلا أنه لم يستطع التصدي لهذه الجريمة (الجرائم الماسة بالوثائق البيومترية الالكترونية).
3. المشرع الجزائري لم يشرع قانونا خاصا قائم بذاته للتحكم بهذه الجريمة كونها حديثة، ويتم الاعتماد على القوانين الأساسية.
4. القوانين الجنائية القائمة لا تكفي من حيث المبدأ لمجابهة هذا الشكل الجديد من الاجرام، وإلا أنه هناك جدل فقهي حول إمكانية تطبيق النصوص الموضوعية العقابية للجرائم التقليدية (التزوير، الإتلاف، السرقة).
5. محاولة المشرع الجزائري استدراك الوضع وسن تشريع جديد يتجاوب مع الطبيعة الخاصة لهذه الجرائم الحديثة، حيث قام بتعديل قانون العقوبات بموجب القانون رقم 15/04 مستحدثا فيه جملة من النصوص جرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات وتم إصدار قانون 07/18 المتضمن حماية المعطيات ذات الطابع الشخصي للأشخاص الطبيعيين.
6. قصور القوانين الإجرائية إذ أن معظم إجراءات التحقيق والمتابعة الجزائية وأحيانا تتعارض مع طبيعة الوسائل المستخدمة لتنفيذ الجرائم التي يكون محلها المعلومات أو البيانات وهذا الأمر يشكل عقبة كبيرة أمام رجال الضبطية القضائية.
7. قبول الدليل الالكتروني بوصفه وسيلة إثبات أمام القضاء الجزائي من عدمه يتوقف على عنصرين أساسيين الأول هو المشروعية والثاني في الحجة والمصداقية.

في خلاصة ما توصلنا يمكن تصنيف جملة من التوصيات التي قد تساهم في التقليل من الآثار السلبية لكثير من التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة، تتمثل هذه التوصيات فيما يلي:

1. ندعو المشرع الجزائري إلى إصدار تشريع خاص ومستقل للجرائم الماسة بالوثائق البيومترية الالكترونية يوضح فيه الطبيعة الخاصة لهذه الجرائم ووضع عقوبات خاصة لهذه الجريمة تتلاءم وإياها.
2. ينبغي على المشرع التدخل لمعالجة هذا القصور في النصوص الحالية وذلك باستحداث قواعد قانونية موضوعية وإجرائية يكون مجالها أوسع وأساسها أنجع.
3. إحداث تعاون قضائي دولي يساهم في مواجهة هذه الظاهرة الجرمية المستحدثة.
4. ضرورة التدخل من قبل المشرع الجزائري بأساليب تحفظية ووقائية أكثر فعالية لتصدي هذه الجريمة.
5. تعزيز مستوى الأمان والحماية للوثائق البيومترية.
6. تجريم أي فعل يمس بالوثائق البيومترية الإلكترونية.

قائمة المصادر

والمراجع

أولا المصادر

أ- القوانين والأوامر:

1. الأمر 155/66 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.
2. الأمر 156/66 المؤرخ 08 جوان 1966 المتضمن قانون العقوبات المعدل والمتمم.
3. 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 العدد47 المؤرخة في 16 أوت 2009.
4. القانون رقم 14-03 المؤرخ في 2014/02/24 المتعلق بسندات ووثائق السفر، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 16 الصادر في 2014/03/23.
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 الديموقراطية الشعبية العدد34المؤرخة في 10 يونيو سنة 2018.

ب- المراسيم:

1. المرسوم الرئاسي رقم 143-17 المؤرخ في 21 رجب 1483 الموافق لـــ 18 أفريل 2017 المتعلق بتجديد كيفيات إعداد بطاقة التعريفة الوطنية وتسليمها، الجريدة الرسمية للجمهورية الجزائرية الديموقراطية الشعبية العدد 25 الصادرة بتاريخ 19 أفريل 2017.
2. المرسوم التنفيذي رقم 58-16 المؤرخ في 2016/02/03 المتعلق بشروط إعداد وإصدار جواز السفر الاستعجالي، الجريدة الرسمية للجمهورية الجزائرية الديموقراطية الشعبية العدد 07 الصادر في 2016/02/07.

ج- المناشير:

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

ثانيا المراجع

أ- الكتب

1. أمين طعباش، الجماية الجنائية للمعاملات الإلكترونية، ط01، مكتبة الوفاء القانونية، الإسكندرية، 2015.
2. أحمد غازي، ضمانات المشتبه فيه أثناء التحريات الأولية، دار هومة (ط.3)، الجزائر 2011.
3. أمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، (ط2)، دار هومة الجزائر، 2010.
4. أحمد عاصم عجيلة، الحماية الجنائية للمحررات الالكترونية، دار النهضة العربية، القاهرة، مصر، 2014.
5. أسامة أحمد المناعسة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة، ط 1، دار الثقاف للنشر والتوزيع، عمان، 2014.
6. الحلبي محمد علي سالم، الوجيز في أصول المحاكمات الجزائية، ط 1، دار الثقافة للنشر، الأردن، 2005 .
7. بلحاج العربي، أبحاث ومذكرات في قانون الفقه الإسلامي، ديوان المطبوعات الجامعية، بن عكنون، الجزائر 1996.
8. حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، القاهرة، 2013.
9. حجازي عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، القاهرة، 2002.

10. حجازي عبد الفتاح بيومي حجازي، الحكومة الالكترونية ونظامها،(د.ط)،الكتاب 2، دار الفكر الجامعي، الإسكندرية، 2004
11. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، 2011.
12. خالد محمد المهيدي، التحقيق الجنائي العملي في الجريمة التقليدية والمعلوماتية، ط 2، دار العزيز للطباعة والنشر، دبي،2012.
13. رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط 1، منشورات الحلبي الحقوقية، بيروت، 2012.
14. زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر،2011.
15. ضياء مصطفي عثمان، السرقة الالكترونية، الطبعة الأولى، الأردن دار النفائس للنشر والتوزيع.
16. طلال أبو عفيفة، شرح قانون العقوبات القسم العام، الطبعة الأولى، دار الثقافة، الأردن 2000.
17. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دار النهضة العربية، القاهرة، 2000.
18. عبد الرحمان خلفي، الإجراءات الجنائية في التشريع الجزائري والمقارن، ط 2، دار بلقيس، الجزائر 2016.
19. عبد اللهأوهايبية، شرح قانون الإجراءات الجزائية، (د.ط)، الجزائر، دار هومة، 2005.
20. عبد العزيز سعد، جرائم التزوير وخيانة الأمانة، واستعمال المزور، دار هومة. الجزائر، (د.ط)، 2005.
21. عبد الإله هلالي،إلزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، (د.ط)، دار النهضة العربية، القاهرة، 2000.
22. علي حسين الطوالبة. التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة. عالم الكتاب الحديث. أربد، الطبعة الأولى 2004.

23. شيماء عبد الغني محمد عطاالله، الحماية الجنائية للتعاملات الإلكترونية، دار النهضة العربية، مصر، سنة 2013.

24. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2010.

25. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت. دار الكتب القانونية، مصر، 2006.

26. محمود حماد مرهج الهيثي، جرائم الحاسوب، ماهيتها، موضوعها، أهم صورها و الصعوبات التي تواجهها، ط 1، دار المناهج، 2006.

27. محمود نجيب حسني، النظرية العامة للقصد الجنائي، (د.ط)، دار النهضة العربية، القاهرة 1988.

28. منصور دحماني، الوجيز في القانون الجنائي العام (د.ط)، دار العلوم للنشر والتوزيع ،عنابة 2006.

29. محمود نجيب، شرح قانون العقوبات القسم الخاص، دار النهضة العربية القاهرة، (ط.4)، مصر،سنة 2012.

30. مدحت عبد الحليم رمضان. الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية. القاهرة 2000.

31. محمد أمين الشوابكة، جرائم الحاسوب والأنترنت، الجريمة المعلوماتية، ط ،1 دار الثقافة للنشر والتوزيع، الأردن 2007.

32. محمود خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائي المقارن، د.ط، دار الجامعة الجديدة، الإسكندرية 2007.

33. محمد فهمي الموسوعة الشاملة لمصطلحات الحاسب الالكتروني،د.ط، مطابع المكتب المصري الحديث. القاهرة، 1991.

34. نبيلة هبة هروال، الجوانب الجزائية لجرائم الانترنت، ط ،1 دار الفكر الجامعي، مصر،2007.

35. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2005.

36. هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية،ط01، دار النهضة العربية، القاهرة، 1997.

37. هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.

38. هنوني نصر الدين ويقدح دارين، الضبطية القضائية في القانون الجزائري، ط 2، دار هومة, الجزائر، 2011.

39. ياسر محمد الكومي محمود أبو حطب، الحماية الجنائية والأمنية للتوقيع الإلكتروني، منشآت المعارف، الإسكندرية، 2004.

ب-الرسائل الجامعية

- **أطروحات الدكتوراه:**

1. براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة دكتوراه. جامعة مولود معمري تيزي وزو 2018.

2. شول بن شهرة، الحماية الجنائية للتجارة الإلكترونية، أطروحة دكتوراه في علوم تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم حقوق، جامعة محمد خيضر، بسكرة.

3. صالح شنين، الحماية الجنائية للتجارة الإلكترونية – دراسة مقارنة، أطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بلقايد تلمسان، 2012،

- **مذكرات الماجستير**

1. جدي نسيمة، مذكرة ماجستير بعنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات، جامعة وهران، 2014.

2. سعيداني نعيم آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية تخصص جنائي كلية الحقوق والعلوم السياسية جامعة الحاج لخضر باتنة 2012.

3. معتوق عبد اللطيف. مذكرة ماجستير بعنوان الإطار القانوني لمكافحة الجرائم المعلوماتية في التشريع الجزائري والتشريع المقارن جامعة الحاج لخضر باتنة 2011.

ج – المجلات:

1. أحمد بن مسعود جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري مجلة الحقوق والعلوم الإنسانية العدد الأول جامعة الجلفة 2017.
2. أسماء عنتر مكافحة الجرائم المستحدثة في التشريع الجزائري (التسرب نموذجا) مجلة القانون العام الجزائري والمقارن العدد 6 / 2017 جامعة عبد الحميد بن باديس، مستغانم.
3. براهيمي جمال مكافحة الجرائم الالكترونية في التشريع الجزائري المجلية النقدية كلية الحقوق والعلوم السياسية جامعة مولود معمري تيزي وزو.
4. بلهادي حميد،حجية الدليل الرقمي في الإثبات الجنائي مجلة البحوث والدراسات القانونية والسياسية المجلد التاسع العدد الأول جامعة البليدة 2، 2019.
5. تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون رقم 18-07، دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد04، جامعة يحي فارس، المدية، 2019.
6. حابس يوسف زيدات، مدى استيعاب النصوص التقليدية للسرقة الإلكترونية، دراسة مقارنة، مجلة مركز حكم القانون ومكافحة الفساد، العدد09، دار جامعة حمدين خليفة للنشر، 2019.
7. حمودي ناصر. الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري المجلة الأكاديمية للبحث القانوني العدد 2 جامعة آكلي محند أولحاج البويرة 2016.
8. جبار فطيمة. مراقبة الاتصالات الإلكترونية بين الحظر والإباح في التشريع الجزائري مجلة الدراسات القانونية المقارنة العدد الثالث ديسمبر 2016.
9. دنيا ثابت زادا، مراقبة الاتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والإنسانية، العدد06، جامعة تبسة.
10. رزيقة مخناش، الخدمة العمومية الإلكترونية على مستوى البلدية في الجزائر، مجلة الدراسات القانونية والسياسية، العدد 02، جوان 2006، جامعة محمد لمين دباغين، سطيف.

11. رمزي بن صديق، تزوير المحررات الالكترونية بين قابلية الخضوع للقواعد التقليدية وضرورة مراعاة الخصوصية مجلة الاجتهاد للدراسات القانونية والاقتصادية العدد 02 المركز الجامعي لتامنغست 2018.
12. رابح وهيبة الجريمة المعلوماتية في التشريع الاجرائي الحزائري مجلة الباحث للدراسات الأكاديمية العدد 4 جامعة عبد الحميد بن باديس مستغانم 2014.
13. رضا هميسي تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية جوان 2012 جامعة ورقلة.
14. شرف الدين وردة، بلجراف سامية، الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري، مجلة المنار للبحوث والدراسات القانونية والسياسية العدد 3 ديسمبر 2017 جامعة محمد خيضر بسكرة.
15. طعباش عز الدين، الحماية الجزائرية للمعطيات الشخصية في التشريع الجزائري، دراسة في ظل قانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المجلة الأكاديمية للبحث القانوني العدد 02/ 2018.
16. عبد الله حسين علي محمود إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، محور القانون الجنائي دبي 28 أفريل 2008.
17. عزالدين عثماني، عفاف خذيري، الحماية القانونية للمعطيات ذات الطابع الشخصي في التشريع الجزائري، دراسة في ظل القانون رقم 18-07، المجلة الدولية للبحوث القانونية والسياسية، العدد 01، جامعة العربي التبسي، تبسة2020.
18. فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور و----- كإجراءات تحقيق قضائي في المواد الجنائية مجلة العلوم الإنسانية العدد 33 جوان 2010 كلية الحقوق والعلوم السياسية جامعة منتوري قسنطينة.
19. قهوجي علي عبد القادر الحماية الجنائية لبرامج الحاسب، بحث منشور بمجلة الحقوق للبحوث القانونية والاقتصادية، كلية الحقوق جامعة الإسكندرية 1992.
20. كعواش رؤوف الإدارة الالكترونية لجوازات السفر البيومترية في الجزائر، مجلة تاريخ العلوم، العدد الثامن الجزء الأول كلية الحقوق والعلوم السياسية جامعة جيجل.

21. ليندا بن طالب، التفتيش في المنظومة المعلوماتية، مجلة العلوم القانونية والسياسية، العدد16، جامعة مولود معمري تيزي وزو، 2017.

22. نور الهدى محمدي، حجية الدليل الرقمي في اثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، العدد الحادي عشر جامعة باتنة 2017.

23. يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، عدد48، جامعة باجي مختار عنابة، 2016.

ملخص:

هدفت هذه الدراسة إلى التعرف على مدى حماية الوثائق البيومترية الالكترونية من قبل المشرع الجزائري، حيث تجلت هذه الحماية بتوفير حماية جزائية موضعية وإجرائية في النصوص القوانين الأساسية، إلا أنه باتت هذه القواعد الموضوعية والإجرائية المقرر لمتابعة الجرائم التقليدية لا تتلاءم مع طبيعة هذا النوع من الإجرام ولا تعتبر كافية لبلوغ الهدف الذي تتطلع إليه، غير أن محدودية هذه القوانين دفع المشرع إلى وضع قانون خاص والمتمثل في القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

والقانون 07/18 المتضمن حماية المعطيات ذات الطابع الشخصي للأشخاص الطبيعيين ونظرا للتطورات السريعة والمستمرة التي تعرفها هذه الظاهرة، لابد من التفكير من قبل المشرع الجزائري في التوجه نحو التعاون التشريعي والقضائي لوضع نصوص خاصة تجرم الجرائم الماسة بهذه الوثائق سابقة الذكر ووضع عقوبات خاصة لهذه الجريمة تتلاءم وإياها.

Summary

The aim of this study is to identify the extent to which electronic biometric documents are protected by the Algerian Legislature.this protection is reflected in the provision of objective and procedural Penal protection in the basic laws. however, these substantive and procedural rules established for the follow-up to traditional crimes are not compatible with the nature of this type of crime and are not considered sufficient to achieve the objective to which it aspires. however, the limitations of these laws have led the Legislature to draft a special law, namely, Act No. 04/09, containing the rules for the prevention and control of crimes related to information and Communication Technology. In view of the rapid and ongoing developments in this phenomenon, the Algerian Legislature must consider moving towards legislative and judicial cooperation to establish special provisions prohibiting serious crimes against these aforementioned documents and to establish appropriate special penalties for such crimes.

الفهرس

الفهرس: