وزارة التعليـــم العالـــي والبحث العلمـــي
جامعـــة العربـــــي التبســـــي –تبســـــة–
كليـــة الحقـــــوق والعلوم السياسية
قســـــم الحقـــــوق

آليات مكافحة جريمة التزوير الالكتروني

أطـــروحة لنيـــل شهـادة دكتـــوراه العلوم فـي القانـــون الجنائي

إعداد الطالبـــــة:
وفـــــاء صدراتي

إشـــراف الأستاذ الدكتور:
الطاهـــــر دلول

لجنـــــــة المنـــاقشـــــة:

الإسم واللقب	الرتبة	الجامعة الأصلية	الصفة
سعدي حيدرة	أستاذ التعليم العالي	جامعة العربي التبسي –تبسة–	رئيسا
الطاهر دلول	أستاذ التعليم العالي	جامعة العربي التبسي –تبسة–	مشرفا ومقررا
الأخضربوكحيل	أستاذ التعليم العالي	جامعة العربي التبسي –تبسة–	عضوا مناقشا
السايح بوساحية	أستاذ محاضر "أ"	جامعة العربي التبسي –تبسة–	عضوا مناقشا
عثامنية كوسر	أستاذ محاضر "أ"	جامعة عباس لغرور –خنشلة–	عضوا مناقشا
آمنة بن الطاهر	أستاذ محاضر "أ"	جامعة العربي بن مهيدي –أم البواقي–	عضوا مناقشا

السنة الجامعية: 2020 – 2021

شكر وتقدير

الحمد لله الذي رزقنا هذا دون حول ولا قوة منا،اللهم اجعله علما نافعا

وارزقنا به رزقا واسعا وبارك لنا فيه.

كما أتقدم بخالص الشكر والعرفان إلى أستاذي البروفيسور: الطاهر دلول

على تفضله بقبول الإشراف على هذه الأطروحة وتقديم التوجيه إلى غاية إنهائها.

كما أشكر أعضاء اللجنة الموقرة لقبولهم مناقشة هذه الأطروحة.

وشكري وتقديري موصول لكل من قدم لي يد العون من قريب أو بعيد في انجاز هذا العمل.

إهداء

أهدي هذا العمل المتواضع

إلى عائلتي وكل من تمنى لي التوفيق والنجاح.

مقدمة

أولا:التعريف بالموضوع

إن ثورة المعلومات والتقنيات الحديثة التي لم تشهد لها البشرية مثيلا من قبل قد فرضت نفسها على واقع الحياة المعاصرة، فقد دخلت التكنولوجيا جميع مجالات الحياة،إلا أن التطور الحاصل في تكنولوجيا المعلومات وظهور الشبكة العالمية للانترنت بقدر ما سهلت سبل الحياة واختصرت الوقت والجهد وما قدمته للبشرية من تسهيلات وخدمات وإيجابيات غيرت حياة الشعوب وساهمت في تطورها ورقيها، بقدر ما كان لها جانب سلبي أثر على حياة الناس ومصالحهم ومصالح الدول، وتتمثل ذلك في إساءة البعض استخدام هذه التكنولوجيا وتطويع الانترنت وغيره من الوسائل الالكترونية وكذا ارتكاب نوع جديد من الجرائم وهي الجرائم الالكترونية، والتي تتم عبر معدات وأجهزة الكترونية أو باستخدام شبكة الانترنت لارتكابها.

وتعد شبكات المعلومات ونظم التبادل الالكتروني للبيانات تطبيقا للاستخدام الحديث لهذه التكنولوجيا، وهو ما أدى إلى ظهور وسائل وأساليب الكترونية تقوم في كثير من الأحيان بأداء وظائف الوسائل التقليدية كالمحررات الالكترونية التي تتيح انجاز المعاملات بين الأفراد والمؤسسات والتي تعد أحد الأدوات المهمة التي يتم استخدامها في تنفيذ فكرة الحكومة الالكترونية، لما لها دور كبير في توفير النفقات والوقت والمجهود، وتذليل العقبات والحد من الأنظمة البيروقراطية في تسيير شؤون الدولة والمواطنين.

إلا أن استعمال هذه الوسائل لا يخلو من المخاطر التي تقع عليها ولعل أهمها التزوير وتغيير في مضمون هذه المحررات، والتي تستوجب أن تكون بصدد مواجهة حقيقة لها، وهذا ما يدعو إلى ربط الصلة بين المحررات الالكترونية والمصالح التي ترتبط لها هذه المحررات، والتشريعات الجنائية الخاصة بحمايتها، ولهذا يجب العمل على حماية المحررات وصيانتها وعدم المساس بها ومنع تزويرها، مما يكفل للأفراد الطمأنينة واستقرار المعاملات، كما أنه يؤدي إلى أن يصبح في النهاية دليلا قابلا للإثبات شأنه شأن المحرر الورقي، وهو ما يؤدي إلى استقرار النظام القانوني وقلة المنازعات بين أطرافه.

وقد تدخلت التشريعات في مختلف دول العالم لإعطاء قيمة إثباتية للمحررات الالكترونية تساوي قيمة المحررات الورقية، ، لأن غير ذلك يجعل المحررات التقليدية في وضع أعلى درجة من المحررات الالكترونية من حيث طرق الإثبات، مما يعرقل تطور التعامل عبر الوسائل الالكترونية.

وفي ضوء تعاظم استخدام التعاملات الالكترونية ظهرت حاجة المجتمع الدولي إلى الأحد بفكرة إحداث تعديلات في القوانين السارية، والأخذ بفكرة المحرر الالكتروني وتنظيم تطبيقاته، وضمان عدم المساس به قانونيا أو فنيا وإضافة القوة القانونية له في الإثبات.كما أن التوسع في استخدام المحررات الالكترونية في كثير من المجالات، دفع مجرمو المعلوماتية لارتكاب جرائمهم، خاصة جريمة التزوير مما يهدد الثقة في التعامل بتلك المحررات، ومدى حجيتها في الإثبات، ما يدفع إلى ضرورة وضع آليات لمكافحة هذا السلوك الإجرامي وذلك بالنص على تجريمه والعقاب عليه.

ثانيا:أهمية الموضوع: تظهر أهمية موضوع "آليات مكافحة جريمة التزوير الالكتروني" في عدة أوجه يمكن إيجازها فيما يلي:

1- تظهر أهمية دراسة "آليات مكافحة جريمة التزوير الالكتروني" التي تنبع من أهمية موضوع الجرائم التي ترتكب بواسطة أجهزة الحاسب الآلي وتقنياتها، لاسيما في ظل التطور السريع والمتسارع في استخدام هذه الأجهزة والانترنت، والغموض الذي يحيط بجريمة التزوير الالكتروني، حتى في الدول التي أدخلت في تشريعاتها أنماط هذه الجرائم، خاصة وأنها تتم عن طريق استخدام التقنيات الحديثة والمعاصرة، وهذا ما جعل التصدي لها بالآليات اللازمة يكتسب أهمية خاصة، ومن ثم اتخاذ المسائل اللازمة لحماية المحررات والوثائق الالكترونية تجريما ومكافحة ومنعا.

2-إن جريمة التزوير الالكتروني لها معالمها الخاصة إذ ترتكب من طرف مجرمين ذوي كفاءة عالية وتتم باستخدام تقنيات حديثة ومعاصرة، ما يجعل إثباتها صعب، كما أن معظم الدراسات والأبحاث القانونية التي عنيت بالجرائم الالكترونية عموما ركزت على الجانب الموضوعي فقط، في حين إثباتها ومكافحتها يحتاج إلى آليات إجرائية معقدة غير المعروفة في الجرائم التقليدية من خبرة وتفتيش وتسرب واعتراض ومراقبة، والتي تمس بالحق في الخصوصية، وهذا بسبب خصوصية هذا النوع من الجرائم أيضا.

3-نظرا للتوسع المتزايد في استخدام المحررات الالكترونية في مجالات عديدة، ازداد معه جرم التزوير هذا، ما يهدد الثقة في التعامل بتلك المحررات، وهذا أثار معه الكثير من الجدل والنقاش سواء حول حجية هذه المحررات في الإثبات، أو حول مدى تطبيق نصوص قانون العقوبات الخاصة بجريمة التزوير التقليدية، وطرق التزوير التي من هنا جاءت الضرورة الملحة لحمية المتعاملين بهذه المحررات وفرض الثقة على التعامل بها.

4-إن هذه الدراسة جاءت في وقت تسعى فيه العديد من الدول إلى إعادة النظر في قوانينها الإجرائية الجزائية مسايرة للتطورات التكنولوجية من أجل تقديم الآليات اللازمة لمواجهة جريمة التزوير الالكتروني واقتراح الحلول القانونية المناسبة لهان وتغطية الفراغ التشريعي في هذا المجال، لمواجهة الإجرام الالكتروني المتطور.

ثالثا: أسباب اختيار الموضوع: دفعنا إلى اختيار الموضوع عدة أسباب منها ما هو موضوعي ومنها ما هو ذاتي:

1-الأسباب الموضوعية:تتمثل في

أ-تعد الجرائم الالكترونية، وعلى رأسها جريمة التزوير الالكتروني، إحدى أخطر الظواهر الإجرامية المستحدثة، حيث أنه يسهل ارتكابها وتنفيذها الذي لا يستغرق غالبا إلا دقائق معدودة، وأحيانا تتم في بضع ثوان، كما أن محو آثار هذه الجريمة وإتلاف أدلتها غالبا ما يلجأ إليه الجاني عقب ارتكابه للجريمة، إضافة إلى أن مرتكبي الجريمة يلجأون دائما إلى تخزين البيانات المتعلقة بأنشطتهم الإجرامية في أنظمة الكترونية مع استخدام شفرات أو رموز سرية لإخفائها عن أجهزة العدالة، مما يثير مشكلات كبيرة في جمع الأدلة وإثبات هذه الجرائم،وهذا ما جعلنا نبحث في هذا الموضوع لتوضيح معالم هذه الجريمة، وكذا الوقوف عن الجهود المبذولة للحد من هذه الجريمة على الصعيدين الوطني والدولي.

ب -إن خطورة هذه الجرائم، و سرعة انتشارها كان السبب في اختيارنا لهذا الموضوع من بين جملة من الجرائم التي جرمتها التشريعات ثم وصف الجرائم الالكترونية، خاصة وأن هذه الجريمة ترتكب من قبل عصابات متخصصة ومتمرسة.

ج- بعد التطور الذي شهده العالم بشكل هائل ومتسارع في التكنولوجيا، أصبح الاعتماد على التقنية المعلوماتية الحديثة سواء في المؤسسات المالية أو المرافق العامة أمرا حتميا، ومن هنا دعت الضرورة إلى تبني ما يعرف بمصطلح "الحكومة الالكترونية" من خلالها توسيع الاعتماد على المحررات الالكترونية، ومن هنا كان لزاما من التطرق لموضوع تزويرها، ومدى تجريمه وكذا وضع العقاب على كل اعتداء من شأنه المساس بهذه المحررات.

2-الأسباب الذاتية:تتمثل في

أ-الرغبة الذاتية في البحث في مجال المعلوماتية، خاصة وأن هذه الدراسة تندرج تحت فرع جديد من فروع القانون، وهو القانون المعلوماتي إن صح التعبير الذي بدأ يفرض قواعد على الفروع المختلفة للقانون الجنائي، الذي يناول جرائم لم تكن معهودة من قبل في القانون الجنائي التقليدي.

ب-الرغبة في إثراء المكتبة القانونية بمراجع تخص الجرائم الالكترونية عموما، وجريمة التزوير الالكتروني على وجه الخصوص، حيث أن لم يتناول هذا الموضوع بشكل كبير، وإن وجدت فإنها تعالج الجانب الموضوعي، ما نتج عنه قلة وندرة المراجع والمؤلفات التي تعرضت للجانب الإجرائي، وهو ما أثار اهتمامنا للبحث وإثراء النقاش القانوني في هذا الموضوع.

رابعا: الدراسات السابقة:

يعد موضوع آليات مكافحة جريمة التزوير الالكتروني من المواضيع الحديثة، إلا أن هناك بعض الدراسات التي تطرقت إلى هذا الموضوع من بينها:

1-الهام بن خليفة، الحماية الجنائية للمحررات الالكترونية من التزوير، أطروحة دكتوراه علوم، جامعة الحاج لخضر، باتنة، الجزائر، 2016.حيث تناولت الباحثة موضوع الدراسة من خلال بابين تطرقت في الباب الأول للحماية الموضوعية من التزوير.أما الباب الثاني تطرقت فيه للحماية الإجرائية للمحررات الالكترونية من التزوير.

2-براهمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية أطروحة دكتوراه علوم، جامعة محمد خيضر، بسكرة، الجزائر، 2015.وقسمت الدراسة إلى فصل تمهيدي وبابين ،تمت الإشارة في الفصل التمهيدي إلى تأثير المعلوماتية على الأنظمة القانونية،أما الباب الأول خصص

لدراسة الوثيقة المعلوماتية محل التزوير،في حين تناولت الباحثة في الباب الثاني الصيغ التشريعية في تجريم تزوير الوثيقة المعلوماتية.

3-حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه علوم جامعة الحاج لخضر، باتنة، الجزائر، 2016.وقسم الباحث الدراسة إلى ثلاث فصول ،تطرق في الفصل الأول للإطار المفاهيمي للجريمة المعلوماتية،أما الفصل الثاني فتناول الباحث فيه مسألة شرعية إجراءات البحث والتحقيق في الجرائم المعلوماتية والجهات المختصة بتنفيذها ،في حين خصص الفصل الثالث لدراسة الإجراءات الخاصة بالبحث والتحقيق في الجرائم المعلوماتية وآثارها.

خامسا:أهداف الدراسة: ترمي هذه الدراسة إلى تحقيق عدة أهداف يمكن إيجازها فيما يلي:

1-الإجابة عن إشكالية البحث وتساؤلاته الفرعية.

2-استخلاص أهم الفروق الموجودة بين الشكل التقليدي للتزوير، والشكل المستحدث للتزوير، من خلال مقابلة جميع العناصر المكونة لكليهما.

3-عرض الجهود الدولية والإقليمية والدولية لمكافحة جريمة التزوير الالكتروني.

سادسا: صعوبات البحث:

مما لا شك فيه أن كل عمل أو بحث تعتريه بعض الصعوبات والعراقيل، ولعل أهم هذه الصعوبات التي واجهتنا في إعداد هذا البحث هي:

1-قلة المراجع المتخصصة في الجانب الإجرائي لجريمة التزوير الالكتروني بحد ذاتها مع الاعتراف بتوفر المراجع بشكل كبير فيما يتعلق بالجريمة الالكترونية غير أنه لا تتوفر المراجع الكافية المتعلقة بجريمة التزوير الالكتروني بصفة شاملة.

2-إن موضوع الدراسة يجمع بين جانبين على نفس القدر من الأهمية وهما القانون والمعلوماتية، حيث لا يمكن دراسة هذا الموضوع من الناحية القانونية دون التقنية ما خلف لنا صعوبات في البحث نظرا لعدم التخصص في المعلوماتية، وعدم الإلمام بالمصطلحات التقنية ذات الصلة بالموضوع.

سابعا: منهج البحث:

للإحاطة بكل جوانب الموضوع ومحاولة للإجابة عن الإشكالية المطروحة في هذه الدراسة اعتمدنا على المناهج التالية:

المنهج الوصفي: وهذا ما تقتضيه دراسة المفاهيم العامة، من خلال توضيح تعريفات قانونية وفقهية للتزوير الالكتروني وبيان خصائصها وأركانها، وأهم صور الجرم، وكذا وصف أهم الإجراءات وآليات مكافحة هذا النوع من الإجرام.

المنهج التحليلي: وهذا بقصد تحليل آليات وإجراءات و الحلول التي وضعت لمكافحة جريمة التزوير الالكتروني وتحليلها بشكل من التفصيل ثم بيان الاستنتاجات بشأنها، ومن ثمة تقديم الحلول المناسبة على ضوء ما توصل إليه الفقه والتشريع والقضاء المقارن.

كما تم الاستئناس بالمنهج المقارن ، حيث تعرضنا إلى بيان موقف التشريعات المقارنة سواء اللاتينية أو الأنجلوساكسونية من جريمة التزوير الالكتروني، وكذا توضيح الإجراءات التي اعتمدها مختلف التشريعات والأنظمة في مواجهة هذه الجريمة. هذا كمحاولة منا لسد الثغرات في النصوص القانونية والوصل إلى اقتراح حلول مناسبة لها.

ثامنا: إشكالية الدراسة:

للوقوف عند جريمة التزوير الالكتروني وبيان جملة من الإجراءات والآليات بغية التصدي لهان وتسليط الضوء على هذه الآليات والتركيز على المستجدات في هذا المجال، ارتأينا طرح الإشكالية الرئيسية التالية:

ما مدى فعالية الآليات الموضوعية والإجرائية التي وضعتها التشريعات الجنائية في مواجهة جريمة التزوير الالكتروني؟ وهل تطبيق هذه الإجراءات كافيا وفعالا لاحتواء متغيرات هذا النمط المستحدث من الإجرام؟

وفي سبيل الإجابة عن هذه الإشكالية تثور مجموعة من التساؤلات الفرعية:

1-ما المقصود بالتزوير الالكتروني كإحدى الجرائم الالكترونية، وما هي وسائل وطرق ارتكاب هذه الجريمة؟

2-ما هي الآليات التي وضعها المشرع الجزائري للحد من هذه الجريمة؟

3-فيما تتمثل الجهود الإقليمية والدولية في إطار التعاون الدولي لمكافحة جريمة التزوير الالكتروني؟

تاسعا:-خطة البحث:

قصد الإجابة على إشكالية البحث وتساؤلاته الفرعية، ارتأينا تقسيم الإجابة عليها وفق بابين:

الباب الأول: الآليات الموضوعية لمكافحة جريمة التزوير الالكتروني، وقد قسمنا هذا الباب إلى فصلين، تطرقنا في الفصل الأول إلى الإطار المفاهيمي لجريمة التزوير الالكتروني، تناولنا في المبحث الأول منه مفهوم التزوير التقليدي، في حين خصصنا المبحث الثاني لمفهوم التزوير الالكتروني. أما الفصل الثاني من هذا الباب فتناولنا فيه القواعد الموضوعية لمكافحة جريمة التزوير الالكتروني، وثم هو بدوره تقسيمه إلى مبحثين، الأول جاءت تحت عنوان القواعد الموضوعية لمكافحة جريمة التزوير الالكتروني على مستوى التجريم. أما المبحث الثاني فخصص لبيان القواعد الموضوعية لمكافحة جريمة التزوير الالكتروني على مستوى العقاب.

الباب الثاني: الآليات الإجرائية لمكافحة جريمة التزوير الالكتروني وتم تقسيم هذا الباب إلى فصلين، تطرقنا في الفصل الأول منها إلى الآليات الإجرائية لمكافحة جريمة التزوير الالكتروني على المستوى الداخلي، وثم تقسيم هذا الفصل إلى مبحثين، الأول تناولنا فيه قواعد الاختصاص القضائي في جريمة التزوير الالكتروني، أما المبحث الثاني فدرسنا فيه القواعد الإجرائية لجمع الأدلة في جريمة التزوير الالكتروني.أما الفصل الثاني من هذا الباب فتعرضنا فيه للجهود الدولية لمكافحة جريمة التزوير الالكتروني، وتم تقسيمه إلى مبحثين، المبحث الأول تطرقنا فيه إلى الجهود الدولية لمكافحة جريمة التزوير الالكتروني في إطار الأجهزة الدولية، في حين خصصنا المبحث الثاني لدراسة التحديات التي تواجه التعاون الدولي في مجال مكافحة جريمة التزوير الالكتروني.

وانتهى البحث بخاتمة تم فيها عرض أهم النتائج والتوصيات الخاصة بالموضوع.

الـبـاب الأول

الآليات الموضوعية لمكافحة جريمة التزوير الالكتروني

الباب الأول: الآليات الموضوعية لمكافحة جريمة التزوير الالكتروني

إن التطور الحاصل في تكنولوجيا الحاسب الآلي وظهور شبكة الانترنت بقدر ما سهلت سبل الحياة واختصرت الوقت والجهد وما قدمته للدول والأفراد من تسهيلات وخدمات وإيجابيات بقدر ما كان لها جانب سلبي أثر على حياة الناس ومصالح الدول نتيجة إساءة استخدام هذه التكنولوجيا وتطويع الانترنت وغيره من الوسائل الإلكترونية لارتكاب نوع جديد من الجرائم وهي الجرائم الإلكترونية والتي تتم عبر معدات وأجهزة إلكترونية أو باستخدام شبكة الانترنت[1] لارتكابها .

وتعتبر الجرائم الإلكترونية أو جرائم الحاسب أو جرائم التقنية العالية، ظاهرة إجرامية مستجدة نسبيا[2]، إذ تعد نوعا من الإجرام المعاصر الذي يثير الكثير من المشكلات من نواحي عديدة أهمها

[1]– تعود أصول كلمة انترنت إلى الكلمة الانجليزية internet وهي منقسمة إلى قسمين الأول inter وتعني البينية وكلمة net وتعني شبكة وعلي فتكون الترجمة الحرفية هي الشبكة البينية / للمزيد انظر : محمد إبراهيم سعد النادي، جرائم الانترنت بين الشريعة الإسلامية والقوانين الوضعية –دراسة مقارنة– الطبعة الأولى، مكتبة الوفاء، مصر، 2017، ص 17بعدها .

[2]– لقد اختلفت تسميات الجريمة الإلكترونية وشكل ما يسمى "بأزمة المصطلح "، من تلك التسميات نعتتها بأنها جرائم إساءة استخدام الكمبيوتر، أو جرائم الاحتيال الكمبيوتر أو الجريمة المعلوماتية أو حتى وإن تعددت المصطلحات فإن مصطلح الجريمة الالكترونية هو الأدق[2]، لأن البرامج والمعلومات أثناء تواجدها في النظام أو أثناء معالجتها أو انتقالها ما هي إلا عبارة عن نبضات الكترونية ولابد من التعامل معها بلغة الآلة .

جرائم التقنية العالية أو جرائم الهاكرز. ولقد تعددت المصطلحات التي أطلقت على الجرائم الناتجة عن الاستخدام غير المشروع لهذه التقنية، فلم يتفق الفقه على مصطلح واحد، فالبعض يطلق عليها الجرائم الالكترونية والجريمة المعلوماتية infraction informatique والغش المعلوماتي la fraude informatique أو جرائم الكمبيوتر L'infraction de l'ordinateur أو computer crimes أو par l'ordinateur crime favorisée، جرائم الانترنت criminalité par internet أو جرائم التكنولوجيا crimes technologique أو الجريمة الافتراضية cyber criminalité أو الانحراف الافتراضي cyber délinquance وهي مجموعة من الجرائم المرتبطة بالأنظمة الالكترونية والشبكة المعلوماتية وخصوصا شبكة الانترنت .

إلا أنه وفي اعتقادنا أنه ومهما كانت التسمية فإن هذه الجرائم ذات طابع مزدوج طابع تقني من حيث وسائل الاتصال والسلوك في حد ذاته وصوره ونتائجه انطلاقا من شبكة الاتصالات والحواسب الآلية وصولا لتبادل المعلومات والبيانات، وطابع قانوني كون هذه السلوكات هي جرائم وبالتالي الانصراف إلى نظرية الجريمة من حيث النص التجريمي والعقاب ما يدفع إلى البحث في

البعد القانوني لتلك السلوكيات ومحاولة ضبطها بقواعد تجريمية لردع مرتكبيها.

صعوبة اكتشاف هذه الجرائم وصعوبة إثباتها، إضافة للسرعة التي ترتكب بها الجريمة وهو ما يسهل ارتكابها، ويسهل كذلك طمس معالمها قبل اكتشافها نظرا لما يتمتع به المجرم المعلوماتي من ذكاء ومهارة تقنية عالية ومعارف فنية في مجال المعلوماتية.

وتعد جريمة التزوير الإلكتروني إحدى أهم الجرائم الإلكترونية التي تلحق ضررا سواء على الصعيد الخاص كونها تمس الفرد، وقد يكون هذا الضرر اقتصاديا أو اجتماعيا أو سياسيا أو تجاريا، إضافة إلى الأضرار العامة التي تتمثل في تضليل العدالة وفقدان الثقة العامة للمجتمع ما يؤدي إلى خلق حالة من الفوضى وعدم الاستقرار في المعاملات .

وللإحاطة بهذه الجريمة ارتأينا تقسيم هذا الباب إلى فصلين نستهل الأول برفع الغموض عن جريمة التزوير الإلكتروني ببيان المفاهيم العامة لهذه الجريمة، في حين نخصص الفصل الثاني لدراسة القواعد الموضوعية للجريمة على مستوى التجريم والعقاب، وذلك بتحديد أركان الجريمة وأنواع هذه الجريمة، ناهيك عن وضع الجزاء الجنائي الذي يتناسب مع درجة خطورة التزوير ودرجة خطورة المزور الإلكتروني أيضا .

وقد اتسع مفهوم ونطاق الجرائم المعلوماتية أو الالكترونية وظهرت تعريفات عديدة لهذه الجرائم تختلف حسب ضيقها واتساعها، كما أن فقهاء القانون الجنائي لم يتفقوا على الوصف القانوني السليم أو التسمية الدقيقة لهذا المصطلح وهذا ما يثبت أن الظاهرة معقدة ولا يمكن حصرها، خاصة أمام غياب التعريف القانوني الدقيق لهذا المصطلح وترك الأمر إلى الفقهاء لإعطاء مفاهيم وتصورات مختلفة ما جعل الأمر أكثر تعقيدا، ويعتبر هذا الاختلاف مصدر التداخل أو الخلط لهذه المصطلحات سواء على مستوى مجال انعكاسه، أو المصطلح المختار شكل عائقا أمام رجال القانون لبحث وفهم الجريمة . voir : Gassin, R, le droit pénal de l'informatique, les systémes de traitements automatique des données, commentaire de la loi 88/18 du 18/01/1988 relative à la fraude informatique, J.C.P, dalloz, France , P5

الفصـــل الأول

المفاهيم العامة لجريمة التزوير الإلكتروني

الفصل الأول: المفاهيم العامة لجريمة التزوير الإلكتروني

تعد جريمة التزوير الإلكتروني ظاهرة إجرامية مستحدثة، وذلك لارتباطها بتكنولوجيا المعلومات والاتصالات والكمبيوتر. وقد نشأت وتطورت هذه الجريمة مع نشوء وتطور الكتابة ونظام التوثيق. وساهمت في تطورها ثورة المعلومات والتكنولوجيا الرقمية من خلال تغيير طبيعة الوثائق الرسمية الإدارية حيث بدأ التحول نحو النموذج الإلكتروني لإنجاز مختلف المعاملات على مستوى الإدارات العامة، حتى أصبحت إدارات رقمية، وهو ما دفع بمختلف التشريعات إلى تجريم كل ما من شأنه المساس بهذه الوثائق ووضع عقوبات رادعة لكل من تسبب بالمساس بمحتواها وحمايتها جنائيا.

وللوقوف عند البناء القانوني لجريمة التزوير الالكتروني يقتضي التطرق إلى مفهوم التزوير سواء كان بمدلوله التقليدي أو الالكتروني، حيث نتطرق في المبحث الأول إلى بيان مفهوم التزوير التقليدي. لنعرج في المبحث الثاني إلى مفهوم جريمة التزوير الالكتروني.

المبحث الأول: مفهوم التزوير التقليدي

عرفت جريمة التزوير ونشأت مع نشوء الكتابة وشيوع استعمالها في مختلف جوانب الحياة، ومما لاشك أن الكتابة كانت حجر الأساس في تطوير الحياة البشرية، فهي الوعاء الذي ينقل به الناس معالم حضارتهم وعلومهم، ومن هنا جاءت أهمية الوثائق والمستندات والمدونات والمحررات المختلفة بوصفها أدوات لتوثيق المعلومات والمعاملات والعقود وغيرها، فكان لابد أن تتعرض لضروب شتى من التحريف والتزوير لتغيير حقيقتها وتحريف بياناتها ومعلوماتها .

لذا كان من الأهمية بمكان أن نقف عند تحديد مفهوم جريمة التزوير التقليدي وذلك ببيان عناصرها وخصائصها مع إبراز أوجه التفرقة بينها وبين بعض الجرائم القريبة منها وهذا في المطالب الآتية:

المطلب الأول: تعريف التزوير التقليدي

امتد مفهوم التزوير ليشمل كافة أنواع الغش ما يثير إشكالا يتعلق بتحديد المقصود منه، ففي المجال الجنائي نجد التشريعات العقابية تحدد فقط وسائله وطرقه. فالتشريع المصري يقصره على المحررات وتقليد الأختام والأوراق الرسمية، أما الألماني فيقصره على المحررات وكذلك المشرع

الفرنسي، إلا أنه تطورت التشريعات في البلدين الأخيرين لمواكبة التطور التكنولوجي في المعالجة الآلية للبيانات وأضفت الحماية على أي أوعية أخرى تشملها البيانات المعالجة آليا غير المحررات، في حين توسع المشرع السوري إلى حد ما في نصوص التزوير وأضاف الصك أو المخطوط والأختام والتوقيع والسجلات والبيانات الرسمية.[1]

أما المشرع الجزائري من خلال قانون العقوبات فلم يورد تعريف للتزوير، حيث اكتفى ببيان الطرق التي ترتكب بها جريمة التزوير والعقوبات المقررة لها، هذا ما يدفعنا إلى البحث في التعريف اللغوي للتزوير مع بيان التعاريف الواردة في بعض التشريعات العقابية المقارنة، وهذا على النحو الآتي:

الفرع الأول: التعريف اللغوي للتزوير

التزوير لغة لفظ مشتق من الزور، وهو الكذب والباطل، وقيل شهادة الباطل ورجل زور، وقود زور، وكلام مزور مموه بالكذب، وقيل محسن، والتزوير تزيين الكذب وقيل إصلاح الشيء قبل كل إصلاح للشيء من خير أو شر فهو تزوير، والتزوير فعل الكذب والباطل.[2]

والتزوير هو محاولة تزيين الكذب وطمس الحقيقة وإلباس الباطل بثوب الحق فجوهر التزوير هو الكذب الذي يهدف إلى إنشاء حقيقة قائمة.[3]

ويعني أيضا إصلاح الكلام وتهيئته، وهي مشتقة من الزور وتعني الكذب والباطل فيقال كلام مزور مموه بالكذب .[4]

---

[1]– فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية –دراسة مقارنة – دون طبعة، منشورات الحلبي الحقوقية، لبنان، 2003، ص 232.

[2]– جمال الدين أبو الفضل محمد بن مكرم بن منظور الأنصاري الإفريقي المصري، لسان العرب، المجلد الرابع، دار الكتب العلمية، لبنان، 2002، ص 389.

[3]– إسماعيل بن حماد الجوهري، تاج اللغة وإصحاح اللغة العربية، الطبعة الرابعة، دار العلم للملايين، بيروت، لبنان، 1987، ص 674.

[4]– فتوح الشاذلي، عفيفي كامل عفيفي، مرجع سابق، ص 232.

ويقصد بالتزوير تغيير الحقيقة أو إحلال أمر غير صحيح محل الصحيح الواقع عن الأمور، فلا تزوير إذا لم يحدث ذلك، والتزوير في المحررات هو كذب مكتوب، وليس كذب بالقول لأن ذلك يعني شهادة الزور.[1]

الفرع الثاني: التعريف الفقهي للتزوير

التزوير فقها هو كل وسيلة يستعملها شخص ليغش بها آخر .[2]وجوهر التزوير هو الكذب المكتوب والكذب _بصفة عامة _ وهو سلوك شائن لا يحفل به النظام القانوني أحيانا ولو ترتب عليه ضرر للغير متى كان بوسع المكذوب عليه أن يفحصه ويتبين عدم صدقه.[3]

وقد عرف الأستاذ جون بول دوسي التزوير بأنه كل تغيير أو تزييف أو نفي للحقيقة أو الواقع أو الأصل، يكون الهدف منه خداع الآخرين، ويتميز بتزييف الحقيقة ومن شأنه إلحاق الضرر، ويرتكب عمدا في محرر من شأنه أن يستعمل في الإثبات .[4]ويعتبر التزوير إظهار للكذب في محرر كمظهر الحقيقة وذلك غشا لعقيدة الغير .[5]

كما يعرف بأنه تغيير الحقيقة في المحرر بإحدى الطرق التي نص عليها القانون على نحو يوقع ضررا بالغير وبنية استعمال هذا المحرر فيا أعد له.[6]

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

---

[1]– الهام بن خليفة، الحماية الجنائية للمحررات الالكترونية من التزوير، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر، 2016،ص 53.

[2]– فتوح الشاذلي، عفيفي كامل عفيفي، المرجع السابق، ص 232.

[3]– نبيل صقر، الوسيط في الجرائم المخلة بالثقة العامة، دون طبعة، دار الهدى، الجزائر، 2015، ص 190.

[4]– جمال نجيمي، جرائم التزوير في قانون العقوبات الجزائري، دون طبعة، دار هومة، الجزائر، 2013، ص 270.

[5]– رمسيس بنهام، الجرائم المضرة بالمصلحة الجامعة دون طبعة، منشأة المعارف الإسكندرية، مصر، 1986، ص162.

[6]– عبد الفتاح بيومي حجازي، الحكومة الالكترونية، الكتاب الثاني، الطبعة الأولى، دار الفكر الجامعي الإسكندرية، مصر، 2008، ص 177 .

وعليه فجوهر التزوير هو الكذب المكتوب، والتزوير يفقد الثقة العامة في المحررات ويخل تبعا لذلك بالضمان واليقين والاستقرار في المعاملات وسائر مظاهر الحياة القانونية في المجتمع، فالناس يعتمدون على الأوراق المكتوبة لإثبات علاقاتهم والدولة تعتمد عليها في ممارسة اختصاصاتها المتنوعة، ولا يتاح للمحررات المكتوبة أداء هذا الدور إلا إذا منحها الناس ثقتهم، فآمنوا بصدق البيانات التي تثبتها، أما إذا كان تعارضها والحقيقة هو الوضع الغالب، فإن ذلك يؤدي إلى رفض الناس الاعتماد عليها، مما يؤدي غلى تعثر التعامل بين الأفراد واضطراب نشاط الدولة .[2]

وقد تأثر الفقه الجزائري والمصري بالفقه الفرنسي فيما يخص تعريف التزوير، ولاسيما بجيل الوسط من فقهاء القانون الجنائي وعلى رأسهم الفقيه EMILE Garçon، إذ عرف هذا الأخير التزوير بأنه :" تغيير الحقيقة بقصد الغش في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شانه أن يسبب ضررا ".[3]

الفرع الثالث: تعريف التزوير في إطار نصوص قانون العقوبات

لقد اعتمدت بعض الدول نهجا معينا في تعريف التزوير بصفة عامة، حيث تم توسيع نصوص قانون العقوبات في مجال التزوير، ومن هذه الدول نجد فرنسا، وذلك من خلال تعديل نصوص قانون العقوبات المتعلقة بالتزوير.

فبالرجوع إلى القسم الأول ضمن الكتاب الرابع من قانون العقوبات الفرنسي تحت عنوان الاعتداءات ضد الثقة العامة نجد أن المادة 441 فقرة 01 المعدلة في 14 ماي 1993 تنص على أن التزوير يقوم على كل تغيير في الحقيقة بغش من شانه أن يسبب ضررا، والذي يرتكب بأي طريقة كانت في محرر مكتوب أو كل دعامة أخرى للتعبير عن الفكر يكون الغرض منه إثبات حق أو واقعة لها آثار قانونية .[4]

---

[1]– عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم التزوير والانترنت، دون طبعة، دار الكتب القانونية، مصر، 2008، ص 137 .

[2]– محمود نجيب حسني، جرائم الاعتداء على الأموال، دون طبعة، دار النهضة العربية، مصر، 1992، ص 252.

[3]– نبيل صقر، مرجع سابق، ص 191.

ويستنتج من النص السابق أن المشرع الفرنسي أعطى مفهوما واسعا للتزوير واعتبره كل تغيير للحقيقة عن طريق الغش وأي طريقة كانت دون تحديد لطرق ووسائل التزوير ،وأن يكون على وعاء مكتوب سواء ورقيا أو الكترونيا بشرط أن يكون هذا الوعاء يثبت حقا أو مركزا قانونيا، أو يمكن استخدامه كدليل لإثبات واقعة قانونية .

أما المشرع المصري فقد عالج التزوير في المحررات في المواد من 211 إلى 227 من قانون العقوبات ولم ينص على تعريف محدد للتزوير وأركانه واقتصر على طرقه.

في حين عرف قانون العقوبات اللبناني التزوير في المادة 453 من قانون العقوبات بأنه:" تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج به يمكن أن ينتج عنه ضررا أدبيا أو ماديا أو اجتماعيا ".

أما المشرع الجزائي الأردني فقد عالج جريمة التزوير في قانون العقوبات في الفصل الثاني من الباب الخامس تحت عنوان (الجرائم المخلة بالثقة العامة) حيث عرفت المادة 260 التزوير على أنه: (تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج بهما نجم أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي)، وبهذا يكون قد خالف بعض التشريعات التي لم تعرف التزوير وإنما اكتفت ببيان الطرق التي يقع بها، كما سبق الإشارة وكما هو الحال في القانون الفرنسي والمصري .

أما المشرع الجزائري فقد تناول قانون العقوبات في القسم الثالث إلى السادس من الفصل السابع التزوير في المحررات في المواد من 214 إلى 222. وقد نصت المادة 214 على أنه :(يعاقب بالسجن المؤبد كل قاض أو موظف أو قائم بوظيفة عمومية ارتكب تزويرا في المحررات العمومية أو الرسمية أثناء تأدية وظيفته :

1_ إما بوضع توقيعات مزورة،

---

[4]– Article 441 « Constitue un faux toute altération frauduleuse de la vérité de nature à causer un préjudice et accomplie par quelque moyen que ce soit dans un écrit ou tout autre support d'expression de la pensée qui à pour objet ou qui peut avoir pour effet d'établir la preuve d'un fait ayant des conséquences juridiques ».

2_ وإما بإحداث تغيير في المحررات أو الخطوط أو التوقيعات،

3_ وإما بانتحال شخصية الغير أو الحلول محلها،

4_ وإما بالكتابة في السجلات أو غيرها من المحررات العمومية أو بالتغيير فيها بعد إتمامها أو قفلها".

وعليه فمن خلال تحليل نص المادة بشكل مبسط ومختصر نستنتج أن تطبيق المادة 214 يتطلب ضرورة توفر عدد من العناصر التي لا يمكن أن تتصور قيام ولا نشوء جريمة التزوير في المحررات العمومية أو الرسمية ،والمتمثلة في العنصر المادي والمتمثل في الوقائع التي من شأنها تزييف الحقيقة، إضافة إلى عنصر الوظيفة أو الصفة والذي يعني أن يكون المتهم يمارس مهنة القاضي أو موظف عام، أو يقوم بخدمة عامة في إطار قوانين الدولة وبرخصة منها كالموثقين والمحضرين القضائيين .[1]

وعليه بتسليط الضوء على المواد 214 إلى 229 من قانون العقوبات نجد أن المشرع الجزائري لم يعط تعريفا للتزوير على غرار بقية التشريعات كالفرنسي والمصري، والملاحظ أيضا أنه لم يجعل التزوير جريمة واحدة، بل أورده على أنواع متفاوتة العقوبة والمتمثلة في التزوير في المحررات الرسمية أو العمومية الواردة في المواد من 214 إلى 217 والتزوير في المحررات التجارية أو المصرفية أو العرفية وهذا في المادتين 219 و220، إضافة إلى التزوير في بعض الوثائق الإدارية والشهادات وهذا في المواد من 222 إلى 229 .

وانطلاقا مما تم بسطه نجد أن جوهر التزوير هو الكذب المكتوب والكذب بصفة عامة، فالتزوير يفقد الثقة العامة في المحررات ويخل تبعا لذلك بالضمان واليقين والاستقرار في المعاملات وسائر مظاهر الحياة القانونية في المجتمع فالناس يعتمدون على الأوراق المكتوبة لإثبات علاقاتهم، والدولة تعتمد عليها في ممارسة اختصاصاتها المتنوعة ولا يتاح للمحررات المكتوبة أداء هذا الدور إلا إذا منحها الناس ثقتهم، فآمنوا بصدق البيانات التي تثبتها، أما إذا كان تعارضها والحقيقة هو الوضع

[1]– للمزيد انظر: عبد العزيز سعد، جرائم التزوير وخيانة الأمانة واستعمال المزور، الطبعة السادسة، دار هومة، الجزائر، 2013، ص 19 وما يليها .

الغالب، فإن ذلك يؤدي إلى رفض الناس الاعتماد عليها مما يؤدي إلى تعثر التعامل بين الأفراد واضطراب نشاط الدولة .[1]

وبناء على ما سبق نستنتج أن التزوير هو كل تغيير عمدي للحقيقة – أو كذب أو غش متعمد– من شأنه أن يسبب ضررا بالطرق المحددة قانونا في محرر يثبت واقعة لها آثار قانونية يقصد الغش أو بنية استعمال المزور من أجله.

ومن هذا المنطلق تتحدد الأركان التي تبنى عليها جريمة التزوير والمتمثلة في الركن المادي وهذا بتغيير الحقيقة ما بسبب ضررا للغير بإحدى الطرق المنصوص عليها قانونا، إضافة إلى الركن المعنوي الذي يتطلب ضرورة توافر القصد الجنائي العام والخاص في السوق، حيث يبقى هذا الخطر ساريا مع التزوير .[2]

المطلب الثاني: التفرقة بين التزوير وجرائم أخرى مشابهة

سبقت الإشارة إلى أن التزوير هو تغيير حقيقة المحرر بإحدى الطرق المنصوص عليها قانونا تغييرا من شأنه إحداث ضرر، وبنية استعماله كمحرر صحيح .

وتقترب جريمة التزوير مع جرائم أخرى مشابهة كالتقليد واستعمال المحرر المزور إضافة إلى جريمة النصب، إلا أنه ثمة هناك فروقات نوردها فيما يلي :

الفرع الأول: الفرق بين التزوير والتقليد:

التقليد[3]هو إنشاء شيء مشابه للشيء الذي يشمله القانون بحمايته، ويتحقق بصناعة شيء أو اصطناع خاتم يماثل الشيء أو الخاتم الذي يشمله القانون بحمايته. وعلى ذلك فالتقليد يعني خلق شيء أو خاتم لم يكن له وجود من قبل .[1]

[1]– محمود نجيب حسني، المرجع السابق، ص 255.

[2]– Louis Gorron, L'incrimmation du faux et du mensonge en droit pénal, 2011, P12.

[3]– إن عبارة التقليد contrefait تعني إنشاء محرر أو وثيقة إدارية أو شهادة غير صحيحة وغير حقيقية تشبه أو تماثل تماما وثيقة إدارية أو شهادة في شكلها ومضمونها بحيث ينخدع بها الشخص العادي و يعتقد أنها وثيقة صحيحة لا

ويقصد بالتقليد المحاكاة والتشبه، وهو صناعة شيء على نمط شيء آخر بصورة تؤدي إلى انخداع الجمهور وتضليلهم هذا من خلال إجراء بعض التعديلات على هذا الشيء بالزيادة والنقصان.[2]

والتقليد قد يكون حرا، أي يتمرن الكاتب أو الشخص المقلد كثيرا على الموضوع الذي يريد تقليده إلى أن يصل إلى مرحلة التيقن من تقليده ثم يقوم بعملية التقليد، وقد يكون مقيدا بالموضوع ويضعه أمامه ويقوم بتقليده خطوة بخطوة، ويتم التقليد غالبا في تزوير التوقيعات أو بصمات الأختام .[3]

ويقصد بالتقليد تحرير كتابة في محرر تشبه كتابة تشخص آخر بهدف الإبهام بأنها صادرة منه ولا يشترط هنا الاتفاق بل يكفي أن يعتقد الشخص المقلد بأن ما حرره يشبه ما قلده.[4]

فالتقليد يقوم على محاكة تتم بها المشابهة بين الأصل والتقليد، والعبرة فيه بأوجه الشبه لا بأوجه الاختلاف، بحيث يكون من شأنه أن ينخدع به الجمهور في المعاملات، وفي هذا المعنى قررت محكمة النقض المصرية : " أنه لا يلزم في التزوير المعاقب عليه أن يكون متقنا بحيث يلزم لكشفه دراية خاصة، بل يستوي أن يكون واضحا لا يستلزم جهدا في كشفه أو متقنا يتعذر على الغير أن يكشفه ما دام أن تغيير الحقيقة في الحالتين يجوز أن ينخدع به بعض الناس ".[5]

لبس فيها .أما عبارة التزييفAltère فهي عبارة تصدق على كل عمل من شأنه أن يؤدي إلى وضع بيانات ووقائع كاذبة مكان وقائع صحيحة وصادقة .

[1]– نبيل صقر، المرجع السابق، ص 175.

[2]– عامر محمود الكسواني، التزوير المعلوماتي للعلامة التجارية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص 203.

[3]– محمد أحمد وقيع الله، أساليب التزييف والتزوير وطرق كشفها، الطبعة الأولى، دار الأكاديميون للنشر والتوزيع، الأردن، 2014، ص 23.

[4]– شريف الطباخ، التزوير والتزييف في ضوء الفقه والقضاء، الطبعة الثانية، المركز القومي للإصدارات القانونية، مصر، 2006، ص 39.

[5]– وفي هذا المعنى قررت محكمة النقض المصرية : " أنه لا يلزم في التزوير المعاقب عليه ان متقنا بحيث يلزم لكشفه دراية خاصة، بل يستوي أن يكون واضحا لا يستلزم جهدا في كشفه او متقنا يتعذر على الغير أن يكشفه ما دام أن تغيير الحقيقة في الحالتين يجوز أن ينخدع به بعض الناس "، نقض مصري 9 مارس 1982، مجموعة أحكام النقض مصري، السنة 33 رقم 64، 31000/ عن نبيل صقر، المرجع السابق، ص 176.

و بناء على ذلك فالتقليد يعني خلق شيء أو خاتم لم يكن له وجود من قبل، وهو بهذا يختلف عن التزوير الذي يعني إدخال تغيير على شيء موجود وصحيح في الأصل، تغييرا يحقق مصلحة لمزور ما كانت لتتحقق لو ظل على أصله صحيحا .

وقد استعمل المشرع الجزائري تعبير التقليد، لأن بعض الأشياء التي شملتها الحماية القانونية تأبى طبيعتها التزوير فلا تتحقق إلا بالتقليد، مثال ذلك الأختام التي لا يتصور عملا تزويرها حيث لا فائدة من التزوير، فالمقلد إذا كان يقصد استعمال الختم فلابد من تقليده بإنشائه مطابقا للختم الأصلي، ويعني ذلك أنه لا يشترط اجتماع فعل التقليد مع فعل التزوير لقيام الجريمة، فيكفي لتحققها ارتكاب الجاني لأحد الفعلين وتعد جريمة تقليد الأشياء المنصوص عليها في المادتين 205 و 206 جريمة عمدية، يتخذ ركنها المعنوي صورة القصد الجنائي.

ولا يكفي في هذه الجريمة القصد العام بل يلزم توافر قصد خاص لقيامها، فالقصد العام يتحقق بعلم المقلد أو المزور بماهية الفعل الذي يأتيه، بأن من شأنه التقليد أو التزوير لشيء أو محرر مما ورد ذكره في النصوص المواد 205 و 206 من قانون العقوبات . وينبغي أن تتجه إرادة المقلد أو المزور إلى إتيان فعل التقليد أو التزوير على المحل الذي يحميه المشرع .[1] أما القصد الخاص يتمثل في نية استعمال الشيء المقلد أو المزور فيها زور من أجله. فالتزوير لا يقوم إلا إذا توافرت هذه النية لدى المتهم، ولا يشد عن هذه القاعدة تقليد أو تزوير الأشياء التي ورد ذكرها في المادة 204 من قانون العقوبات . ولا مجال للبحث في القصد الخاص إلا إذا ثبت توافر القصد العام، لكن توافر القصد العام لا يعني بالضرورة ثبوت القصد الخاص لدى المتهم وإن كان يفترض وجوده ومع ذلك فإن هذا الافتراض يقبل إثبات العكس، فيجوز المتهم بالتقليد أو التزوير كان لإجراء تجربة علمية أو لإظهار مهارته الفنية في هذه الأمور أو لمجرد إشباع هوايته في تقليد الأشياء الدقيقة، فإذا عجز عن

[1]–تنص المادة 205 من الأمر 156/66 المتضمن قانون العقوبات المعدل والمتهم على أنه :" يعاقب بالسجن المؤبد بكل من قلد خاتم الدولة أو استغل الخاتم المقلد .... "

وتنص المادة 206 من ذات الأمر على أنه :" يعاقب بالسجن المؤقت من خمس (05) سنوات إلى عشر (10) سنوات وبغرامة من 500,000 دج إلى 1,000,000 دج، كل من قلد أو زور، إما طابعا وطنيا أو أكثر وإما مطرقة أو أكثر مستخدمة في علامات الغابات، وإما دمغة أو أكثر مستخدمة في دمغ المواد الذهبية أو الفضية، أو استعمل طوابع أو أوراق أو مطارق أو دمغات مزورة أو مقلدة ".

إقامة الدليل عن تخلف نية الاستعمال، توافرت في حقه جريمة التقليد أو التزوير، لأن ثبوت العلم والإرادة يرجح توافر نية استعمال الشيء المقلد أو المزور في عرض محدد .[1]

وغالبا ما يقترن الاصطناع بالتزوير وذلك بوضع إمضاء مزور للدلالة على صدور المحرر المصطنع ممن نسب إليه هذا الإمضاء، ومع ذلك فقد يتصور الاصطناع في محرر بغير أن يشتمل على إمضاء لشخص ما، وتصور ذلك سهل في المحررات الرسمية، وللاصطناع صورتان أن يخلق الجاني محررا لم يكن موجودا من قبل، أو أن يخلق محررا ليحل محررا أخر بعد التعديل .[2]

وكثيرا ما يقترن التقليد بإحدى طرق التزوير، ذلك أن المحرر المقلد إذا وقع عليه بإمضاء أو ختم مقلد كان لدينا، فضلا عن التقليد، تزوير بطريقة وضع إمضاءات أو أختام مزورة، وإذا كان التقليد بإضافة عبارات أو كلمات إلى محرر مع توخي تقليد خط باقي المحرر كان لدينا فضلا عن التقليد، تزوير بتغيير المحررات أو زيادة كلمات، ومع ذلك فمن المتصور أن يقع التزوير بطريقة التقليد وحده، كمن يقلد خط التغيير في ورقة ممضاة منه على بياض أو يقلد خط الغير في ورقة، أو يقلد خط تاجر ويثبت في دفاتره أمورا تعتبر حجة عليه، ومن هذا القبيل أيضا تقليد تذاكر السكة الحديدية أو ما شابه ذلك، فإن التقليد في هذه الصور لا يحتاج إلى تقليد إمضاء وهو في ذلك تزوير معاقب عليه .[3]

ومن خلال ما سبق تبين لنا أن التقليد يقصد به المحاكاة، وهي في مفهوم التزوير إنشاء محرر على مثال محرر آخر أو أن يحرر المتهم كتابا بخط يشبهه خط شخص آخر، سعيا لأن ينسب إله هذا المحرر، ولا يشترط في التقليد أن يبلغ حدا من الإتقان، بل تكفي المحاكاة على نحو ينخدع بها بعض الناس إلى حد وهمه بصحة المحرر، وغالبا ما يكون التقليد معه وسيلة أخرى من طرق التزوير كما لو أنهى المقلد المحرر بإمضاء أو ختم أو أضاف عبارة يمكن أن يخلق محررا جديدا بهذا التقليد فيسمى اصطناع وهي إحدى طرق التزوير،فالاصطناع هو خلق محرر بأكمله ونسبته إلى غير

[1]– نبيل صقر، المرجع السابق، ص 177.

[2]– شريف الطباخ، المرجع السابق، ص 40 .

[3]–نفس المرجع والصفحة.

محرر، وهناك فارق بين التقليد والاصطناع، ففي الاصطناع لا يهم الجاني مدى التشابه بين خطه وخط الغير عكس التقليد، وذلك لأنه يصنع محررا جديدا بكامله بينما التقليد يعالج جزءا من المحرر.[1]

الفرع الثاني: الفرق بين التزوير والاستعمال المزور:

إن جريمة استعمال المحرر أو المستند المزور هي استعمال الورقة المزورة والاحتجاج بها لدى فرد أو جهة من الجهات، وتكون هذه الجريمة بمجرد الاحتجاج بالمحرر المزور فعلا ولو عدل بعد ذلك عن التمسك به، ولا يلزم أن يكون الفاعل هو الذي قدم المحرر المزور، بل تتوافر الجريمة في حقه ولو احتج بمستند قدمه غيره .على أنه لا وجود لجريمة الاستعمال حيث لا تزوير، كما انه لا عبرة بمن يجري الاحتجاج بالمستند في مواجهته، سواء كان فردا أو جهة قضائية.[2]

فجوهر السلوك الإجرامي في هذه الجريمة هو فعل الاستعمال، وذلك بأن يحتج الجاني على غيره بالمحرر المزور، وفي ذلك لا يكفي إبراز المحرر العرفي المزور على أنه حقيقي بل يقدم إلى المجني عليه لأجل الاستفادة من هذا السلوك.[3]

وعليه يعد استعمال المستند المزور هو الركن المادي لجريمة استعمال المستند المزور بل وأنه القاعدة الأساسية التي تقوم عليها الجريمة.

وبالرجوع إلى المشرع الجزائري نجده قد نص على تزوير المحررات بمعزل عن جريمة استعمالها، فجعل كل منهما مستقلة عن الأخرى وجريمة قائمة بذاتها، بحيث نص على استعمال الأوراق العمومية أو الرسمية في المادة 218 من قانون العقوبات، وعلى استعمال الأوراق العرفية أو التجارية أو المصرفية في المادة 221، وعلى استعمال الوثائق الإدارية والشهادات في المواد 222 الفقرة 1 و 223 و 227 فقرة 2 و 228 فقرة 3 .

---

[1]– للمزيد انظر : عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والانترنت، دون طبعة، دار الكتب القانونية، مصر، 2008، ص 225، وما بعدها .

[2]– أحمد محمود خليل، جرائم تزوير المحررات دون طبعة، المكتب الجامعي الحديث، مصر، 2008، ص ص 121، 122 .

[3]– عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنت في التشريعات العربية، الطبعة الأولى، دار النهضة العربية، مصر، 2009، ص 92.

و لم يحدد المشرع الجزائري معنى الاستعمال المعاقب عليه، ولا حتى المشرع الفرنسي كذلك مما جعل الفقه والقضاء يجتهدان في تحديد ماهية فعل الاستعمال وقد ذهب الفقيه جارو garou إلى وجوب أن تكون هناك علاقة تتزامن بين فعل التزوير وفعل الاستعمال، فلابد أن يكون هنا الارتباط بين الفعلين "الاستعمال والتزوير [1].

أما الفقيه جارسو Garçou فقد اعتنق مفهوم موسع لفعل الاستعمال حيث يرى أن كل فعل يستعمل أو يستخدم فيه المستند المزور يعد مشكلا جريمة الاستعمال دون اشتراط أن يستخدم المحرر فيما زور من أجله .[2]

وترتبط جريمة استعمال المزور بجريمة التزوير ارتباطا عضويا كاملا، من حيث أنه لا يمكن تصور وجود الاستعمال دون إثبات قيام التزوير، بمعنى أنها مبنية ومؤسسة فعليا على إثبات وقائع علمية، ولأن الحكم بإدانة المتهم لارتكابه الاستعمال المزور دون الاستناد إلى إثبات وجود وثيقة مزورة بفعل المتهم نفسه، أو فعل غيره يجعل هذا الحكم، حكما غير مؤسس ويعين إلغاؤه .[3]

ويختلف مفهوم الاستعمال عن مفهوم التزوير ذاته، فبالرغم من وجود علاقة بين النصين المتعلقة بوجود التزوير، إلا أنه يبقى لمفهوم الاستعمال ذاتية تختلف عن مفهوم التزوير نابعة من وجود نصين قانونيين، أحدهما بالتزوير والآخر بالاستعمال، ويترتب على هذا المفهوم نتائج عديدة منها أن الفاعل في جريمة الاستخدام لا تطبق عليه عقوبة الاشتراك في جريمة التزوير .[4]

وقد أكدت المحكمة العليا في عدة مناسبات استقلالية جريمة استعمال المحرر المزور عن جريمة تزوير المحرر .[5]

---

[1]– خثير مسعود،الحماية الجنائية لبرامج الكمبيوتر،دون طبعة،دار الهدى،الجزائر،2010،ص139.

[2]– محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دون طبعة، دار المطبوعات الجامعية مصر، 2004، ص 140.

[3]– عبد العزيز سعد، المرجع السابق، ص 78 .

[4]– خثير مسعود، المرجع السابق، ص 141.

[5]– ج 9 –7–1981، ملف رقم 25134 مجموعة قرارات الغرفة الجنائية للمحكمة العليا ص 156، قرار 5–12–1989 ملق 703، 66، ج، بغدادي، الاجتهاد القضائي في المواد الجزائرية، ج2 / انظر في ذلك حسن بوسقيعة،

كما أكدت التشريعات العقابية بما يعتبر جريمة تزوير المحرر جريمة مستقلة عن جريمة استعماله وهو مزور، فليس الاستعمال ركنا في التزوير، وليس فعلا لاحقا، فلا يوقع من أجله عقاب وإنما هو جريمة مستقلة عن التزوير[1]، حيث أنه يعاقب مرتكب التزوير ولو لم يستعمل المحرر المزور، وأن من يستعمل المحرر المزور يعاقب على فعله ولو لم يرتكب التزوير أو يشترك فيه، ويعاقب حتى وإن كانت جريمة التزوير لا يمكن متابعتها لكون مرتكبها ظل مجهولا أو أن الدعوى أدركها التقادم، وإذ كان من ساهم في التزوير هو الذي استعمل المحرر المزور، فإنه يكون مسؤولا عن الجريمتين وتوقع عليه عقوبة واحدة هي العقوبة الأشد طبقا للمادة 32 من قانون العقوبات .[2]

ولما كانت جريمة استعمال المزور جريمة مستقلة ومنفصلة عن جريمة التزوير ذاتها وتختلف عنها من حيث عناصر تكوينها، ومن حيث العقوبات المقررة لها[3]، ومن حيث سقوطها بالتقادم، فجريمة استعمال المزور جريمة آنية تتم بمجرد الاحتجاج أو التمسك بالمحرر بصرف النظر عما يطرأ بعد ذلك، ولا يهم إن تحققت الغاية التي استخدم المحرر لأجلها، أما جريمة التزوير فهي وقتية غير متجددة الحدوث خلافا لجريمة الاستعمال كونها جريمة متجددة الحدوث، بمعنى أن الجريمة تتم وتنتهي ويتجدد حدوثها وانتهاؤها تبعا للأغراض المختلفة التي تستعمل فيها الورقة المزورة، فكلما استعمل المحرر مرة لغرض معين تحقق ركن الاستعمال، وكل مرة يستعمل فيها المحرر تعتبر جريمة.[4]

الوجيز في القانون الجزائي الخاص – الجرائم ضد الأشخاص والجرائم ضد الأموال، الجزء الأول، الطبعة السابعة، دار هومة، الجزائر، 2007، ص 317 وما بعدها .

[1]– على سبيل المثال : القرار الإعدادي رقم 14 تاريخ 1987/12/20 الصادر عن الغرفة الإدارية لمحكمة بيروت البدائية الذي قضى أنه :" استعمال التزوير هو جرم مستقل فلا يجوز إدغامه بجرم التزوير وجعلهما جرما واحدا " / عن نزيه نعيم شلالا، دعاوى التزوير واستعمال المزور، دون طبعة، منشورات الحلبي الحقوقية، لبنان 2002، ص 55.

[2]– محمود نصيب حسني، شرح قانون العقوبات القسم الخاص وفقا لأحدث التعديلات التشريعية، المرجع السابق، ص 348 .

[3]– احسن بوسقيعة، المرجع السابق، ص 436.

[4]– لا تختلف العقوبات المقررة للتزوير في المحررات العرقية أو التجارية أو المصرفية عن تلك المقررات لاستعمال المزور، فهي الحبس من سنة إلى 5 سنوات وغرامة من 500 إلى 2,000 دج أو من 500 إلى 2,000 دج في

أما فيما يتعلق بعناصر الجريمة فعناصر قيام جريمة التزوير تختلف تماما عن عناصر قيام جريمة استعمال المزور وذلك تبعا لاختلاف طبيعة كل منهما عن الأخرى، حيث أن جريمة التزوير المنصوص عليها في المادتين 214_215 من قانون العقوبات تجعل من صفة المزور عنصرا أساسيا، بينما المادة 216 تغفل هذا العنصر، ومن جهة أخرى فإن جريمة التزوير تقوم على تغيير الحقيقة في المحرر تغييرا ماديا أو معنويا .

أما عناصر جريمة استعمال المزور فإن صفة المتهم المتابع بجريمة استعمال الورقة المزورة كونه قاضيا أو موظفا لا تدخل في الاعتبار، ومن جهة أخرى فإن جريمة الاستعمال لا علاقة لها بعنصر التغيير، وإنما يؤسس على فعل استظهار الوثيقة المزورة وتقديمها إلى الجهة المختصة لاستعمالها والاستفادة منها.[1]

وإذا كانت جريمة التزوير تتفق مع جريمة استعمال المزور من حيث أن كل منهما قابلة للسقوط والانقضاء بمرور الزمن، وفقا للأوضاع والقواعد المنصوص عليها في المواد 6،7،8 من قانون الإجراءات الجزائية، إلا أنهما يختلفان من حيث بداية الحساب لمدة التقادم،فبينما يبدأ حساب تقادم دعوى جريمة التزوير من تاريخ وقوع الجريمة، أو من تاريخ آخر إجراء من إجراءات التحقيق أو المتابعة، فإن حساب تقادم دعوى جريمة استعمال المزور يبدأ من تاريخ التخلي صراحة عن استعمال الوثيقة المزورة وعدم الاحتجاج بها تجاه الغير باعتبار أنها جريمة مستمرة على عكس جريمة التزوير التي تعتبر جريمة آنية وقتية .

وفي هذا المعنى صدر قرار عن المحكمة العليا أن الجريمة المستمرة يبدأ حساب تقادمها من يوم انتهاء الفعل الجرمي، أي من تاريخ التخلي تماما عن تكرار الفعل[2] .

المحررات العرقية / انظر المادة 220 من قانون العقوبات الجزائري. كما لا تختلف العقوبات المقررة للتزوير في بعض الشهادات عن تلك المقررة لاستعمال المحرر المزور .

أما استعمال المحررات الرسمية أو العمومية المزورة فعقوبتها تختلف عن تلك المقررة للتزوير إذ يعاقب على الاستعمال بالسجن المؤقت من 15 إلى 10 سنوات، سواء حصل التزوير من الموظف المختص بالتحرير أو غيره هي أدنى من عقوبة التزوير الذي يرتكبه غير الموظف المختص وهي السجن المؤقت من 10 إلى 20 سنة سجن "، / وأدنى بكثير من عقوبة التزوير الذي يرتكبه الموظف المختص (السجن المؤبد) / انظر المادة 218 من قانون العقوبات الجزائري .

[1]– عبد العزيز سعد، المرجع السابق، ص 79.

[2]– نفس المرجع، ص 79.

وخلاصة القول بشأن الاتفاق والاختلاف بين جريمة التزوير وجريمة استعمال المزور، ومدى الارتباط القائم بينهما هو أنه على الرغم من وجود ارتباط بينهما يجعل قيام جريمة الاستعمال متوقفة على قيام وإثبات جريمة التزوير بحيث لولا توفر التزوير لما قامت جريمة الاستعمال للمزور .[1]

ويكمن جوهر الاختلاف كون أن كل جريمة منهما مستقلة عن الأخرى ومنفصلة عنها، ولا يمكن الوقوع في الخطأ واعتبارهما جريمة واحدة ذات وصفين متكاملين هما التزوير واستعمال المزور، خاصة وان الأول يقع بأفعال تختلف بطبيعتها عن أفعال الاستعمال، فإذا كان التزوير يقوم على تغيير الحقيقة في محرر، فإن الاستعمال يتأسس على فعل الاستظهار بوثيقة مزورة وتقديمها إلى الجهة المختصة لاستعمالها والاستفادة منها، وتغيير الحقيقة يكون بطرق محددة على سبيل الحصر، أما الاستعمال فيكون بأي فعل يتضمن إبراز المحرر والتمسك بقيمته كما لو كان صحيحا .[2]

أما بخصوص تقادم العقوبة وباعتبار أن جريمة التزوير جريمة وقتية فهي تتقادم من يوم ارتكابها بعكس جريمة استعمال الوثيقة المزورة التي يبدأ تقادمها من يوم تركها والتخلي نهائيا عن استعمالها

الفرع الثالث: الفرق بين التزوير والنصب:

تعد جريمة النصب من الجرائم المادية وأشدها خطورة وأكثرها، فالجاني في هذه الجريمة يخاطب ملكة الفكر والخيال وملكة الشعور والإرادة لدى من يتلقى هذه المخاطبة منه لاقتناعه بتسليم المال، مما ينقل حيازة المال إلى الجاني، [3] ويتمثل أساس جريمة النصب[4] في الاستيلاء على المال المنقول

[1]– عبد العزيز سعد، المرجع السابق، ص 80.

[2]– رؤوف عبيد، جرائم التزييف والتزوير، الطبعة الرابعة، مطبعة الاستقلال، مصر، 1984، ص 173.

[3]– حنان ريحان المضحكي، الجرائم المعلوماتية – دراسة مقارنة – الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2014، ص 306.

[4]– تجدر الإشارة إلى أن النصب كان في القانون الروماني صورة من جريمة سلب مال الغير والتي تشمل أيضا السرقة وخيانة الأمانة، وكان تشريع الثورة الفرنسية الصادر عام 1791 أو من وضع نص خاص للنصب ثم جاء تشريع عام 1810 متضمنا العقاب عليه بوصفه جريمة قائمة بذاتها لها خصائصها ومميزاتها التي تميزها عن السرقة .

المملوك للغير بنية التملك ويتم برضا المجني عليه نتيجة لما وقع عليه من تأثير احتيالي من الجاني.[1]

وقد تعرض قانون العقوبات الجزائري لجريمة النصب في المادة 372 من قانون العقوبات[2] حيث نص على :" كل من توصل إلى استلام أو تلقي أموال أو منقولات أو مستندات أو تصرفات أو أوراق مالية لو وعود أو مخالصات أو إبراء من التزامات أو الحصول على أي منها أو شرع في ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر بغرامة من 20000 إلى 100,000 دج".

ومن خلال نصوص جريمة النصب يتضح لنا أن الشارع لم يحدد تعريفا له ومن ثم بات على الفقه الاجتهاد لوضع تعريف للنصب.

فعرفه البعض بأنه :" الاستيلاء على مال منقول للغير بوسيلة احتيالية تحمل المجني عليه على التسليم في ماله ".[3]وعرفه البعض بأنه :" الاستيلاء على الحيازة الكاملة عمدا بطريق الحيلة أو الخداع على مال مملوك للغير ".[4]

ويتكون الركن المادي لجريمة النصب من ثلاثة عناصر تتمثل في استعمال وسيلة من وسائل التدليس والواردة على سبيل الحضر في المادة 372 وهي استعمال أسماء أو صفات كاذبة، وكذا استعمال المناورات الاحتيالية التي تتحقق إذا اصطحب الكذب بأعمال مادية أو مظاهر خارجية يستعين بها المتهم لإقناع الضحية بصدق القول كنشر الأكاذيب أو استغلال صفة، كما قد يستعين

[1]– خثير مسعود، المرجع السابق، ص 56.

[2]– هذه المادة مقتبسة من نص المادة 313 من قانون العقوبات الفرنسي، ويلاحظ على هذا النص أنه جاء مبتورا ولا يؤدي المعنى المتوخى حسب ما يتبين من النص في نسخته الفرنسية حيث جاء النص كالآتي :" .... أو صفات كاذبة وإما باستعمال مناورات احتيالية لإيهام الغير بوجود سلطة خيالية أو اعتماد مالي خيالي أو لإحداث الأمل في الفوز بأي شيء... " وتقابل هذه المادة أيضا المادة 336 من قانون العقوبات المصري .

[3]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دون طبعة، منشاة المعارف، مصر، 1997، ص 73 .

[4]– محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، المرجع السابق، ص 528.

المتهم بأوراق مزورة أو غير مزورة ينسب صدورها إليه وغيرها من الأشياء التي يرى فيها المحتال صلاحيته لإقناع المجني عليه بكذبه .[1]

أما العنصر الثاني فيتمثل في سلب مال الغير ويتعلق الأمر بالأموال والمنقولات والسندات والتصرفات والأوراق المالية والوعود والمخالصات والابراءات من الالتزامات، أما العنصر الثالث فيتمثل في وجود رابطة سببية بين الوسائل الاحتيالية وتسليم الأشياء الذي يكون لاحقا على استعمال التدليس وأن تكون هذه الوسائل الاحتيالية من شانها أن تؤدي إلى تسليم أعمال نتيجة انخداع الضحية .[2]

وتعد جريمة النصب من الجرائم العمدية التي يتطلب لتحققها توافر القصد الجنائي باعتباره انصراف الإرادة إلى السلوك المادي للجريمة وهو عالم بذلك، إضافة إلى القصر الخاص والمتمثل في نية الكذب بغية سلب المجني عليه من ماله كله أو بعضه [3].

ويقترب التزوير من النصب، ففي كلاهما يتم جعل أمور غير حقيقية في صورة أمور حقيقية وصادقة، أي أنهما يقومان على الكذب، أو استعمال طرق احتيالية لتحقيق الغرض المنشود من كل جريمة، حيث أن النصيب يقوم فيه الجاني بالاحتيال من أجل الحصول على ثروة الغير المنقولة، بحيث يستعمل أسماء أو صفات كاذبة أو طرق احتيالية أخرى تساهم في إقناع المجني عليه وانصياعه لرغبة المحتال فيسلم له طواعية وعن طيب خاطر أمواله المنقولة.[4] فالتزوير يقترب من النصب لأنهما يتفقان في الكذب وإلباس أمور على غير حقيقتها ثوب الحقيقة .[5]

وإذا كان التزوير والنصب ينطويان على تغيير الحقيقة إلا أنهما يختلفان اختلافا جوهريا ذلك أنه في التزوير يشترط وقوعه على محرر، أما النصب فيمكن وقوعه دون ذلك أو بمحرر كوسيلة لارتكابه، وقد تجتمع الجريمتين في فعل إجرامي واحد، ولكن القانون الفرنسي أطلق طرق التزوير ولم تعد محددة على سبيل الحصر.[6]

---

[1]– للمزيد انظر : احسن بوسقيعة ،المرجع السابق، ص 317 وما بعدها .

[2]– للمزيد انظر : حنان ريحان مبارك المضحكي، المرجع السابق، ص ص 309، 310 .

[3]– رمسيس بهنام، المرجع السابق، ص 532.

[4]– آمال بن خليفة، المرجع السابق، ص 57.

[5]– فتوح الشادلي، عفيفي كامل عفيفي، المرجع السابق، ص 233.

[6]– نفس المرجع والصفحة .

وهناك فروق جوهرية بين جريمتي التزوير والنصب تعطي لجريمة التزوير ذاتية خاصة بها، ومن أهم الفروق أن النصب يشترط لقيامه أن يؤدي الاحتيال أو الكذب أو تغيير الحقيقة بالطرق الاحتيالية إلى سلب كل ثروة المجني عليه أو بعضها، أي أن المحتال يتسلم مال منقول مملوك للغير عن إرادة ولو كانت معيبة بعيب من عيوب الإرادة وهو الغلط، أما التزوير فيتحقق بمجرد تغيير الحقيقة بإحدى الطرق المحددة على سبيل الحصر، ولا يشترط تسلم الجاني لأموال معينة، ويحصل فيها التوقيع على المحرر أو تغييره بدون علم أو إرادة المجني عليه.

المبحث الثاني: مفهوم جريمة التزوير الالكتروني

تعد جريمة التزوير الالكتروني إحدى أنواع الجرائم الالكترونية، وتعتبر من أخطر طرق الغش التي تقع في مجال المعلوماتية، على اعتبار أن أجهزة الكمبيوتر والانترنت أصبحت محلا في غالب الأحوال للأوراق ولم يقتصر ذلك على مجال معين بل تعدت إلى كافة المعاملات مثل عمليات الدفع وطلبات البضائع وتحويل الأموال.

فقد ساهمت ثورة المعلومات والتكنولوجيا الرقمية في إرساء معالم التحول نحو النموذج الالكتروني لانجاز مختلف المعاملات على مستوى الإدارات التي أصبحت بدورها رقمية، وهذا ما دفع تشريعات الدول إلى تجريم كل ما من شأنه المساس بهذه الوثائق وحمايتها جنائيا من كل أشكال التزوير.

وسنحاول من خلال هذا المبحث بيان تعريف التزوير الالكتروني كجريمة ترتكب في بيئة الكترونية بكل ذكاء واحترافية في المطلب الأول، ثم نبين خصائص هذه الجريمة في المطلب الثاني، لنقف أخيرا عند التفرقة بين جريمة التزوير الالكتروني وجرائم أخرى مشابهة في المطلي الثالث.

المطلب الأول: تعريف التزوير الالكتروني

لما أصبح النظام المعلوماتي جزءا لا يتجزأ من حياة الأفراد اليومية، ومع الانتشار المتزايد المعلومات أصبح هناك قلق متزايد من ارتكاب جرائم تزوير البيانات والمعلومات المخزنة أو المنقولة عبر شبكة الانترنت، ما يشكل انعكاسا سلبيا على الثقة التي يوليها الأفراد للنظام المعلوماتي .

وإزاء ضيق نطاق النصوص التقليدية للتزوير الذي يقع في مجال المعالجة الالكترونية نجد أن بعض التشريعات العقابية بما فيها قانون العقوبات الجزائري وكذا المصري لم يتضمن تعريفا للتزوير، حيث اكتفت ببيان الطرق التي يرتكب بها التزوير وأنواعه والعقوبات المقررة لها .

لذا سنحاول من خلال هذا المطلب إعطاء التعريف الفقهي لجريمة التزوير الالكتروني وبيان بعض التعريفات الواردة في بعض التشريعات بخصوص هذه الجريمة وذلك على النحو الآتي بيانه:

الفرع الأول: التعريف الفقهي للتزوير الالكتروني

نتعرض في هذا الفرع لتعريف التزوير الالكتروني كإحدى الجرائم الالكترونية التي ترتكب بواسطة الحاسب الآلي أو شبكة حاسوبية، أو داخل نظام حاسوب تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية، بمعنى أنها تتمثل في المساس العمدي بأنظمة الحاسب الآلي ومكوناته وبرامجه باستخدام أي تقنية حديثة من تقنيات الحوسبة والاتصال، حيث يكون الفاعل فيها ملما بهذه التقنية، ومن شأن هذا السلوك المساس بمصلحة محمية قانونا والتي تتمثل في الحق في سرية وتكاملية ووفرة وإتاحة المعلومات .[1]

ويعرف التزوير الالكتروني بأنه:" تغيير للحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية وذلك بنية استعمالها .[2]

كما يعرف أيضا :" التزوير الذي يتم بوسيلة معلوماتية في محرر معلوماتي أو بوسيلة الكترونية في محرر الكتروني ".[3]

ويعرف التزوير الالكتروني أيضا بأنه:" تغيير للحقيقة بأي وسيلة كانت سواء كان ذلك في محرر أو دعامة طالما أن هذه الدعامة ذات أثر في إنشاد حق، أو لها شأن في إحداث نتيجة معنية".[4]

---

[1]– زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي دون طبعة،دار الهدى، الجزائر 2011، ص 43.

[2]– علي عبد القادر الفهوجي، المرجع السابق، ص 63.

[3]– عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنت في التشريعات العربية، المرجع السابق، ص 49.

[4]– أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الآلي، دراسة مقارنة الطبعة الأولى، دار النهضة العربية، مصر، 2000، ص 407.

ويعد التزوير الالكتروني كل تغيير للحقيقة في البيانات أو المعلومات المعالجة عن طريق الحاسب الآلي، والتي أصبح لها كيان مادي ملموس يقابل أصل المحرر المكتوب.[1]

وعرف أيضا بأنه تغيير في حقيقة مستند معلوماتي يهدف الجاني من وراء استخدامه والاستفادة منه.كما عرف بأنه ذلك التزوير الذي ينصب على مخرجات الحاسب الآلي، أي البيانات والمعلومات الخارجة منه بشرط أن تطبع على دعامة مكتوبة أو مسجلة أي يكون لها كيان مادي يمكن إدراكه، ولم تم تغيير الحقيقة دون طباعة، وذلك أمر وارد، فلا يمكن أن يطلق عليه تزوير .[2]

وهناك جانب من الفقه من عرف التزوير الالكتروني بأنه الأفعال العمدية وغير الشرعية التي من شأنها إلحاق الضرر المادي بالغير، سواء بإتلاف المعطيات الالكترونية أو فسخها أو تعديلها أو إدخالها أو صنعها أو بجميع أشكال الاعتداء على عمل النظام المعلوماتي، وذلك بهدف التزوير والحصول على مردود اقتصادي لفائدة الفاعل أو لفائدة الغير.[3]

من خلال التعريفات السابقة يتضح لنا أن التزوير الالكتروني يرتبط بتغيير الحقيقة ويكون عن طريق التلاعب في المعلومات الموجودة داخل الجهاز الآلي عن طريق الحذف أو الإضافة ثم إخراجها عن طريق دعامة معلوماتية، وذلك بنية الإضرار بالغير .

ويؤكد الفقد على أن التزوير يجب أن يتم عن طريق مخرجات الحاسب الآلي، وهي المعلومات التي انفصلت وأخرجت من الحاسب في شكل طباعة مكتوبة، أو في شكل دعامة الكترونية، أما المعلومات التي يتضمنها نظام المعالجة الآلية للمعطيات أي المسجلة في ذاكرة النظام، والتي تعد جزء منه، فإن الاعتداء عليها بالتلاعب سواء بإدخال معلومات عليها وتعديلها أو حذفها لا يشكل تزويرا الكترونيا، وإنما يشكل جريمة التلاعب غير المصرح به بمعلومات نظام المعالجة الآلية للمعطيات

[1]– عبد الفتاح بيومي حجازي، الحكومة الالكترونية، الكتاب الثاني، المرجع السابق، ص 180.

[2]– أحمد حسام طه تمام، المرجع السابق، ص 357 .

[3]– علي كحلون، الجريمة المعلوماتية، وتوجهات محكمة التعقيب، مجلة الأخبار القانونية، تونس، السنة السابقة عدد 127/126، جانفي 2012، ص 16 / عن الهام بن خليفة، المرجع السابق، ص 69 .

.وهي جريمة منصوص عليها في المادة 394 مكرر 1 من القانون العقوبات الجزائري، والمادة 323 الفقرتين الثانية والثالثة من قانون العقوبات الفرنسي .[1]

وعليه التزوير في النطاق المعلوماتي يتم عن طريق تغيير الحقيقة على الشرائط أو المستندات التي تمثل مخرجات الحاسب الآلي طالما أن التغيير ذاته قد طال البيانات والموجودة في جهاز الحاسب، شرط حصول الضرر، والذي يتمثل في اهتزاز الثقة المفترضة في المحررات الرسمية عند وقوع التزوير الالكتروني في المحرر أو المساس بحقوق أحد الأفراد إن محل التزوير المعلوماتي محررا عرفيا .[2]

وتغيير الحقيقة يمكن تصور وقوعه على المحررات في نطاق المعلوماتية مثل تغيير الحقيقة في محرر من مستخرجات النظام المعلوماتي، وقد يتم الاعتداء عليه قبل خروجه ولكن لا يكون تزويرا إلا بعد خروجه على دعامة مكتوبة أو مسجلة .[3]

وما يمكن قوله أن جريمة التزوير الالكتروني تعد من الجرائم الالكترونية التي يمكن أن ترتكب أثناء معالجة وتحليل البيانات لتخرج في الأخير بشكل مزور، أو تنصب مباشرة على مخرجات الحاسب الآلي، أي البيانات والمعلومات الخارجة منه والمثبت على دعامة مكتوبة والتي إنتاجها عن طريق الطابعات الملحقة بالحاسب أو على دعامة الكترونية كالأشرطة الممغنطة والأقراص المغناطيسية، والمصغرات الفيلمية وغيرها من الدعامات الالكترونية، أو تعرض المعالجة على شاشة الكمبيوتر .[4]

ومن خلال استعراض هذه التعاريف نلخص إلى أن التزوير الالكتروني هو تغيير الحقيقة في المستندات المعالجة آليا وذلك بنية استعمالها فيما زور من أجله ما يؤدي إلى إلحاق ضرر بالغير .

---

[1]– رشيدة بوكر، جرائم الاعتداء على نظام المعالجة الآلية للمعطيات، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012، ص 262 .

[2]– عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 140 .

[3]– أحمد حسام طه تمام، المرجع السابق، ص 390 .

[4]– عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص ص 183، 184.

الفرع الثاني: التعريف التشريعي للتزوير الالكتروني:

سبقت الإشارة إلى أن التزوير في هو تغيير الحقيقة بقصد الغش في محرر بإحدى الطرق المبنية في القانون تغييرا من شانه أن يسبب ضررا بالغير.

وإزاء ضيق النصوص التقليدية للتزوير بشأن مواجهة التزوير الذي يقع في المجال الإلكتروني، نجد أن بعض التشريعات العقابية بما فيها قانون العقوبات الجزائري والمصري لم تتضمن تعريفا للتزوير، حيث اكتفت ببيان الطرق التي يرتكب بها التزوير وأنواعه والعقوبات المقررة له.

لكن هناك بعض التشريعات العقابية التي أوردت تعريفا للتزوير يحدد مدلوله ويبين أركانه، ومن بين هذه التشريعات قانون العقوبات الفرنسي من خلال القسم الأول ضمن الكتاب الرابع تحت عنوان "الاعتداءات ضد الثقة العامة " وهذا في المادة 441 المعدلة في 14 ماي 1993 حيث نصت هذه الأخيرة على أن التزوير يقوم على كل تغيير في الحقيقة بغش من شأنه أن يسبب ضررا، والذي يرتكب بأي طريقة كانت في محرر مكتوب أو كل دعامة أخرى للتغيير عن الفكر الذي يكون الغرض منه إثبات حق أو واقعة لها آثار قانونية.

والملاحظ على نص المادة أعلاه أن المشرع الفرنسي لم يحدد طرق التزوير بشرط أن يكون على كتابة سواء ورقية أو الكترونية وبالتالي أدرج جريمة التزوير الالكترونية ضمن جرائم التزوير العادية للمحررات حماية للثقة المقترحة في هذه المستندات وبالتالي امتدت الحماية إلى المحررات المعلوماتية سواء كانت تخضع للمعالجة الآلية أم لا؟ .[1]

ولعل من أهم الأسباب التي أدت بالمشرع الفرنسي إلى إدراج هذه الجريمة ضمن جرائم التزوير العادية للمحررات هو أنه بصدور هذا القانون خرجت جريمتا تزوير المستندات المعالجة آليا واستعمالها من بين جرائم الاعتداء على نظام المعالجة الآلية للمعطيات، وهو أمر منطقي يجد مبرره في اختلاف المصلحة المحمية بالقانون والتي تقف وراء تجريم كل منهما، فالمصلحة المحمية من تجريم الاعتداء على نظام المعالجة الآلية للمعطيات هي مصلحة فردية تخص صاحب هذا النظام المعلوماتي التي ومن يسيطر عليه فردا أو شركة في حين أن المصلحة التي يحميها القانون بصدد

[1]– عبد الفتاح بيومي حجازي، الدليل الجنائي في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 143 .

جريمة التزوير في المستندات والمحررات، ومنها تزوير المستندات المعلوماتية وهي حماية الثقة العامة في المستندات أيا كان شكلها، وبذلك تتضح أهمية هذا التعديل في أنه لم يقصر الحماية على المستندات المعالجة آليا فقط، وهنا امتدت الحماية إلى المستندات المعلوماتية سواء كانت تخضع لهاته المعالجة آليا أم لا؟.

وعليه تستوعب هذه الصيغة التزوير في أي وعاء يحمل أفكار ومعان لها قيمة قانونية في مجال إثبات حق أو مركز قانوني، متجاوزة معنى المحرر الورقي إلى أشكال أخرى، بل حتى وتلك التي لم يتوصل إليها العلم بعد، كما أن هذه الصيغة جاءت مطلقة من حيث بيان طرق وقوع التزوير لأن ذلك يرتبط بجانب تقني أن تتعدد الأساليب وتصبح لا حصر لها .[1]

أما المشرع المصري وبالرجوع إلى نص المادة 23 من قانون التوقيع الالكتروني فنجدها تشير إلى أن التزوير الالكتروني يتم بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر، وهي صيغة لم تكن موفقة في النص على طرق التزوير لتعددها واختلافها وتجددها لذلك أردفها بعبارة " أو بأي طريق آخر " .

كما أن المشرع المصري لم يبين طبيعة الوثيقة المعلوماتية محل الحماية، حيث لم يتطرق لتلك القيمة القانونية التي تتمتع بها تلك المعلومات التي تتضمنها، مما سيؤدي إلى الخلط بين فكرة المحرر وأفكار أخرى هي محل حماية من القانون غير أن لا تدخل في مدلول المحرر .[2]

وقد عرفت الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية "اتفاقية بودابست "[3] التزوير الالكتروني وهذا في المادة " 07 منها تحت عنوان بأنه التزوير المرتبط بالحاسب الآلي وهو يتكون من خلق أو تعديل غير مصرح به للبيانات المسجلة بطريقة من شأنها أن تجوز هذه البيانات المسجلة له قوة دامغة مختلفة عن سياق المعاملات القانونية، والتي تكون مؤسسة على صحة البيانات

---

[1]– براهمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة بسكرة، الجزائر، ص 194 .

[2]– أشرف توفيق شمس الدين، حجية المحررات الالكترونية في الإثبات، ورقة عمل مقدمة في ندوة المعاملات القانونية الالكترونية وعقود التجارة الالكترونية، دبي، 2007، ص 40 .

[3]– حرص مجلس أوروبا على التصدي للجرائم المعلوماتية من خلال اتفاقية بودابست الموقعة في 2001/11/23 المتعلقة بالإجرام الكوني وتتضمن 48 مادة .

المستخرجة من خلال هذه البيانات المستخرجة، وبالتالي يمكن أن تكون موضوعا لخداع المصالح القانونية المحمية .

وبالرجوع إلى المشرع الجزائري نجد قد نص على جرائم التزوير في المحررات وهذا في المواد من 214 إلى 229 من قانون العقوبات، دون أن يعطي تعريفا للتزوير ولا بيان أركانه بل اكتفى ببيان أنواع جرائم التزوير والتي تتمثل في التزوير في المحررات الرسمية أو العمومية الواردة في المواد 214 إلى 217 والتزوير في المحررات التجارية أو المصرفية أو العرقية في المواد 219 و 220 والتزوير في بعض الوثائق الإدارية والشهادات في المواد من 222 إلى 229 .

من خلال استعراض هذه التعاريف نستنتج أن التزوير الالكتروني هو تغيير الحقيقة في مخرجات أنظمة الحوسبة والاتصال والتي يمكن الاحتجاج بها لإثبات الحقوق بأي طريقة كانت من شأنها إلحاق الضرر بالغير، وبنية استعمالها فيما زور من أجله .

المطلب الثاني: خصائص جريمة التزوير الالكتروني :

لقد أفرزت ثورة الاتصالات والمعلومات وسائل جديدة للبشرية تجعل الحياة أفضل من ذي قبل، غير أنها فتحت الباب على مصرعيه لظهور صور من السلوك المنحرف اجتماعيا التي لم يكن من الممكن وقوعها في الماضي .فمن جهة فقد سمحت نظم الحاسب الآلي بظهور صور جديدة من الجرائم التي لم تكن موجودة في الماضي ومن جهة أخرى أتاحت هذه النظم الفرصة لارتكاب الجرائم التقليدية بطرق غير تقليدية .

فوقوع الجريمة في مسرح رقمي وفضاء افتراضي تخيلي لا يعرف الملموس أضفى عليها جملة من الخصائص تنفرد بها عن الجريمة التقليدية فارتباط جريمة التزوير الالكتروني بجهاز الحاسوب والانترنت يضفي عليها خصوصية غير عادية تميزها عن باقي الجرائم التقليدية ولا تتعلق هذه الخصوصية بالجريمة فحسب، إنما تتعدى ذلك لتميز مرتكب الجريمة والمجني عليه أيضا .

ولتوضيح هذه الخصائص ارتأينا تقسيم هذا المطلب إلى ثلاث فروع،نتناول في الفرع الأول بيان خاصية صعوبة الكشف جريمة التزوير الإلكتروني،أما الفرع الثاني فقد خصصناه لكون جريمة التزوير الالكتروني عابرة للحدود،ثم تطرقنا في الفرع الثالث لتفرد شخصية المجرم الإلكتروني.

الفرع الأول: صعوبة الكشف عن جريمة التزوير الإلكتروني

إن الجرائم الإلكترونية تتصف بالخفاء، أي عدم وجود آثار مادية يمكن متابعتها، وهي خطيرة، وصعبة الاكتشاف أو هي صعبة في تحديد مكان وقوعها، أو مكان التعامل معها، بسبب اتساع نطاقها المكاني، وضخامة البيانات.[1]

وتتميز جريمة التزوير الإلكتروني بأنها جريمة لا تترك أي أثر مادي على الوثيقة المزورة، فهي جريمة تقع في بيئة الكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الالكترونية غير مرئية ولا توجد مستندات ورقية، حيث لا نشاهد آثار التغيير بالإضافة أو بالحذف باستخدام أدوات أو مواد كيميائية، بينما لا تظهر هذه الآثار في النوع الأول حيث تتم الجريمة من خلال الوصول إلى المعلومات وتغيير مضمونها، فهي جريمة فنية غير ملموسة، وبالتالي يتعذر ترك الدليل المادي على التزوير و يتعذر إثباته حيث أن هذه الجريمة تتم في بيئة افتراضية، وإذا تم اكتشافها فإن ذلك يحصل بالصدفة .[2]

فهذه الجرائم لا تترك أثرا لها بعد ارتكابها، علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت، فهذه الجرائم لا تترك أثرا، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظم الجرائم الالكترونية يتم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها، فهذه الجرائم من الجرائم المستحدثة التي لا تترك شهود يمكن استجوابهم ولا أدلة مادية يمكن فحصها، ومن هنا تأتي صعوبة الكشف عن هذه الجرائم .[3]

وما يزيد من صعوبة الاحتفاظ الفني بآثار الجريمة ويعرقل عملية الإثبات في مجال هذه الجرائم إعاقة الوصول إلى الدليل غير المرئي بوسائل الحماية الفنية فهي في الغالب يكون مرمزا أو مشفرا (كاستخدام المجرم المعلوماتي لكلمات السر أو دس تعليمات خفية فيها أو ترميزها).[4]

---

[1]– خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009، ص 79

[2]– عبد الله بن مسعود محمد السبراني، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الالكتروني، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011، ص 66 .

[3]– خالد ممدوح إبراهيم، المرجع السابق، ص 80.

[4]– نبيلة هبة هروال، جرائم الانترنت –دراسة مقارنة – أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2014، ص 49 .

وتجدر الإشارة إلى أنه كثيرا ما تكتشف هذه الجرائم بمحض الصدفة البحتة ومن بين أسباب اختفاء هذه الجرائم إحجام المجني عليه عن الإبلاغ عنها، إذ نجد أن أغلب الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك تكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها[1]، خصوصا إذا كان المجني عليه عبارة عن مؤسسات مالية كالبنوك والمؤسسات الادخارية، حيث تخشى مجالس إدارتها عادة أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها وانصرافهم عنها .[2]

إضافة إلى هذا فإنه يستلزم لكشف الجرائم الالكترونية عموما والتزوير الالكتروني بصفة خاصة والاهتداء إلى مرتكبيها وملاحقتهم قضائيا استراتيجيات تحقيق وتدريب خاصة، أي خبرة فنية تتلاءم مع طبيعة هذا الجرم وتسمح بتفهم ومواجهة الخصوصيات التي يقوم ويرتكز عليها هذا الأخير والأساليب التي تستخدم في ارتكابه لهذا وجدت أجهزة العدالة (الضبطية القضائية، جهات التحقيق، القضاة) نفسها غير قادرة على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذا النوع المستحدث والفريد من الإجرام، أي أنها أصبحت فاشلة في مواجهته[3]، فقد لا يتعاملون بمهارة واحتراف مع الدليل الالكتروني، كأن يتسبب الشرطة أو الجهات المختصة بالتحقيق بدون قصد أو بطريق الخطأ في إتلاف الدليل الالكتروني أو تدميره كما في حالة محو البيانات الموجودة على الأسطوانة الصلبة، وقد يتجاهل المحقق الدليل الالكتروني تماما ظنا منه أنه غير مهم، أو لا يقوم بمصادرة جهاز الكمبيوتر المستخدم في ارتكاب الجريمة أو ملحقاته مثل الطابعة أو الماسح الضوئي[4].

---

[1]– ويجدر التنويه إلى أن جرائم الانترنت التي تم الإبلاغ عنها إلى السلطات المختصة لم تتعدى 15 / فمثلا نجد أن بريطانيا تشهد حوالي 300 جريمة انترنت، ولا يبلغ إلا عن 90 منها وذلك لجهل الأشخاص بها وبمدى خطورتها واعتقادهم بنقص خبرة الشرطة وعدم قدرتها في ملاحقة مرتكبها والتحقيق فيها / نبيلة هبة هروال، المرجع السابق، ص 49.

[2]– هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، دون طبعة، مكتبة الآلات الحديثة، مصر، 1994، ص 146.

[3]– هشام فريد رستم، المرجع السابق، ص 27.

[4]– خالد ممدوح ابراهيم، المرجع السابق،ص 81.

كما أن جريمة التزوير الالكتروني تعد من الجرائم التي تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها، فقد يستخدم الجاني اسما مستعارا أو يرتكب فعله من خلال إحدى مقاهي الانترنت، فجرائم التزوير تتم دون تحديد شخص مرتكبها أو ضبط المحرر المزور[1].

الفرع الثاني: جريمة التزوير الالكتروني عابرة للحدود

إن تعيير " الجريمة العابرة للدول أو العابرة للحدود أو جرائم عبر الوطنية هي تلك التي تقع بين أكثر من دولة، بمعنى أنها لا تعرف بالحدود الجغرافية للدول. وفي عصر الحاسب الآلي ومع انتشار شبكة الاتصالات العالمية (الانترنت)، أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة بحيث يغدو أمر التنقل والاتصال فيما بينهما أمرا سهلا، طالما حدد عنوان المرسل إليه، أو أمكن معرفة كلمة السر، وسواء تم ذلك بطرق مشروعة أو غير مشروعة .[2]

في ظل هذه البيئة يمكن أن توصف جرائم التقنية بأنها جرائم عابرة للدول، إذ غالبا ما يكون الجاني في بلد، والمجني عليه في بلد آخر، كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه، ولهذا تعتبر الجرائم الالكترونية شكلا جديدا من الجرائم الوطنية أو الإقليمية أو القارية .

فالجريمة الالكترونية لا تعترف بالحدود بين الدول والقارات ولذلك فهي جريمة عابرة للقارات، فهي تعتبر شكلا جديدا من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل جرائم التعدي على قواعد البيانات، وتزوير وإتلاف المستندات الالكترونية، والاحتيال المعلوماتي وتزوير وسرقة بطاقات الائتمان وغيرها، ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أصقاع الأرض، انعكست أيضا على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في

[1]– (IP يقصد به العنوان الرقمي الذي يميز ويحدد هوية الجهاز) لكن هذا الرقم غير موحد على المستوى العالمي، إذ أن هناك أقلية من الدول التي تتبعه دون غيرها وخاصة الدول العربية /للمزيد انظر: نبيلة هبة هروال، المرجع السابق، ص 52–53.

[2]– جلال محمد الزغبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية،دراسة مقارنة،الطبعة الأولى،دار الثقافة للنشر والتوزيع،الأردن،2010، ص 91.

انتهاكاتهم للقانون، وهو ما يعني أن مساحة مسرح الجريمة الالكترونية لم تعد محلية، أي أنها أصبحت عالمية .[1]

الفرع الثالث: تفرد شخصية المجرم

تتطلب الجرائم الالكترونية على عكس نظيراتها التقليدية حرفية عالية لارتكابها أي يجب أن يتمتع المجرم فيها المسمى بمجرم الانترنت أو "المجرم التقني " أو " المجرم المعلوماتي " أو الهاكر، و ظهر هذا المصطلح لأول مرة في الستينات ولم يكن يشير أبدا إلى الإجرام، إذ أطلق في بدايته المبرمجين ذوي قدرات تقنية عالية المستوى في معهد ماساتشوستش للتكنولوجيا وكذا جامعة ستانفورد وجامعة باركلي في الولايات المتحدة الأمريكية، ولقد استخدم بهدف الكشف عن نقاط الضعف للأنظمة المعلوماتية وكذا وضع طريقة لحمايتها وخاصة فيما يخص وسائل الاتصال فنظام unix مثلا هو اختراع الهاكر Ken Thompson .

ويمكن تعريف المجرم التقني بأنه:" كل مجرم سلك سبيل التقنية لارتكاب جرمه، ذلك عن طريق استخدامه لتقنية المعلومات ".[2].

كما يمكن تعريف المجرم التقني بأنه :" شخص فائق الذكاء في المعلوماتية "، أي أنه يتمتع بمستوى مهاري خاص يدل على الكفاءة والصلاحية والأهلية التقنية، إذ يملك هذا الأخير الجبروت في الاختراق وارتكاب أفعال تقنية عبر العالم الافتراضي بطريقة لا يمكن للعامة القيام حتى ولو كانوا يملكون خاصية التعامل الحاسوبي أو شخص يرغب ويهوى فهم واستخدام الحيل التقنية لاكتشاف الأنظمة، وهو شخص يملك المهارات لاكتشاف تفاصيل الأنظمة المبرمجة والاستحواذ على موجوداتها التي تهمه .[3]

---

[1]– خالد ممدوح إبراهيم، المرجع السابق، ص 77.

[2]– نبيلة هروال، المرجع السابق، ص 52 .

[3] – Hacker «l'est un jeune surdoué en informatique», et « c'est une cyber talent et petit prodige du piratage ».

Ce terme désigne à l'origine « une personne qui aime comprendre et utiliser les finesses technique du programmes, il qualifie aussi aujourd'hui les délinquants pénétrant par

فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها، فإن الأمر يختلف بالنسبة للجرائم الالكترونية في جرائم فنية تقنية في الغالب الأعم، ومن يرتكبها عادة ما يكون من ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الانترنت .فعلى سبيل المثال فإن الجرائم الالكترونية ذات الطابع الاقتصادي مثل التحويل الالكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية عالية جدا من قبل مرتكبها .[1]

كما يتميز المجرم المعلوماتي أيضا بفئاته وأنماطه المختلفة[2]، وأساس التمييز بين تلك الأنماط هو الباعث أو الدافع إلى ارتكاب الجريمة بينما هو ساذج لدى البعض لا يتعدى الرغبة في الاستطلاع والاستكشاف فهو خبيث لدى البعض الآخر فقد يكون ماليا أو سياسيا أو غيره .

---

effraction dans des site informatique ». voir Mohamed buzabar, la criminalité informatique sue l'internet, journal de loi , N°1jurisclasseur communication , 2002 , P44

[1]– نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص 58

[2]– من بين أهم تصنيفات مجرمي المعلوماتية التصنيف القائم على أساس أغراض الاعتداء الذي أورده كل من william paul serger, vontrach davide icove في مؤلفهم جرائم الكمبيوتر الصادر عام 1995 حيث تم تصنيف مجرمي المعلوماتية إلى ثلاث طوائف : المخترقون، المحترفون والحاقدون

أ– **المخترقون** : وفي هذه الطائفة يوجد نوعين وهما : الهاكرز والكراكز

– **الهاكرز (hacker)** أو المتسلل وهو شخص بارع في استخدام الحاسب الآلي وبرامجه ولديه فضول في استكشاف حسابات الآخرين وبطرق غير مشروعة .

– **الكراكز (crackers)** أو المقتحم وهو شخص يقوم باقتحام نظام الحاسوب لإلحاق الضرر أو العبث بمحتوياته أو سرقتها، والسمة المميزة للمقتحمين هي تبادلهم فيما بينهم.

ب– المحترفون : هذه الطائفة تعد الأخطر من بين مجرمي الكمبيوتر والانترنت حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم وللجهات التي كلفتهم وسخرتهم لارتكاب جرائم الحاسوب ويتسم أفراد هذه الطائفة بالتكتم

ج– الحاقدون : هذه الطائفة تغلب عليهم عدم توافر أهداف وأغراض الجريمة المتوفرة لدى الطائفتين المتقدمتين فهم لا يسعون إلى إثبات القدرات التقنية والمهارية وفي نفس الوقت لا يسعون إلى إثبات القدرات التقنية والمهارية وفي نفس الوقت لا يسعون إلى مكاسب مادية أو سياسية وإنما يحرك نشاطهم الرغبة في الانتقام والثأر كأثر لتصرف صاحب العمل معهم، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوضعهم موظفين أو مشتركين او على علاقة بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشاة المستهدفة في نشاطهم، وتغلب على أنشطتهم من الناحية التقنية استخدام تقنيات الفيروسات والبرامج الضارة وتخريب النظم وإتلاف كل أو بعض معطياته /

ولذلك فجرائم التزوير لا ترتكب بالصدفة أو عن طريق الخطأ، بل هي جرائم يخطط لها بخبرة أشخاص ذوي مهارة فنية عالية وخبرة وذكاء، وهي ذات طابع ذهني علمي تعتمد على المعلومات والمعارف الفنية والتكنولوجية التي فرضها التقدم العلمي . كما أن الكثير من هذه الجرائم يقع بغية الحصول على المال كما هو الحال عند تزوير البطاقات الائتمانية، واختراق أنظمة البنوك وتزوير أوامر الدفع والتحويل الالكتروني للأموال، فالدافع المادي يمثل الحاجة التقليدية لهذا الهجوم وهو تأمين متطلبات العيش بطرق غير قانونية وغير مشروعة وغير متعبة .[1]

ولذلك قد تقع هذه الجرائم من طرف موظفي البنوك من يملكون التقنية والكفاءة العالية للتلاعب بالبيانات عن طريق إدخال معلومات مصطنعة، وكذلك المبرمجين الذي يكلفون بتحديث وصيانة البرامج المصرفية مما يمكنهم من التلاعب بهذه البرامج.[2]

المطلب الثالث: الفرق بين جريمة التزوير الالكتروني وجرائم أخرى مشابهة

تعد جريمة التزوير الالكتروني من الجرائم الالكترونية الأكثر تعددا وتشعبا، بدرجة يصعب التفريق بينها إلى حد كبير، ولا يدرك الاختلاف بينهما إلا المتمعن بدقة من حيث الأركان والخصائص.

فقد يكون لجريمة التزوير الالكتروني علاقة بجرائم الكترونية أخرى أخرى كجريمة التلاعب غير المصرح به في نظام المعلومات وبعض الجرائم الالكترونية الأخرى كجريمة الإتلاف وجريمة الاحتيال المعلوماتي، أو قد يكون لها علاقة بجريمة الدخول غير المشروع لنظام المعالجة الآلية .

كما أن التزوير الالكتروني قد يتقارب ويتشابه مع التزوير التقليدي ما يدفعنا إلى التأكد من أنهما يشكلان جريمة واحدة أم لا ؟

للمزيد انظر: أمين طغباش، الحماية الجنائية للمعاملات الالكترونية،الطبعة الأولى ،مكتبة الوفاء القانونية ،مصر،2015، ص ص 24،25.

[1]– أسامة سمير حسين، الاحتيال الالكتروني الوجه القبيح للتكنولوجيا، الطبعة الأولى، دار الجنادرية للنشر والتوزيع، الأردن، 2011، ص 96

[2]– براهمي حنان، المرجع السابق، ص 199 .

وعليه سنحاول من خلال هذا المطلب التطرق إلى الفرق بين جريمة التزوير الالكتروني وجرائم أخرى مشابهة، وهذا ببيان الفرق بين جريمة التزوير الالكتروني والتزوير التقليدي وهذا في الفرع الأول، في حين نخصص الفرع الثاني إلى بيان الفرق بين جريمة التزوير الالكتروني وجريمة الإتلاف المعلوماتي،أما الفرع الثالث نحاول فيه إبراز التفرقة بين جريمة التزوير الالكتروني وعلاقة بجريمة الاحتيال المعلوماتي . لنعرج في الأخير إلى بيان الفرق بين جريمة التزوير الالكتروني وجريمة التلاعب في بيانات نظام معالجة البيانات.

الفرع الأول: الفرق بين جريمة التزوير الالكتروني والتزوير التقليدي.

سبقت الإشارة أن التزوير هو تغيير حقيقة محرر، بإحدى الطرق المقررة قانونا تغييرا من شأنه إحداث ضرر، وبنية استعماله كمحرر صحيح، هذا بالنسبة للتزوير التقليدي، أما التزوير الالكتروني فهو كل تغيير في حقيقة مستند معلوماتي يهدف الجاني من وراءه لاستخدامه والاستفادة منه .

وانطلاقا مما تم تفصيله حول هذين النوعين من التزوير، يتضح لنا أن الركن المادي والمعنوي في الجريمتين هو نفسه، فالركن المادي في الجريمتين يقوم على السلوك الإجرامي المتمثل في تغيير الحقيقة وهو ما يسبب ضررا للغير.

أما بخصوص الركن المعنوي للجريمتين فيتطلب توافر كل من القصد الجنائي الخاص إلى جانب القصد الجنائي العام وهو نية استعمال المحرر فيما أعد لأجله.

ويتبين أيضا أن البيانات أو المعلومات التي يتضمنها المحرر في كلا من الجريمتين هي بيانات تصلح لأن تكون دليلا للإثبات أي مما يحتج به، وإذا كانت لا قيمة لها في الإثبات، فليس هناك مجال للتحدث عن التزوير بنوعيه .

وفي حقيقة الأمر ورغم هذا التشابه الكبير بينهما إلا أن هناك اختلاف يمكن القول أنه طفيف يتمثل بداية في أن المحرر في التزوير التقليدي هو محرر عادي، بينما المحرر في التزوير المستحدث هو الكتروني، فهو أحد مستخرجات الحاسب الآلي الورقية أو المسجلة.

ورغم هذا الاختلاف إلا أن التشريعات تعطي كلا من المحررين نفس القوة التدليلية وتعتبرهما عبارة عن كتابة متسلسلة لحروف أو أرقام أو رموز أو أوصاف أو إشارات أو أية علامات المهم أن تكون قابلة للإدراك ومفهومة.[1]

كما أن التزوير في المحرر الالكتروني يمكن تغيير الحقيقة فيه في أي وقت، وبكل سهولة، من أيا كان ولا يتسنى كشفه أو الوقوف عليه أو إقامة الدليل على وقوعه، فمثلا التزوير الواقع على التوقيع الالكتروني يسهل ارتكابه ويصعب اكتشافه ونسبته إلى مرتكبه، لأنه يتألف من شفرة تحدد هوية الموقع، وهذه الشفرة يمكن تغييرها بسهولة جدا .[2]

كما أن هذا التغيير في الحقيقة لا يترك أية آثار مادية، إذ يتأنى لمن ينظر فيه يتأنى أن يكشف ما بداخله، أو يكشف عن طريق الاستعانة الفنية خاصة وإن كان تزوير ماديا .[3]

إن جريمة التزوير الالكتروني وجميع الجرائم الالكترونية تتصف بخاصية تفرد شخصية الجاني _كما سبقت الإشارة في ذلك_ فهذا الأخير يتمتع بحرفية عالية في مجال الحاسب الآلي وثقافة الكترونية كبيرة حتى يتم تزوير البيانات والمعلومات بدقة كبيرة، في أن مرتكب جريمة التزوير التقليدي وبالرغم من كونه الجاني مثقفا، إلا أنه لا يحتاج إلى مثل هذه الثقافة والقدرات والمهارات .

ويستنتج مما تم بيانه لأوجه الشبه والاختلاف بين التزوير التقليدي والالكتروني أن الاختلاف بينهما هو اختلاف شكلي، يتعلق ربما بالتقنية الحديثة وما أفرزته من صعوبة في إثبات الجرائم المرتكبة في وسطها، ومن مجرمين جدد لم تعهدهم البشرية من قبل، وذلك الاختلاف لا يمس إطلاقا أو لا يمت بصلة لبناء الجريمتين ماديا أو معنويا، وهي الأركان الرئيسية التي يقوم عليها، فالفعل واحد، والنتيجة واحدة، والقصد واحد .

فكلا من الجريمتين تشتركان في السلوك المجرم وهو تغيير الحقيقة سواء المحرر أو المستند العادي، أو المستند الالكتروني، والقصد الجنائي واحد هو نية الإضرار بالغير نتيجة لهذا السلوك.

---

[1]– إلهام بن خليفة، المرجع السابق، ص ص 70–71.

[2]– أشرف توفيق شمس الدين، المرجع السابق، ص 573.

[3]– الهام بن خليفة، المرجع السابق، ص 71 .

الفرع الثاني: الفرق بين جريمة التزوير الالكتروني وجريمة الإتلاف المعلوماتي

الإتلاف هو تعييب الشيء على نحو يفقد قيمته الكلية أو الجزئية، أو هو تخريب الشيء محل الجريمة بإتلافه أو التقليل من قيمته وذلك بجعله غير قابل للاستعمال تعطيله[1]، ويقصد بالإتلاف هنا الإتلاف الواقع على برامج الحاسب الآلي ومعلوماته، وكذلك محو تعليمات البرامج أو إتلافها أو البيانات ذاتها، ويطلق عليه مصطلح تدمير نظم المعلومات، فإتلاف معلومات الحاسب الآلي وبرامجه فيه إفقاد لمنفعة هذه البرامج والمعلومات،

فالإتلاف يتمثل في تخريب الشيء موضوع الجريمة بإتلافه أو التقليل من قيمته بجعله غير صالح للاستعمال أو تعطيله.[2]

ومن هنا يمكن القول بتوافر الركن المادي لهذه الجريمة، وذلك بوقوع أفعال التخريب مباشرة على البرامج من إتلاف أو تعطيل وذلك باستخدام بعض الأساليب التقنية الحديثة كزرع بعض الفيروسات المدمرة، أو محو البرنامج مباشرة من خلال الوصول إليه وغيره، وقد يكون إتلاف البرامج بطريقة غير مباشرة ككسر جهاز الكمبيوتر أو إحراقه، أو عن طريق وحدات تشغيل المعلومات بإحراقها أو تفجيرها، أو العبث بمفاتيح التشغيل، أو عن طريق محو بطاقات التعريف بماهية المعلومات المختزنة، أو بإخفاء بعض البطاقات، أو خربشة شريط، بإلقاء السجائر على الأسطوانات، أو بإفساد المعطيات المختزنة مغناطيسيا بإخضاعها لقوى مغناطيسية متلفة .[3]

ومن أمثلة هذا النوع من التخريب ما حدث في إيطاليا عندما قامت مجموعة من الخبراء المتخصصين في التكنولوجيا والتي تنتمي إلى تنظيم "الأولوية الحمراء "[4]، باستخدام الديناميت في تفجير أحد مراكز المعالجة الآلي للمعلومات، ما أدى إلى خسائر بلغت 2 مليون دولار .[1]

---

[1]– حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة المقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2007، ص 312 .

[2]– فتوح الشادلي، عفيفي كامل عفيفي، المرجع السابق، ص 200.

[3]– خثير مسعود، المرجع السابق، ص 62 .

[4]– الأولوية الحمراء هي مجموعة إرهابية من أنصار الثورة السارية والتي تعقد أن إدخال المعالجة الآلية للمعلومات هو عبارة عن خطر من الغرب يستطيع من خلالها إدخال جواسيس متخصصين في المؤسسات الأساسية للدولة.

أما الركن المعنوي لجريمة الإتلاف فيتمثل في القصد الجنائي، فالإتلاف وفقا لما تقدم قد يرد على كل المال أو على جزء منه بشرط أن يكون الإتلاف في الحالة الأخيرة من شأنه أن يجعل المال غير صالح للاستعمال كما أنه لا يشترط أن يتم بوسيلة معينة بشرط ألا تكون هذه الوسيلة مما يخضع لنص عقابي آخر .[2]

وعليه فجريمة الإتلاف المعلوماتي تتم بالاعتداء على البرامج والمعلومات المخزنة في النظام، ويكن ذلك بطريق التلاعب بالبيانات سواء بإدخال معلومات مصطنعة أو إتلاف المعلومات المخزنة بمحوها أو تعديلها أو تغيير نتائجها [3].

ولذلك تتشابه طرق الإتلاف والتزوير الالكتروني، لكن يختلفان من حيث محل الجريمة ونتيجة السلوك المادي فيها، حيث يتم الاعتداء على بيانات وبرامج ويترتب على ذلك أن تصبح غير صالحة للاستعمال، فلا تؤدي وظيفتها المطلوبة، أو يحصل تعديل في برامج التشغيل من خلال اصطناع برنامج بأكمله، وهذه الصورة قد ينتج عنها عمليات تزوير واحتيال مثل قيام شركة أمريكية باصطناع برنامج تم بواسطته عدد وهمي من المؤمن عليهم، ووضع شفرة خاصة بالبرنامج وبرمجته بحيث لا يظهر عند الطباعة إلا الوثائق الصحيحة[4]، وبالتالي يؤدي هذا التعديل إلى تغيير معلومات لها أثر قانوني مما يحدث ضررا للغير، ويكون الغرض من ذلك استعمالها للاستفادة من مزايا معينة، بينما يؤدي الإتلاف إلى عدم الصلاحية للاستعمال، وعدم أداء الشيء المتلف لوظيفته المطلوبة .[5]

---

[1]– زكي زكي أمين حسونة، جرائم الكمبيوتر الجرائم الأخرى في مجال التكتيك المعلوماتي بحث مقدم للمؤتمر السادس للقانون الجنائي المنعقد بالقاهرة في الفترة من 25 إلى 28 أكتوبر 1993، ص ص 480، 481.

[2]– فتوح الشادلي، عفيفي كامل عفيفي، المرجع السابق، ص 201 .

[3]– محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2004 ،ص233

[4]– عزة محمود، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب الآلي، أطروحة دكتوراه، كلية الحقوق، مصر 1994، ص 182.

[5]– براهمي حنان، المرجع السابق، ص 202.

أما التزوير فهو تغيير للحقيقة، فمعنى إدخال تغيير على المحرر المراد تزويره على نحو يغير مضمونه أو شكله ولكن بشكل لا يعدمه أو يهدر قيمته .[1]

فالركن المادي في جريمة إتلاف المعلومات يتمثل إما في إجراء تعديلات جزئية أو كلية لها بصورة غير مشروعة، كما قد يتخذ صورة تدمير هذه المعلومات أو إدخالها بشكل غير مشروع للمعلومات والبرامج، ويتم عن طريق استخدام إحدى وظائف الحاسب الآلي، أما تدمير المعلومات حسب ما ورد في توصية المجلس الأوروبي بخصوص الجرائم المعلوماتية، فهو محوها بصورة كلية أو إخفاءها بحيث لا يمكن الوصول إليها[2].

كما قد يكون الإتلاف عن طريق التخريب، وهذا باستعمال الفيروسات أو البرامج الخبيثة للاعتداء على أجهزة الحاسب الآلي، إذ ازدادت وتيرة هذه الاعتداءات مع انتشار استخدام الانترنت واستعمال الحاسب الآلي[3].

وقد استخدمت العديد من التشريعات التي جرمت الإتلاف المعلوماتي تعبير إخفاء المعلومات أو محوها للتعبير عن تدميرها، وقد تضمنت المادة 462 فقرة 4 من قانون العقوبات الفرنسي لسنة 1988 الخاص بالجرائم المعلوماتية والتي حلت محلها في تعديل سنة 1994 المادة 323 فقرة 3 تجريما لفعل إتلاف المعلومات، ولم يضع المشرع الفرنسي شروطا تتعلق بطبيعة المعلومات بل ترك النص عاما ويتسع ليشمل كافة المعلومات .[4]

---

[1]– عبد الرحمان عبد الله حميد آل علي، جرائم التزوير المعلوماتية، رسالة مقدمة لنيل شهادة الماجستير، أكاديمية شرطة دبي، دون تاريخ، ص .78

[2]–La recommandation N" 89 sur la criminalité informatique ET LE RAPPORT final du comite d'Europe sur le problème de la criminalité ,Strasbourg,.1990

[3]– من أشهر الفيروسات والبرامج الخبيثة فيروس "حصان طروادة" – الذي يتمتع بقدرة كبيرة على الاختفاء داخل البرنامج ثم القيام بتعديله تغييره أو تدمير محتواه، وتستعمل كذلك في إتلاف المعلومات برامج أخرى كبرنامج الدودة وذلك باستخدام فيروس دودة موريس، حيث قام الطالب روبرت موريس، وهو باحث في الدكتوراه في الولايات المتحدة الأمريكية بإعاقة أكثر من ستة ألاف جهاز حاسب الخاص بوكالة الفضاء الأمريكية ناسا مستخدما برامج الدودة على شبكة الانترنت ما رتب خسائر فدرت ب 12 مليون دولار.إضافة إلى فيروس القنبلة الزمنية والقنبلة المنطقية . NAZA

[4] – Bibent Hichel , le droit du traitement de l'information, Nathan, paris 2000, P121.

أما المشرع الجزائري فلم يغفل عن تجريم فعل إتلاف المعلومات، فقد نص على تجريم فعل إتلاف المعلمات، وهذا ضمن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وهذا في المادة 394 مكرر من قانون العقوبات بقولها: (يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة(1) وبغرامة من 50.000دج إلى 200.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة .

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000دج إلى 300.000 دج

الفرع الثالث: الفرق بين جريمة التزوير الالكتروني وجريمة الاحتيال المعلوماتي :

مع انتشار الاحتيال في مجال المعلوماتية ظهر الاهتمام بتعريفه كنوع مستقل عن النصب والاحتيال في الصورة التقليدية، حيث صار يطلق عليه مصطلح الاحتيال المعلوماتي، ولو أن جوهر النصب واحد في الجريمتين أي يستعمل الجاني وسائل احتيالية للاستيلاء على مال الغير، إذ يعتبر الاحتيال عنصرا من عناصر الركن المادي لجريمة النصب.

ويكمن الفرق بين النصب والاحتيال في صورته التقليدية والاحتيال المعلوماتي في محل السلوك الإجرامي المتمثل في المعلومات ونوع الوسائل الاحتيالية التي يلجأ إليها الجاني، والتي تتمثل غالبا في التلاعب في معطيات ومعلومات الحاسب الآلي المخزنة، كما أن الوسائل الاحتيالية في جريمة النصب في الأفعال التي ذكرها المشرع على سبيل الحصر[1] من استعمال لأسماء كاذبة أو صفات كاذبة أو سلطة خيالية إلى غير ذلك، فإن وسائل الاحتيال في جريمة الاحتيال المعلوماتي يمكن أن تتخذ عدة صور مختلفة .

فالاحتيال هو كل تظاهر أو إيماء يكون صالحا لإيقاع المجني عليه في الغلط بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي، أي أن المجني عليه في جريمة الاحتيال هو من جازت عليه حيلة الجاني فانخدع بها وسلمه ماله .[2]

[1]– المادة 372 من الأمر 156.66 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات الجزائري، المعدل والمتمم

[2]– محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات،الطبعة الثانية،دار النهضة العربية، مصر،1998، ص 123.

وقد أوردت التوصية رقم 9 للمجلس الأوروبي تعريفا للاحتيال المعلوماتي، أقرته هيئة الأمم المتحدة، وبينت من خلاله السلوك الإجرامي لفعل الاحتيال المعلوماتي، وجاء فيها بأن الإدخال أو المحو أو التعديل أو كتب البيانات أو برامج الحاسوب أو التدخل المؤثر في معالجة البيانات التي تسبب خسارة اقتصادية لشخص آخر، يقصد الحصول على منفعة اقتصادية غير مشروع له .[1]

كما عرف البعض الاحتيال المعلوماتي بأنه الاحتيال الذي يرتكب باستخدام الحاسب الآلي وأنظمة الاتصال بهدف الربح المادي، وأقرت هيئة الأمم المتحدة للاحتيال تعريفا، جاء فيه بأنه الإدخال أو المحو أو التعديل أو كبت البيانات أو برامج الحاسب الآلي أو التدخل المؤثر في معالجة البيانات التي تسبب خسارة اقتصادية أو فقد حيازة ملكية شخص آخر بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر .[2]

وتقوم جريمة الاحتيال المعلوماتي عن طريق التلاعب في البيانات المدخلة وهذا بإدخال المعلومات والبيانات المراد معالجتها آليا، ومن ثم التلاعب بها إما عن طريق الجاني أو طريق شخص آخر حسن النية[3]، ومن أهم وسائل التلاعب تغيير المعلومات إما بشكل كلي أو جزئي وهذا من خلال إضافة أجزاء إليها أو استبدالها بمعلومات أخرى[4]، كما يتم التلاعب من خلال حذف جزء منها أو حذفها كلها ومن وسائل التلاعب بالبيانات إخفاءها أو إعاقة الوصول إليها .

---

[1] – la recommandation N°9 sur la criminalité informatique et le rapport final du comite d'Europe sue le problème de la criminalité, Strasbourg , 1990

[2]– غانم مرضى الشمري، الجرائم االمعلوماتية،الطبعة الأولى،الدار العلمية للنشر والتوزيع،الأردن، 2016، ص 59 .

[3] –Bainbridge David, Hacking the unauthorised access of computer system, the legal implications. MI, Rev, March1989 p 292

[4]– ومن أمثلة ذلك قيام مستخدم في بنك Indo.swez باختلاس مبلغ سبعة ملايين فرنك فرنسي، وبعد أن قام بتحويلات لنقود وهمية خزنت على ذاكرة الحاسب وقام بنقلها إلى محررات مصنعة ثم قام بفتح حساب باسمه في بنك سويسري / للمزيد انظر محمد سامي الشوا، المرجع السابق، ص 73 .

كما تتم جريمة الاحتيال المعلوماتي عن طريق التلاعب بالبرامج وهو الاحتيال المعلوماتي بحق وذلك بوسيلتين تتمثل الوسيلة الأولى في تغيير البرامج المطبقة داخل الحاسب الآلي وإجراءات تعديلات عليه [1].

ويكون الجاني في أغلب الأحيان من التقنيين من ذوي الخبرة أما الوسيلة الثانية فتتمثل في تطبيق برامج إضافية تهدف إلى تعديلات المعلومات المخزنة في الحاسب الآلي .[2]

كما تتم جريمة الاحتيال الالكتروني من قبل شخص مدخلا للبيانات ولا مبرمجا، حيث يقوم بفك رموز الشفرة الخاصة بنظام التحويل الالكتروني للأموال داخل البنوك ومن ثم يقوم بتحويل مبالغ مالية لحسابه الخاص[3].

من خلال ما تم استعراضه نلاحظ مدى ارتباط الاحتيال الالكتروني أو المعلوماتي بالتزوير الالكتروني خاصة عندما يتم تزوير بطاقات الدفع الالكتروني بعميل لدى بنك معين من أجل استغلالها في الحصول على السلع والخدمات، ويعتبر استخدام بيانات هذه البطاقة عبر شبكة الانترنت

---

[1]– من أمثلة هذه الوسيلة قيام شخص يدعى E.Royce يعمل في مؤسسة تجارية، بتعديل برنامج بشكل صار يقوم باقتطاعات بمبالغ زهيدة على فترات مختلفة من خلال الصفقات التي أبرمتها المؤسسة مع المنتخبين الموزعين / عن محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة، الأردن، 2005، ص 57 .

[2]– ومن أمثلة هذه الوسيلة قيا مبرمجين في بريطانيا سنة 1988 بتصميم برنامج محاسباتي يمكن مستخدميه من خلال استعمال شفرة خاصة أن يتلاعب في البيانات المتعلقة بقيمة الضريبة المضافة، ثم قاما بتوزيعه على 120 محل تجاري، وتم بيع الشفرة إلى 12 محل من بين 120 مقابل مبالغ ضخمة تجاوزت 1,000,00 جنيه استرليني، وبعد تقديمها للمحاكمة أدينا بتهمة التلاعب في البرامج، وحكم عليهما بالحبس مدة تسعة أشهر وبغرامة قدرها 34,000 جنيه استرليني Bainbridge David, ip cit , P 294

[3]– من أشهر الحالات بهذا الخصوص هي حالة الخبير في الكمبيوتر ستانلي ريفكين rafkin stanly سنة 1978 في بنك لوس أنجلس هو the Security pacifico banc حيث بعد ملاحظته لكيفية إجراء عمليات التحويل الالكتروني وكذا الشفرة المستخدمة لذلك بفضل تمتعه بحرية الحركة داخل البنك باعتباره خبيرا به، وعن طريق هاتف خارج البنك استطاع أن يتصل بشبكة المعلومات الخاصة بالبنك وتحويله لمبلغ عشر ملايين دولار أمريكي إلى بنك آخر في نيويورك ثم إلى بنك آخر في سويسرا، وعمل في تجارة الألماس، ولم يلق عليه القبض إلا بعد أن كشف عن ذلك علانية، حيث قدم للمحاكمة عام 1979 بمحكمة لوس أنجلس التي أدانته بعدة تهم منها التلاعب في نظام التحويل الالكتروني بغرض تحقيق ربح غير مشروع، وحكمت عليه بالسجن لمدة ثماني سنوات .

Voir : Norman (Adrian R.b), computer and the law criminal law journal, vol 15 , 1991 , P 152

احتيالا لأن المجرم استخدم صفة غير صحيحة بطرق احتيالية للحصول على قيمة مالية، كما يعد تخليق بيانات الدفع تزويرا، ويعتبر استخدام البطاقة المزورة من قبيل الطرق الاحتيالية .[1]

فالاحتيال هو الاستيلاء على شيء مملوك للغير بطرق احتيالية بقصد تملك ذلك الشيء، وهذه الطرق الاحتيالية في مضمونها هي تغيير للحقيقة لخداع المجني عليه للوصول إلى نتيجة وهي تسليم المال للجاني، وفي المجال المعلوماتي تتخذ هذه الطرق الاحتيالية أشكالا متعددة للاستيلاء على مال الغير، وقد تقترن بالتزوير .[2]

ويعد التلاعب في البرامج والبيانات والتغيير فيها بما يترتب عليه إيهام المجني عليه بصحتها مما يجعله يسلم بها أحد أساليب التحايل حيث يستخدم الحاسوب كوسيط لذلك .[3]

غير أنه ليس من السهل في الكثير من الأحيان تحديد الوصف القانوني المناسب لهذه الأفعال، كما هو الحال في جرائم الاحتيال المصرفية، حيث يتم الاستيلاء على الأموال من حسابات العملاء، فهو من ناحية إجراء تغيير وتلاعب في البيانات لإيهام صاحب الحساب بصحتها مما يجعله يسلم بها، ومن جهة ثانية إجراء تزوير في البنود المتعلقة بالحسابات وهو من جهة ثالثة استيلاء على أموال الغير دون رضاه، وهو من جهة رابعة إساءة أمانة إذا حصل من قبل الشخص المكلف بحكم وظيفته بالمحافظة على هذا الأموال.[4]

الفرع الرابع: الفرق بين جريمة التزوير الالكتروني وجريمة التلاعب في بيانات نظام معالجة البيانات

مع زيادة التعامل بالحاسبات الآلية في العديد من المجالات، ظهرت الحاجة إلى إضافة نوع من الحماية الجنائية لنظام الحاسب الآلي وبرامج تشغيله، وهذا بالنظر إلى ما تحتويه من معلومات وبيانات مخزنة في هذه الأنظمة وارتباطها بمصالح حيوية للأفراد والمؤسسات.

[1]– محمد أمين الشوابكة، المرجع السابق، ص 202 .
[2]– براهمي حنان، المرجع السابق، ص 198 .
[3]– محمد أمين الشوابكة، المرجع السابق، ص 185 .
[4]– براهمي حنان، المرجع السابق، ص 198 .

ولأن للمجرم الالكتروني أهداف وأعراض مختلفة من اعتدائه على الحاسب، فقد ظهرت أشكال من الجرائم لم يكن لها وجود من قبل كجرائم اختراق نظام المعالجة الآلية للمعطيات ما تعرف بجرائم التلاعب في نظام المعالجة الآلية للمعطيات. ويعتبر نظام المعالجة الآلية للمعطيات الشرط الأولي للبحث في توافر أو عدم توافر أي جريمة من جرائم الاعتداء على نظام المعالجة فإذا تخلف هذا الشرط لا يكون هناك مجال للبحث في مدى توافر أركان أي جريمة من الجرائم الماسة لنظام المعالجة الآلي للمعطيات.

وقد سعى المشرع الجزائري من خلال تعديل قانون العقوبات إضافة قسم سابع مكرر من الباب الثاني من الكتاب الثالث عنوانه "المساس بأنظمة المعالجة الآلي للمعطيات " مكرر إلى 394 مكرر7، وأرسى هذا القسم وضع حماية فعالة لأنظمة المعالجة الآلية للمعطيات.

وهذه الجرائم تفترض وجود نظام للمعالجة الآلية " وهو كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام المعالجة الفنية ". [1]

أما النظام المعلوماتي فيعرف بأنه مجموعة من الأجزاء المترابطة التي تتفاعل مع البيئة ومع بعضها البعض لتحقيق هدف ما عن طريق قبول المدخلات وإنتاج المخرجات من خلال إجراء تحويلي منظم .[2]

ولقد أولت مختلف التشريعات العقابية جريمة التلاعب غير المشروع بالمعطيات أهمية كبيرة حيث تعتبر هي بداية لجرائم أخرى، بمعنى أن الجرائم الأخرى ما هي إلا نتائج تترتب عليها .

وتعتبر جريمة التلاعب في بيانات نظم المعطيات هي ثاني جريمة ينص عليها المشرع الجزائري بعد جريمة الدخول أو البقاء غير المشروع هذا في المادة 394 مكرر 1 وتقابلها المادة 323 فقرة 3 من قانون العقوبات الفرنسي، وأيضا المادة 4 فقرة 1 من الاتفاقية الأوروبية المنظمة في بودابست بتاريخ 2001/11/23 حول جرائم الفضاء المعلوماتي .

[1]– علي عبد القادر القهوجي، المرجع السابق، ص 43.

[2]– عبد الفتاح بيومي حجازي، جرائم الكمبيوتر في التشريعات العربية، المرجع السابق، 2009، ص 9.

وقد نصت المادة 394 مكرر 1 من قانون العقوبات الجزائري على أنه :" يعاقب بالحبس من 6 أشهر إلى ثلاث سنوات وبغرامة من 500,00 دج إلى4,000,000 دج كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها ".

ويتجسد النشاط الإجرامي في جريمة التلاعب في بيانات نظم المعلومات في إحدى الصور الثلاث هي الإدخال والمحو (الإزالة) والتعديل ولا يشترط اجتماعها، بل يكفي أن يصدر الجاني هذه الأفعال حتى يقوم الركن المادي مع عدم وجود التصريح بذلك وهذا يما يدل عنه مصطلح بطريق الغش ".[1]

ولذلك فإن السلوك الإجرامي في هذه الجريمة موضوعه محدد، وهو الاعتداء على المعطيات، فالجريمة في هذا الغرض تقع على المعطيات أي البيانات التي تمت معالجتها، دون المعلومة ذاتها، ولذلك يخرج من نطاق هذه الجريمة البيانات التي لم تعالج بعد، ولم تدخل إلى نظام معالجة البيانات، كذلك البيانات التي أدخلت إلى النظام، لكن لم تبدأ بعد أي خطورة في معالجتها وكذلك المعلومات التي انفصلت عن النظام وسجلت على شريط ممغنط أو قرص مبرمج أو القرص الضوئي، وهو ما يطلق عليه F.M وذلك لأنها أصحبت خارج النظام، النص يحمي المعلومات المعالجة داخل النظام أو ذلك التي في طريقها للمعالجة، بل اتخذت خطوة أكثر في مراحل معالجتها.[2]

ويتم السلوك الإجرامي في هذه الجريمة عن طريق فعل الإدخال والذي يتحقق بإضافة معطيات جديدة على الدعامة الخاصة به، وقد يتم إدخال هذه البيانات بقصد التشويش على صحة البيانات القائمة، ولعل اصطناع المعلومات وإدخالها إلى النظام هو أكثر الأمور سهولة وخصوصا في أول مراحل التشغيل وهي مرحلة إدخال المعطيات لمعالجتها .[3]

أما المحو فيقصد به إزالة جزء من المعطيات المسجلة في الحاسب الآلي أو إضافة جزء من المعطيات إلى المنطقة الخاصة بالذاكرة [4]، في حين يقصد بالتعديل تغيير المعطيات الموجودة داخل

---

[1]– غنية باطلي، الجريمة الالكترونية، دون طبعة،الدار الجديدة،الجزائر،2015، ص 173 .

[2]– عبد الفتاح بيومي حجازي، جرائم الكمبيوتر في التشريعات العربية، المرجع السابق، ص 38.

[3]– علي عبد القادر القهوجي، المرجع السابق، ص 59.

[4]– عبد الفتاح بيومي حجازي، جرائم الكمبيوتر في التشريعات العربية، المرجع السابق، ص 40.

النظام واستبدالها بمعطيات أخرى، أو هو تغيير غير مشروع للمعطيات والبرامج يتم عن طريق استخدام إحدى وظائف الحاسب الآلي .[1]

وهذه الأفعال الثلاثة المتمثلة في الإدخال والإزالة والتعديل التي وردت على سبيل الحصر فلا يقع تحت طائلة التجريم أي فعل آخر ولو أدى إلى الاعتداء على المعطيات داخل النظام، كنسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب بينها، إلا أن هذه الأفعال لا تنطوي على إدخال أو إزالة أو تعديل.

و تثير جريمة التلاعب غير المصرح به في نظام معالجة البيانات، إشكالا بخصوص الركن المادي لها، فهل يكفي إدخال البيانات عن طريق الغش بقيام هذه الجريمة أم أن يترتب على هذا الإدخال إفساد البيانات التي يحتويها النظام أو طريقة تحليلها أو تحويلها ؟ وأجابت على هذا السؤال محكمة استئناف باريس في حكمها الصادر في 1990/11/28، واعتبرت أن مجرد إدخال المعطيات بصفة غير مشروعة يشكل جريمة وفقا لنص المادة 323/ 3 من قانون العقوبات الفرنسي .[2] وتشترك جريمة التلاعب في نظام المعالجة الآلي للبيانات مع جريمة التزوير الإلكتروني في أن هذه الأخيرة هي أيضا من الجرائم الالكترونية التي يمكن أن ترتكب أثناء معالجة وتحليل البيانات لتخرج في النهاية بشكل مزور، أو تنصب مباشرة على مخرجات الحاسب الآلي، أي البيانات الخارجة منه والمثبتة على دعامة مكتوبة والتي يتم إنتاجها عن طريق الطابعات الملحقة بالحاسب أو على دعامة الكترونية كالأشرطة الممغنطة والأقراص المغناطيسية، والمصغرات الفيلمية وغيرها من الدعامات الالكترونية .

ومن أوجه التشابه والارتباط بين جريمة التلاعب في نظام المعالجة الآليات وللبيانات وجريمة التزوير الالكتروني، أن جريمة التلاعب بسلوكها الإجرامي مع إدخال أو محو أو تعديل هي بداية لجرائم أخرى من بينها جريمة التزوير الالكتروني، بمعنى أن هذه الأخيرة ما هي إلا نتيجة مترتبة عن جريمة التلاعب غير المشروع .

---

[1]– غنية باطلي، المرجع السابق، ص 176 .

[2]– / عماد بوخرص وحسني غديرة، جرائم الإعلامية في القانون المقارن، الملتقى الجهوي لجرائم الإعلامية، المعهد الأعلى للقضاة، تونس، 2001، ص 177 .

وعليه فهناك تشابه بين جريمة التلاعب غير المصرح به في المعطيات نظام المعالجة الآلي للمعطيات وبين جريمة التزوير الالكتروني من حيث أن محل الاعتداء فيهما ينصب على البيانات التي يتضمنها المحرر أو النظام، كما الاعتداء في ذاته، يتشابه في الجريمتين لغويا فالتلاعب بالإدخال أو المحو أو التعديل هو تغيير في الحقيقة .

أما أوجه الاختلاف بين الجريمتين يكمن في أن المعطيات محل الاعتداء في جريمة التلاعب هي جزء من النظام، أما المعلومات محل الاعتداء في جريمة التزوير هي مخرجات أو منتجات النظام أي منفصلة عنه.[1]

كما تختلف جريمة التلاعب في نظام المعالجة الآلية للبيانات عن جريمة التزوير الالكتروني من حيث الأثر المترتب عنها، فالأثر المترتب عن جريمة التلاعب هو إتلاف النظام وعدم قدرته على القيام بعمله، ومثال على ذلك محو بعض أوامر التشغيل الذي يترتب عليه تعطيل النظام، أما التزوير فلا يتلف المحرر وإنما يبقيه على حاله، والشيء المتغير فيه هو الحقيقة أو إحلال الباطل محل الحق.[2]

ومن أوجه الاختلاف أيضا بين الجريمتين الضرر المترتب عن هذه الجرائم، فجريمة التزوير الالكتروني تتسبب في إحداث ضرر للغير مما يجعل من الجريمة جريمة مادية ذات نتيجة في أن جريمة التلاعب تتحقق بمجرد الإدخال أو المحو أو التعديل ولو لم يترتب عليه أي ضرر، مما يجعل يجعلها جريمة شكلية .[3]

كما تختلف الجريمتان من حيث القصد الجنائي من ورائها، فيهدف الجاني من وراء جريمة التلاعب في نظام المعالجة الآلية للبيانات إلى الإضرار بالمعلومات والنظام دون أن يكون قصد الجاني متجها إلى استغلال أو استخدام تلك المعلومات في شيء ما، بعكس التزوير الذي يكون القصد من وراءه استعمال المحرر المزور فيما زور من أجله، بمعنى الاستفادة منه، لأن تلك المعلومات في المحرر لها قيمة قانونية في الإثبات أي أنها تثبت حقا أو واقعة لها آثارا قانونية، بينما المعطيات في

[1]– الهام بن خليفة، المرجع السابق، ص 69.

[2]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 132.

[3]– أشرف توفيق شمس الدين، المرجع السابق، ص 544.

النظام ليست لها قيمة في إثبات المراكز القانونية، إنما هي عنصر من النظام بالترابط تعمل بالترابط المعنوي مع العناصر المادية الأخرى لتكون هذا النظام .[1]

إضافة إلى ما سبق تختلف الجريمتان من حيث الهدف من تجريمهما، فإذا كان الهدف من تجريم جريمة التلاعب هو حماية النظام أو بمعنى أدق حماية الحق في هذا النظام، أو من له سيطرة عليه، فإن المصلحة من تجريم التزوير هي حماية الثقة العامة في المحررات باعتبارها من وسائل التعامل المدني والتجاري لإثبات الحقوق والالتزامات .

[1]– الهام بن خليفة، المرجع السابق، ص 70.

الفصل الثاني

القواعد الموضوعية لمكافحة جريمة التزوير الإلكتروني

الفصل الثاني: القواعد الموضوعية لمكافحة جريمة التزوير الإلكتروني

احتلت اليوم الدعامات المادية للحاسب الآلي مكانة للمحررات والصكوك، ونظرا لأهمية وخطورة ما تحتويه من بيانات فقد تكون محلا للاعتداء بتغيير حقيقتها بقصد الغش في مضمونها ومن شأنها إحداث أضرار مادية أو معنوية، فقد أصبح التزوير في مجال نظم المعلومات بوصفه أحد أنماط الغش المعلوماتي يشهد تزايدا سريعاً في الآونة الأخيرة؛ كتزوير المستخرجات الإلكترونية وإفشاء أسرارها وتزوير المعلومات المخزنة بداخل الأنظمة المعلوماتية، والضمانة الأبرز لحماية هذه المعلومات هي التشريعات، وذلك بتجريم كل غش يقع عليها وتوقيع العقوبة على كل من يرتكبه مسببا به ضرراً للغير، خاصة وأن اِرتكاب جريمة التزوير الإلكتروني سيكون لها ودون أي شك اِنعكاس سلبي على الثقة التي يوليها الأفراد للنظام المعلوماتي وما يحتويه من معلومات وما يتم استخراجه منه، وهو ما يكفل للأفراد والدولة المعتمدين على التعامل بها، الطمأنينة واستقرار المعلومات.

وعليه سنحاول من خلال هذا الفصل دراسة القواعد أو الأحكام الموضوعية لمكافحة جريمة التزوير الإلكتروني،وهذا من خلال مسألتي التجريم والعقاب وما تتطلبه الأولى من تحديد لأركان هذه الجريمة، وكذا أنواع جرائم التزوير الإلكتروني وصولاً إلى الجزاء المترتب عن هذه الجريمة في المسألة الثانية.

وبناء على ذلك سوف تقسم الدراسة إلى مبحثين نخصص الأول لدراسة القواعد الموضوعية لمكافحة جريمة التزوير الإلكتروني على مستوى التجريم، في حين نخصص المبحث الثاني إلى دراسة القواعد الموضوعية لمكافحة جريمة التزوير الالكتروني على مستوى العقاب.

المبحث الأول: القواعد الموضوعية لمكافحة جريمة التزوير الالكتروني على مستوى التجريم

لقد سمحت التكنولوجيا الحديثة بظهور وسائل وأساليب الإلكترونية تقوم في كثير من الأحيان بأداء وظائف الوسائل التقليدية مثل المحررات الالكترونية، ولما كانت هذه الوسائل الحديثة تتيح إنجاز المعاملات بين الأفراد والمؤسسات فإن استعمالها لا يخلو من المخاطر التي تقع عليها كالقيام بتزويرها، لذا حرصت معظم التشريعات على توفير الحماية القانونية لهذه المحررات، وذلك إما بتعديل النصوص العقابية القائمة أو استحداث نصوص جديدة تتلاءم وطبيعتها.

لذا حرص المشرع الجزائي في دول العالم المختلفة على تجريم التزوير الالكتروني إيمانا منه بأن التزوير في المحررات يهدد الثقة العامة للأفراد وبالتالي يخل باليقين والاستقرار في المعاملات.

وسنحاول من خلال هذا المبحث دراسة القواعد الموضوعية لمكافحة جريمة التزوير الالكتروني على مستوى التجريم، وهذا ببيان الأركان العامة التي تبنى عليها هذه الجريمة من جهة وهذا في المطلب الأول، والتطرق لأنواع التزوير الالكتروني من جهة أخرى وهذا في المطلب الثاني.

المطلب الأول: أركان جريمة التزوير الالكتروني

لقيام جريمة التزوير الالكتروني كغيرها من الجرائم لابد من توافر ركنيين أساسيين هما الركن المادي والركن المعنوي كما هو الحال في جريمة التزوير التقليدية، غير أن الركن المادي لهذه الجريمة يقوم بأفعال مختلفة عن التزوير التقليدي، كما أن هذه الأفعال قد تتشابك مع السلوك الإجرامي لجرائم الإلكترونية أخرى، أو قد تكون مقدمة لارتكاب فعل التزوير، ولذلك لابد من تحديد عناصر الركن المادي لهذه الجريمة بدقة، على اعتبار أن هذه الجريمة تقع في بيئة افتراضية غير ملموسة وهو ما يجعل أشكال وطرق التزوير مختلفة عن جريمة التزوير في شكلها التقليدي.

وإنطلاقا من مبدأ الشرعية إذ لا جريمة ولا عقوبة إلا بنص، وهذا ما يعني أن التزوير إن لم يكون مجرماً بنص قانوني فإن ذلك يعني إفلات المجرم أو المزور الإلكتروني من العقاب.

أما الركن المعنوي فيتخذ إما صورة القصد الجنائي وهو قصد عام يضاف إليه قصد خاص، وسنحاول التطرق إلى هذه الأركان في الفروع الآتية على النحو التالي:

الفرع الأول: الركن المادي

إن الركن المادي في جريمة التزوير الإلكتروني مضمونه تغيير الحقيقة في محور بإحدى الطرق التي حددها القانون تغيير من شأه أن يحدث ضرر للغير.فالركن المادي في جريمة التزوير يعني وقوع نشاط إجرامي من شأنه تغيير الحقيقة في محرر بطريقة، مما نص عليه القانون وأن يكون من شأن هذا التغيير إلحاق الضرر بالغير أو إحتمال حدوثه.

أولاً: عناصر الركن المادي:

ويمكن تقسيم هذه العناصر إلى ثلاثة، أولها تغيير الحقيقة، وثانيهما وجود محرر، أما العنصر الثالث هو الضرر الناتج عن هذا التعبير في الحقيقة، وهذا ما سنوضحه فيما يلي:

أ- تغيير الحقيقة

سبقت الإشارة إلى أن الركن المادي في جريمة التزوير الالكتروني هو تغيير الحقيقة في محرر، ويشترط أن يكون تغيير الحقيقة بإحدى الطرق المنصوص عليها قانوناً.

ويقصد بالحقيقة واقعة معينة لا يختلف عليها الأشخاص، هذا إذا ما تعلقت الحقيقة بمحرر رسمي، أما إذا تعلقت بمحرر عرفي فيقصد بها ما اتفق عليه الطرفان، أو إنشاء حقيقة مخالفة أو تحريف حقيقة قائمة، وأن يكون من شأن هذا التغيير أن تمس بالمركز القانوني للغير.[1]و تغيير الحقيقة يعني إبدالها بما يخالفها، وإذا انتفى هذا التغيير انتفى التزوير حتى لو توهم الجاني أنه يغير الحقيقة فلا يعد مرتكباً لجريمة التزوير.[2]

والمقصود بتغيير الحقيقة القانونية النسبية وليس تغيير الحقيقة الواقعية المطلقة،[*] وتغيير الحقيقة الذي تتطلبه جريمة التزوير أن يكون هناك مساساً بحقوق الغير أو مراكزهم القانونية الثابتة في تلك المحررات،[3] ويكون التغيير كليا أو جزئيا فلا يشترط أن تكون كل بيانات المحرر مخالفة للحقيقة، فينبغي أن تكون إحداهما أو بعضهما مكذوباً ولو كان الآخر صحيحاً.[4]

وتغيير الحقيقة قد يقع بفعل إيحائي وذلك بالإضافة أو الحذف أو التعديل وذلك بالقيام بأفعال مادية مشابهة عن طريق الإدخال والمحو والتعديل، فالإدخال يكون بإضافة معطيات جديدة، أما المحو فيتمثل في إزالة جزء من المعطيات المخزنة داخل النظام بينما يعتبر التعديل تغيير للمعطيات

---

[1]- هلالي عبد الله، شرح قانون العقوبات البحريني-القسم الخاص، الطبعة الأولى، منشورات جامعة البحرين، 2007 ،ص153.

[2]- فتوح الشاذلي، عفيفي كامل عفيفي، المرجع السابق، ص236.

(*)- يرى الفقه في هذا المجال ضرورة التمييز بين نوعين من الحقيقة، الحقيقة المطلقة أو الحقيقة المطابقة للواقع، وهي الحقيقة الواقعية وهي ليست مشمولة بالحماية القانونية وبين الحقيقة الظاهرة وهي الحقيقة المطابقة لما كان يتعين إثباته في المحرر وفقا للقانون وهي الحقيقة المقصود بالحماية، أي الحقيقة القانونية النسبية بمعنى الحقيقة الظاهرة التي أراد أن يثبتها صاحب الشأن في المحرر وفقا للقانون/للمزيد أنظر: محمود نجيب حسيني،جرائم الاعتداء على الأموال ،المرجع السابق، ص219.

[3]- نفس المرجع والصفحة.

[4]- فتوح الشاذلي، عفيفي كامل عفيفي، المرجع السابق، ص236.

الموجودة داخل النظام واستبدالها بمعطيات أخرى،[1] كما يتم التغيير بحذف كلمة أو رقم معين أو بالإضافة أو تعديله، سواء كانت لها معنى مفهوم مدرك للإنسان أو غير مدركة مباشرة مثل تغيير الأمر بالدفع الموجه من بنك لآخر وتزوير الرسالة (الوثيقة) يتم الدفع لحساب المجرم، أو تغيير أرقام موظفين محفوظة داخل النظام والتي لها دلالة مالية، كما يحدث التزوير عن الطريق تغيير أمر التحويل المصرفي، خاصة عندما يعتبر التحويل الالكتروني للأموال وسيلة قانونية لإجراء المعاملات المصرفية بالنص على ذلك تشريعاً.[2]

ويمكن تصور تغيير الحقيقة في النظام الآلي للمعالجة المعلوماتية بتغيير البيانات أو حذفها أو إضافتها أو التلاعب فيها بأي صورة سواء كانت هذه البيانات مخزنة في ذاكرة الآلة أم كانت تمثل جزء من برنامج التشغيل أو برنامج التطبيق.[3]

ب- وجود المحرر:

يعد المحرر الالكتروني أسلوب أو وسيلة حديثة تقوم بأداء وظائف المحررات الورقية، فيما يتعلق بإثبات المعاملات، إلا أنها تختلف عنها في الاستخدام والبيئة التي تنتشر فيها، وتعد من أحدث طرق الإثبات التي ظهرت مع الاستخدام الواسع لتكنولوجيا المعلومات والاتصالات. ولقد اختلفت التشريعات الجنائية بشأن تسمية المحرر، وأطلقت عليه مصطلحات مختلفة؛ مثل: المستند الالكتروني، الكتابة الالكترونية، الوثيقة الالكترونية، المحرر الالكتروني، وعلى الرغم من هذا الاختلاف إلا أنها تحمل معنى واحد.

---

[1]- عبد الرحمن عبد الله حميد آل علي، جرائم التزوير المعلوماتي، الطبعة الأولى، دون ذكر دار النشر،دون مكان،2009، ص96.

[2]- أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، مصر، 2006، ص467.

[3]- يجب التفرقة بين التلاعب في البيانات والبرامج، فالتلاعب في البيانات قد يكون يقصد الإتلاف أو يقصد الاصطناع أو التزوير وهو الأقل احتمالا، فالبرامج تمكن أن يتصور فيها الاصطناع ولا يعد ذلك تزويراً للمحرر بطريق الاصطناع ،وإنما تعتبر تقليد المصنف وفقا لقانون حماية حق المؤلف، انظر في ذلك: فتوح الشاذلي، عفيفي كامل عفيفي، المرجع السابق، ص239.

1-تعريف المحرر:

تغيير الحقيقة موضوع جريمة التزوير هو الذي يكون محله محررا، والمحرر في مضمونه كتابة مركبة من حروف أو علامات تدل على معنى أو فكرة معينة، وإمكانية القراءة البصرية لمحتواه وهو ما تفترضه نصوص التزوير التقليدية في أكثر الدول وكذلك الفقه والقضاء[1].

ويراد بالمحرر كل مسطور يحوي علامات أو كلمات ينتقل بها الفكر أو المعنى من شخص إلى آخر بمجرد النظر إليها[2]. كما يعرف المحرر بأنه مكتوب يفصح عن شخص من صدر عنه ويتضمن ذكراً لواقعة أو تعبيراً عن إرادة، ويكون من شأنه إنشاء مركز قانوني معين أو تعديله أو إنهاؤه أو إثباته.[3]

وقد عرف قانون الأونسترال النموذجي للتجارة الالكترونية المحرر الالكتروني في المادة 02 فقرة 01 كما يلي:"يراد برسالة البيانات المعلومات التي يتم انتشاؤها أو إرسالها أو اِستلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الالكترونية، أو البريد الالكتروني أو البرق أو التلكس أو النسخ البرقي".[4]

---

[1]- هشام محمد فريد رستم، المرجع السابق، ص326 وما بعدها.

(*)-عباس العبودي، تحديات الإثبات بالمستندات الإلكترونية، الطبعة الأولى، منشورات الحلبي الحقوقية لبنان، 2011، ص33.

[2]- فتوح الشاذلي، عفيفي كامل عفيفي، المرجع السابق، ص241.

[3]- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، المرجع السابق، ص44.

[4]- وهو ذات التعريف الوارد في المادة 02 نموذج من قانون الأونسترال النموذجي شأن التوقيعات الالكتروني لسنة 2001.

(*)- لابد من التفرقة بين مستند أو محرر معلومات والذي يعرف بأنه:" محرر معد الإثبات، أو يصلح للإثبات طبقا لمبدأ الثبوت بالكتابة"، وكذلك للمصطلح مستند معلوماتي والذي يعرف بأنه:<<كل محرر تحتوي على معلومات معالجة آليا، فمستند المعلومات ينتج عن إصدار أمر من مشغل الجهاز إلى الطابعة وذلك من يطبع المعلومات التي تم معالجتها آليا داخل جهاز الكومبيوتر، حيث أن البيانات بإدخالها للجهاز تتم معالجتها وتتحول إلى معلومات مفيدة- ويشترط أن يظهر مستند المعلومات لحيز الوجود، وذلك أن يطبع على أوراق طبقا المفهوم المادة 462 فقرة 02 من القانون الفرنسي القديم، أما بالنسبة للمادة 444 فقرة 01 من القانون الجديد، فلا يتم يشترط أن يتم التزوير على المعلومات المعالجة آليا داخل جهاز الكومبيوتر والمسيحية على قرص صلب أو قرص صلب أو قرص مرن/عن محمد أمين الرومي، مرجع سابق، ص111.

وقد سايرت العديد من التشريعات التعريف الوارد في قانون اليونسترال النموذجي كقانون إمارة دبي الخاص بالمعاملات والتجارة الالكترونية، وقانون التوقيع الالكتروني وخدمات الشبكة السوري،وقانون المعاملات الالكترونية البحريني.[1]

فقد عرف المشرع المصري المحرر الالكتروني وهذا في المادة 01 من القانون الخاص بالتوقيع الالكتروني بأنه:"كل رسالة بيانات تنشا أو تدمج أو تخزن أو ترسل تستقبل كليا أو جزئيا بوسيلة الكترونية أو ضوئية أو بأي وسيلة أخرى مشابهة".[2]

أما المشرع الجزائري فقد ساير أيضا التطور الحاصل في الإثبات بالكتابة الالكترونية لكن بطريقة ضمنية وهذا من خلال تعريفه للإثبات بالكتابة، حيث أقر في المادة 323 مكرر 1 من القانون المدني بأنه :"ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام وأية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها وكذا طرق إرساله". فالمشرع هنا اعتبر الكتابة تحمل على أي وسيلة سواء ورقية كانت أو الكترونية ترسل بأي وسيلة كانت يدوية أو الكترونية". [3]

2-خصائص المحرر:

يتميز المحرر الالكتروني بجملة من الخصائص والمزايا ساهمت في الانتشار الواسع له سواء بين الأفراد فيما بينهم في إثبات تعاملاتهم المدنية والتجارية، أو بين الدول في إطار ما يسمى بالحكومة الالكترونية من خلال تبادل الصفقات بينها وبين دول العالم.فالمحرر يجب أن يتخذ شكلا كتابيا وبأي لغة فقد تكون لغة محلية أو أجنبية، ويجب أن تكون الكتابة عبارة عن حروف، والراجح أن

---

[1]- نصت على ذلك المادة 02 فقرة 08 من القانون الخاص بالمعاملات والتجارة الالكترونية لإمارة دبي،وكذا المادة01 فقرة 8 من قانون التوقيع الالكتروني وخدمات الشبكة السوري،والمادة 02 من قانون المعاملات الالكترونية البحريني.

[2]- تقابلها المادة 1316 من القانون المدني الفرنسي المعدلة بموجب قانون إثبات تكنولوجيا المعلومات المتعلق بالتوقيع الالكتروني المؤرخ في 13 مارس 2000.

Loi n" 2000-230 du 13 MARS 2000 portant adaptions du droit de la preuve aux technologie de l informatique et relative à la signature électrique, JORF N" 62 du Mars 2000,p 3968.

3- القانون 10/05 المؤرخ في 18 جمادى الأولى عام 1426هـ الموافق ل6 يونيو سنة 2005 المعدل والمتمم للقانون المدني ،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية المؤرخة في 19 جمادى الأولى 1426 هـ الموافق ل 26 يونيو 2005،ص 17.

تكون علامات اصطلاحية، ولا عبرة بالمادة التي سطرت عليها فقد تكون بالآلة الكاتبة أو مطبوعا كله أو بعضه .[1]

كما تتصف المحررات الالكترونية بالسرعة والائتمان في إبرام المعاملات وذلك في بيئة افتراضية بواسطة شبكة الانترنت، وهذا ما ساعد في انتشار المعاملات الالكترونية بسرعة فائقة.[2] فضلا عما يتميز به المحرر الالكتروني بالسرعة لا يمكن لأحد الإطلاع عليها إلا المرسل والمرسل إليه كونها مستخرجة من تقنيات متطورة ما يضمن الثقة في المحررات الإلكترونية.[3]

وتختلف الكتابة الالكترونية عن الكتابة اليدوية التقليدية من عدة نواحي، فالكتابة العادية ترتبط بكاتب المحرر وتعكس شخصيته وبالتالي يمكن إحالتها إلى خبير لمعرفة مدى صحة نسبتها إليه، أما الكتابة الإلكترونية فإنها لا تختلف في حروفها بحسب من قام بكتابتها .وإذا كانت الكتابة الالكترونية تتكومن من نبضات الكترونية من جهاز فإن الكتابة العادية تتكون من أحبار سائلة أو جافة، إضافة إلى هذا فإن الكتابة الالكترونية غير ثابتة وتحتاج إلى جهاز للإطلاع عليها وقراءتها، في حين الكتابة التقليدية تتميز بالثبات مع إمكانية الإطلاع عليها دون واسطة[4].

ويتضح مما سبق أن المحرر هو عماد جريمة التزوير ويعد شرطا أساسيا لتوافرها، فإذا لم يوجد المحرر لا يتحقق التزوير، إلا أنه لعلّ من أهم العقوبات التي واجهت تطبيق هذا النص الخاص بالتزوير في المحرر الالكتروني هي وجود المحرر،(*) وقد تباين موقف الفقه أو التشريع المقارن بخصوص كيفية التغلب عليها، أو بعبارة أخرى **هل يعتبر المحرر المعلوماتي من قبيل المحررات التقليدية التي يسرى عليها النص الجنائي الخاص بالتزوير؟ وما هو المحرر محل التزوير؟**

لقد ذهب البعض إلى أنه من الصعب الاعتراف بأن البيانات المبرمجة في الكومبيوتر من قبيل المحررات في مفهوم التزوير بسبب أن تلك البيانات لا يتوافر لها خاصية الثبات كما لا يتوافر فيها شرط القابلية للقراءة بشكل مستقل أي أننا نحتاج إلى جهاز –كومبيوتر– لقراءة ذلك المحرر، كما

---

[1]– محمد سامي شوا ،المرجع السابق،ص 155.

[2]– عباس العبودي،المرجع السابق،ص 40.

[3]– للمزيد انظر:الهام بن خليفة ،المرجع السابق،ص 21 وما يليها.

[4]– محمود إبراهيم غازي،الحماية الجنائية للخصوصية والتجارة الالكترونية،الطبعة الأولى،مكتبة الوفاء القانونية، مصر، 2014 ،ص507.

أن جريمة التزوير لا تقع إلا إذا توافرت نية استعمال المحرر فيما زور من أجله، وهذه النية لا تمكن أن تتواجد بالنسبة للبيانات التي لا تزال مبرمجة ذلك أنها غير محدد أصلا لتقديمها للتعامل[1].

إلا أن ذلك مردودً عليه بأن القانون يحمي الثقة التي يمكن يصنعها الناس في المحرر وليس في الكتابة ذاتها ولكن الكتابة تعتبر دليلاً في الإثبات، ومن ثم تمكن أن يقال هناك تقابلا بين نظرية التزوير ونظرية الإثبات، فالقانون لم ينص إلى على تغيير الحقيقة في محرر بطريق من الطرق التي حددها القانون وأن يكون من شأن ذلك إحداث الضرر أو احتماله.[2]

وإذا كان الفكر التقليدي في جريمة التزوير بشرط لكي تكون بصدد محرر يصلح محلاً لجريمة التزوير أن يتخذ شكل الكتابة ، لذلك فالمستندات الالكترونية لا تعتبر من قبيل المحررات الورقية، حيث أنها لا تتمتع بقوة الإثبات التي تتوافر في المحررات .[3]

بيد أن الفكر الحديث ومسايرة منه للتقدم العلمي قد تجاوز بمفهومه التقليدي للمستند الذي يعرفه على أنه ورقة مكتوبة وأصبح تماثل بين المستند الورقي والمستند الالكتروني.[4]

ولقد ظهر اتجاه قوي في دول مختلفة ينادي بالمساواة بين المستند الورقي والمستند الالكتروني مردداً أن سجلات الحاسب الآلي ومخرجاته وما يسجل في ذاكرته والأسطوانات الممغنطة تعتبر من قبيل المستندات.[5] وبالتالي فقد اتسع مفهوم المحرر يشمل ما تمكن أن نطلق عليه المحررات الالكترونية.

وقد تناول المشرع الفرنسي في قانون العقوبات 19 لسنة 1988 تجريم تزوير المستندات الالكترونية واستخراج المستندات المزورة والشروع فيها، والملاحظ أن المشرع إستخدم تعبير المستندات

---

[1]– شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، الطبعة الأولى، دار الجامح الجديدة، مصر، 2007، ص 82.

[2]– محمود إبراهيم غازي، المرجع سابق، ص508.

[3]– إبراهيم طنطاوي، المسؤولية الجنائية عن جرائم التزوير في المحررات، الطبعة الأولى، المكتبة القانونية، 1995، مصر،ص18.

[4]– هلالي عبد الله أحمد، تفتيش نظم الحاسب ونظم الحاسب وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية،مصر، 1997، ص214.

[5]– Kurtz (j) and pussztal (L),computer crimes and other crimes against information technologie in Hungary, 1994,p356.

المعالجة آليا اتفاقا مع وجهة النظر التكتيكية للغة الحاسب الآلي التي تعالج المحررات المعلوماتية فتصبح مستندات معالجة آليا

وقد اعتمد المشرع الفرنسي في القانون الجديد الذي بدأ العمل في مارس 1994 نصا جديداً هو المادة 441 فقرة 1 بأن شمل تغيير الحقيقة في محرر أو أي وعاء آخر لتتصرف على كافة أشكاله، كما توسع القانون الجديد في طرق التزوير فلم تعد محصورة على سبيل الحصر وإنما أطلقها المشرع.

أما بخصوص المشرع الجزائري وعلى الرغم من اِعترافه بالكتابة الإلكترونية كوسيلة لإثبات التصرفات القانونية مثلها مثل السندات العادية، وتوفيره لها الحماية الفنية أو التقنية من خلال قانون التوقيع والتصديق الإلكترونيين، غير أنه لم يعدل في نصوص التزوير كما فعله غيره من المشرعين.

ويرى البعض في هذا الصدد أن مصطلح المحرر المحمي بموجب قانون العقوبات الجزائري يبقى قابلا لأن يشمل الكتابة الرقمية على الدعامات الالكترونية وفقا للتحديد الوارد في القانون المدني، إذ تدخل المشرع أو تجرأ الاجتهاد القضائي ما دام أن النصوص المحلية لا تمنع من تفسير المصطلح وفقا لتطورات العصر حتى ولو لم يطرأ أي تعديل على النصوص لأن باب الاجتهاد كفيل لمعالجة الوضع في ظل النصوص الحالية.[1]

ج- الضرر:

لا يكفي لقيام جريمة التزوير قيام الركن المادي بتغيير الحقيقة في محرر و أن يتم ذلك التغيير بالطرق المنصوص عليها قانونياً، وإنما يجب أن يكون من شأن ذلك إحداث ضرر للغير، فحصول ضرر أو احتمال حصوله شرط للعقاب على جرائم التزوير وبالتالي فإن مجرد قراءة المعلومات على شاشة الحاسب الآلي لا يشكل ضرراً، لذلك يعد الضرر عنصراً جوهرياً لقيام الجريمة.و من عناصر الركن المادي في جريمة التزوير التقليدية، فلا تقوم جريمة التزوير بدون حصول الضرر، وهو كذلك عنصر من عناصر الركن المادي في جريمة التزوير الإلكتروني.

ونظرا لأهمية عنصر الضرر ضمن الركن المادي في جريمة التزوير، فإن جانباً من الفقه يرى أنه ركن مستقل في جريمة التزوير،[2] ويرى جانب آخر من الفقه أنه يفضل أن يكون الضرر عنصراً

[1]- جمال نجيمي، المرجع السابق، ص393.

[2]- محمود نجيب حسني، قانون العقوبات، القسم الخاص، المرجع السابق،ص 282.

من عناصر الركن المادي في جريمة التزوير لارتباطها بالمحرر المزور أو الوثيقة المعلوماتية المزورة.[1]

ويعرف عنصر الضرر في جريمة التزوير بأنه:" كل إخلال أو اِحتمال الإخلال بمصلحة يحميها القانون، ويستوي في ذلك الضرر الجسيم واليسير، والضرر الفعلي والمحتمل، والضرر المادي والضرر الأدنى والضرر الخاص والعام".[2]

وحسب تقسيمات الضرر المذكورة، فإن الضرر الفعلي هو الضرر الذي وقع بالفعل من جراء التزوير، أما الضرر المحتمل فهو الضرر المتوقع حصوله سواء كان سيصيب المجني عليه أو شخصاً آخر.

والمبدأ العام السائد لدى الفقه والمطبق في القضاء هو أن التزوير يعاقب عليه حتى ولو كان الضرر لم يتحقق في الواقع إطلاقا، ويكفي أنه ممكن أو محتمل الوقوع في وقت اِرتكاب الجريمة، إذ يستنتج من هذا المبدأ أن التزوير معاقب عليه مبدئياً حتى ولو لم يعقبه أي استعمال للمحرر المزور،[3] ذلك أن المشرع لم يعلق العقاب على جريمة التزوير على اِستعمال المحرر المزور، لأن الضرر الفعلي يتحقق على وجه يقيني باستعمال المحرر المزور فعلاً، وتنشأ حينئذ جريمة أخرى جديدة قائمة على وجه يقيني باستعمال المحرر المزور فعلاً، هي جريمة الاستعمال، ويكون الضرر محتملاً على قدر احتمال استعمال المحرر المزور مستقبلاً، فإن لم تستعمل تقوم جريمة التزوير على ضرر محتمل الوقوع.[4]

ومن تقسيمات الضرر، الضرر المادي والضرر الأدبي، فالضرر المادي هو كل إخلال بحق المضرور ذي قيمة مالية، أو مصلحة مشروعة له ذات قيمة مالية ويشمل في الحالتين الخسارة التي لحقت بالمضرور والكسب الذي فاته.[5] أما الضرر الأدبي هو ذلك الضرر الذي ينال بالأذى شرف

---

[1]– عبد الفتاح بيومي حجازي، جرائم الكومبيوتر والانترنت في التشريعات العربية، المرجع السابق، ص70.

[2]– فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص وفقا لأحدث التعديلات، الطبعة الثالثة، دار النهضة العربية، مصر، 2012، ص274.

[3]– نفس المرجع ، ص291.

[4]– رؤوف عبيد، المرجع السابق، ص105.

[5]– عايد رجا الخلايلة، المسؤولية التقصيرية الإلكترونية–المسؤولية، الناشة عن إساءة اِستخدام أجهزة الحاسوب والانترنت–دراسة مقارنة ، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2009، ص122.

المجني عليه أو اِعتباره أو كرامته أو سمعته أو مشاعره فهو ضرر لا يقوم بالمال، أي ينال من المكانة الاجتماعية للمجني عليه، وأي قدر من المساس بهذه المكانة يكفي لتحقيق التزوير، كمن يكتب رسالة قذف ويمضيها بإمضاء غيره قصد المساس باعتبار شخص آخر يرتكب جريمة تزوير، وفي معناه الواسع هو مجموع الاعتداءات التي لا يؤثر في الذمة المالية.[1]

وهناك الضرر العام والضرر الخاص، ويقصد بالضرر العام ذلك الضرر الاجتماعي الذي يصيب المجتمع في مصالحه وليست مصلحة فرد بعينه، هذا الضرر العام قد يكون ضرراً ماديا أو أدبياً.[2] ويعتبر ضرراً خاصاً ذلك الإخلال بمصلحة خاصة لشخص أو أشخاص معينين، أما الضرر العام فهو الإخلال بمصلحة من مصالح المجتمع ككل.[3]

ومهما كان نوع الضرر فإن قيامه لازم عن طبيعة التزوير في المحرر الرسمي لأن تغيير الحقيقة فيه بطريق الغش بالوسائل التي نص القانون، ينتج حتما حصول ضرر بالمصلحة العامة لما يترتب على العبث بالمحرر الرسمي من تقليل لقيمتها في نظر الجمهور لحسبانها ذات حجية.[4]

ولذلك فإن التزوير قائم حتى إذا تم تغيير الحقيقة في ورقة رسمية باطلة شكلا لاحتمال حصول الضرر للغير أو للمجتمع فالمحرر الباطل وإن جرده القانون من كل أثر له، فإنه قد تتعلق به ثقة ممن لا يتضح أمامهم ما يشوبه من عيوب ويصح أن ينخدع فيه كثير من الناس الذين يفوتهم ما فيه من نقص، وهذا وحده كاف لتوقيع حصول الضرر بالغير بسبب هذا المحرر.

وقد نصت التشريعات العقابية[5] في تعريفها للتزوير صراحة على أنه لا يقوم أو لا يتأسس إلا على فكرة وجود الضرر، إذ جاء في المادة 441 فقرة 1 من قانون العقوبات الفرنسي أن التزوير يتشكل أو يتأسس أو يبني عن كل تغيير بغش في الحقيقة الذي من شأنه أن يتسبب في الضرر، وهو

---

[1]–Philipe pierre, l'indemnisation du préjudice moral en droit française s.d(www.fondation centimental,org/préjuctice– moral étude–fr).

[2]– عبد الفتاح بيومي حجازي، جرائم الكومبيوتر والانترنت في التشريعات العربية، المرجع السابق، ص71.

[3]– براهمي حنان، المرجع السابق، ص220.

[4]– أحمد خليفة الملط، المرجع السابق، ص445.

[5]– من ذلك المادة 543 من قانون العقوبات اللبناني، والمادة 216 من قانون العقوبات الإماراتي.

ما أكده القضاء في كل من فرنسا وكذلك في مصر[1]، والجزائر،[2] على الرغم من عدم النص عليه صراحة في نصوص التزوير، وكل ما في الأمر أن هناك إشارة بسيطة له مثلا وردت في الفقرة الثانية من المادة 217 من قانون العقوبات الجزائري (...أن يترتب على اِستعمال المحرر أي ضرر الغير...).[3]

وعليه تجمع كافة التشريعات الجزائية وكذلك فقهاء القانون الجنائي ورجال القضاء الجنائي أيضا على أن الضرر في جريمة التزوير يعتبر عنصراً أساسياً من عناصر الركن المادي لقيام هذه الجريمة، بحيث تمكننا القول بأنه إذا انعدم الضرر انعدم وجود وقوع جريمة التزوير.

والقول بمدى توافر ركن الضرر أمر يعود تقديره لقاضي الموضوع حسب موضوع كل دعوى، ولهذا نجد أن القاضي الناظر في دعوى التزوير يجتهد أكثر ما يجتهد وهو بصدد إظهار الضرر الناتج عن دعوى التزوير على اعتبار أن وجود الضرر يؤدي بالضرورة إلى وجود جريمة التزوير شريطة توافر الأركان الأخرى بالطبع، أما انتقاء الضرر فيؤدي بالضرورة إلى انتقاء جريمة التزوير دون الحاجة للبحث عن توافر الأركان الأخرى لهذه الجريمة.[4]

ثانياً- طرق التزوير الالكتروني

إن مجرد تغيير الحقيقة في محرر لا يكفي لقيام جريمة التزوير وإنما يشترط القانون أن يتم بإحدى الطرق التي حصرها القانون، ويجب على القاضي أن يبين في حكمه الطريقة التي وقعت بها

---

[1]- يجب على المحكمة أن تبين توافر الضرر في الحكم الصادر بالإدانة فن أغفلت هذا البيان كان حكمها معيبا مشوباً بالقصور الذي يستوجب نقضه(، نقض 33 مايو سنة 1932 مجموعة القواعد القانونية ج2 رقم 355، ص570، أنظر في ذلك:د/ فوزية عبد الستار، الرجع السابق، ص290.

[2]- حيث أنه فيما يتعلق بانعدام الضرر فإن التزوير في الوثائق الإدارية يتضمن حتما وبقوة القانون وجود الضرر نظراً لما ينجم عنه من مساس بالثقة المفترضة في الوثائق الصادرة عن الإدارة العامة...)، قرار المحكمة العليا الصادر بتاريخ 2011/4/07 (غير منشور)، وأيضا:(...وأم عنصر الضرر فهو مشروط في المحررات العرفية والتجارية...)، قرار المحكمة العليا الصادر بتاريخ 2012/02/02 (غير منشور) للإطلاع أكثر أنظر في جمال نجيمي المرجع السابق ص.ص521-522.

[3]- إلهام بن خليفة، المرجع السابق، ص112.

[4]- عامر محمود الكسواني، التزوير المعلومات للعلامة التجارية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2010ن ص210.

الجريمة وإلا كان حكمة قاصراً يتعين نقصه،[1] ويرى جمهور الفقه أن جريمة التزوير من طائفة الجرائم ذات الوسائل المحددة أو المقيدة، وهي تلك التي يتطلب القانون فيها بالنص الصريح أن تقع بوسيلة محددة أو كيفية بذاتها، بحيث لا يكفي لقيم التزوير تغيير الحقيقة بل يجب أن يتم بإحدى الطرق المحصورة في القانون وعليه ذلك هو حرص المشرع على حصر الدائرة التي يعتبر تغيير الحقيقة فيها تزويراً معاقباً عليه، حتى لا يصير كل كذب مكتوب تزويراً.[2]

ولقد قسم فقهاء القانون الجنائي طرق التزوير إلى طرق التزوير المادي وطرق التزوير المعنوي وسنحاول بيان هذه الطرق كالتالي:

أ- التزوير المادي:

التزوير المادي هو ذلك التزوير الذي يتم بطريقة مادية تترك في المحرر أثر يمكن إدراكه بالحواس، فالتزوير المادي يتم غالباً بعد تدوين المحرر، ولذلك يقرر الفقه الإيطالي أن التزوير المادي هو تغيير في الحقيقة ينصب على مصدر المحرر ذاته، وذلك بأن ينسب المحرر إلى غيره منشئه، أو يتناول بالتعديل صلب المحرر بعد إنشائه من محرره الحقيقي.[3]

وكما سبق الإشارة إليه آنفا أن المشرع الفرنسي لم يتناول طرقا محددة يقع بها التزوير طبقا لنص المادة 441 من قانون العقوبات، بخلاف بعض القوانين الأخرى التي أوردت طرقا معينة للتزوير في صورته التقليدية كالقانون المصري في المواد 296، 289، 112، 714، 221 من قانون العقوبات والمواد من 214 إلى 229 من قانون العقوبات الجزائري، وهذه الطرق ذكرت على سبيل الحصر في جريمة التزوير التقليدية، بخلاف جريمة التزوير الإلكتروني التي أدت إلى ظهور أنماط لا تطالها نصوص قوانين العقوبات الحالية، وتتمثل طرق التزوير في: وضع توقيع مرور، حذف أو إضافة أو تعبير مضمون المحرر والاصطناع.

---

[1]- فتوح الشاذلي، عفيفي كامل عفيفي، المرجع السابق، ص250.

[2]- محمد زكي أبو عامر، شرح قانون العقوبات القسم الخاص، دون طبعة، دار الجامعة الجديدة، مصر، 2015، ص116.

[3]- سامي الشوا، المرجع السابق، ص170.

1- وضع توقيع مزور:

ويقع هذا بأن يوقع المزور على محرر بإمضاء أو ختم لغيره سواء كان شخصا حقيقيا موجوداً في عالم الحياة أو شخصاً خيالياً لا وجود له، وإذا كان موجوداً لا يشترط لوجود التزوير أن يكون الإمضاء مشابها لإمضاء ذلك الغير، فقد جعل التقليد طريقاً آخر من طرق التزوير،[1] فالقانون يكتفي بوضع إمضاءات وأختام مزورة، فمتى وقع المزور على محرر بإمضاء غير إمضائه يعتبر المحرر مزوراً بصرف النظر عن التقليد ويقع التزوير حتى ولو تعذر قراءة التوقيع.[2]

ويترتب على اعتبار الإمضاء مزوراً، أن وضع الإمضاء في المحرر لم يكن تعبيراً عن إرادة صحيحة لمن ينسب إليه المحرر، ومثال ذلك أن يوقع شخص على محرر باسم العائلة بعد أن يضيف إلى الاسم العائلي اِسم شخص آخر بهدف أن ينسب إليه هذا المحرر.[3]

أما عن إمكانية وقوع التزوير الالكتروني بهذه الطريقة فهو أمر وارد إذا ما تأملنا طبيعة وظيفة جهاز الحاسب الآلي وشبكة المعلوماتية التي ترتبط بها هذه الحواسيب سواء كانت نظم معلومات داخلية أو شبكة المعلومات العالمية انترنت، ذلك أن جهاز الحاسب الآلي، أيا كان الموقع وأيا كانت المنظمة الدارية التي يخدم فيها، يتلقى بيانات يغذي عليها نظام ألمعلوماتي وهي المدخلات التي تعكس العمليات والأنشطة داخل المنظمة الإدارية، وهذه المدخلات يقابلها ما يسمى بالمخرجات وهي المعلومات الناتجة عن النظام المعلوماتي للحاسب الآلي، وما بين عملية (الإدخال والإخراج) يقوم الحاسب الآلي بعملية تحليل البيانات ومعالجتها، للوصول إلى مخرجات الحاسب الآلي، إذ أن الحاسب الآلي يعتمد على المعلومة، وهذه المعلومات ذات قيمة في ترتيب حق معين أو أثر قانوني معين فمن السهل تزوير مخرجات الحاسب المتضمنة لهذه المعلومات.[4]

---

[1]- جميل عبد الباقي الصغير، شرح قانون العقوبات –القسم العام–دون طبعة، دار النهضة العربية، مصر،2000 ، ص170.

[2]- فتوح الشاذلي، عفيفي كامل عفيفي، المرجع السابق، ص250.

[3]- محمود نصيب حسيني، المرجع السابق، ص231.

[4]- عبد الفتاح بيومي حجازي، التزوير في جرائم الكومبيوتر والانترنت، المرجع السابق، ص.ص206،205.

ويرى جانب من الفقه بأنه لا يتصور أن التزوير في المحرر الالكتروني بوضع التوقيعات مزورة وأن أكثر ما يقع به هذا النوع الأخير من التزوير هو التزوير في البيانات قبل وأثناء معالجتها.[1]

في حين يذهب أي آخر إلى إمكانية تزوير المحرر الالكتروني عن طريق وضع التوقيع المزور حيث يتم تزوير البيانات في محرر الالكتروني، ثم الحصول على توقيع الشخص المراد إدخاله إلى جهاز الحاسب الآلي عن طريق أخذ صورة له بواسطة جهاز الماسح الضوئي المرتبط به، وبعد ذلك يضاف التوقيع المصور إلى المحرر، وهكذا يتحصل الجاني على محرر الكتروني صحيح من الناحية الشكلية، لكنه في الحقيقة مزوراً لأنه نسب إلى شخص بناءاً على توقيعه ولكن على غير إرادته،[2] وعليه يتم تزوير التوقيع بإدخال توقيع أو ختم أو بصمة عن طريق الماسح الضوئي إلى وثيقة مخزنة داخل الجهاز لتنسب إلى صاحب التوقيع، فمن السهل إدخال صورة توقيع هذه الجهة عن طريق جهاز الماسح الضوئي ليضاف للوثيقة المزورة.[3]

أما إذا كان التوقيع رقميا فإن التوقيع المزور يكون مطابقاً للتوقيع الأصلي، ولكن يتم من خلال سرقة منظومة التوقيع والتوقيع عليها، حيث يعتبر التوقيع سليماً إذا تمت مضاهاته ولكنه ليس صادر من مالك منظومة التوقيع الالكتروني.[4]

وهذه الطريقة تتشابه مع طريقة وضع إمضاء مزور في وثيقة ورقية، والذي يقصد به توقيع الشخص بإمضاء مزور في وثيقة، والذي يقصد به توقيع الشخص بإمضاء غير إمضائه وليس له حق التوقيع به، لكنها مختلفة من الناحية التقنية(*) حيث أصبح هذا الإمضاء عبارة عن منظومة رقمية.[5]

---

[1]– محمد علي العريان، الجرائم المعلوماتية، الطبعة الأولى، دار الجامعة الجديدة للنشر، مصر، 2004، ص142.

[2]– جمال نجيمي، المرجع السابق، ص477.

[3]– عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، المرجع السابق، ص184.

[4]– من تطبيقات هذه الطريقة سرقة منظومة التوقيع الالكتروني الخاصة بطاقات الائتمان والتوقيع عليها دون رضا مالكيها، حيث أن استخدام الرقم السري الخاص بالبطاقة عند استخدامها داخل جهاز السحب الآلي للنقود، إذا تم من شخص غير صاحب البطاقة يعتبر تزويراً للتوقيع، باعتبار أن النقر على مفاتيح الحاسب الآلي يعتبر توقيعا إلكترونياً من صاحب الحق في ذلك/ للمزيد أنظر: إيهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، الطبعة الأولى، دار الجامعة الجديدة، مصر، 2008، ص63.

[5]– ثم ضبط عمليات تزوير من هذا النوع، حيث تعرضت بنوك بدولة الإمارات العربية المتحدة لعملية قرصنة، من خلال قيام محترفين في المعلوماتية بإدخال جهاز في فتحات إدخال بطاقات السحب بأجهزة السحب الآلي، ليقوم هذا الجهاز بتسجيل بيانات جميع البطاقات، ونسخ الأرقام السرية الخاصة بالعملاء، ومن ثم استخدام هذه البيانات على

2- حذف أو إضافة أو تغيير مضمون المحرر:

يتعلق الأمر بأساليب التغيير المادي الذي يدخله الجاني على المحرر بعد إتمام تحريره، أما إذا حدث التغيير أثناء كتابة المحرر فالتزوير يكون معنوياً لا مادياً، وعلى هذا الأساس لا يعد تزوير إدخال المتهم على المحرر تغييراً لا يتغير به معناه، كما لو أضاف لفظ دينار بعد المبلغ أو الرقم المئوي أو الألفي لتاريخ التحرير، كما أنه لا أهمية للوسيلة التي استخدمها الجاني في تغيير مضمون المحررات، فقد يتم ذلك بطريق الإضافة أو الحذف أو التعديل في مضمون المحرر أو في الإمضاءات والأختام.[1]

أما فيما يخص المحرر الالكتروني فإن الجاني ومن خلال استعماله لجهاز الحاسب الآلي يقوم بمعالجة بيانات النص وتغيير بعض محتواه بالإضافة أو الحذف أو التعديل ثم إخراج النص في شكل محرر وتتشابه هذه الصورة من التزوير مع صورا الاعتداء على نظم المعالجة الآلية للمعطيات التي تتم بنفس الأفعال المادية.

ويحدث التغيير بالإضافة بزيادة كلمة إلى اِسم ورد في المحرر أو إلى الإمضاء أو بزيادة رقم لمبلغ مكتوب في المحرر أو في التاريخ أو بزيادة كلمات في مكان خال من المحرر، وأما التغيير بالحذف فيكون بحذف كلمة أو رقم أو سر أو عبارة وردت في المحرر،[2] أيا كانت الوسيلة التي استعملها المزور، سواء بالكشط أو المحو بمادة كيميائية أو جزء من المحرر بالحبر وخلافه.[3]

في حين أن التغيير بطريق التعديل هو الخليط ما بين طريقتي الحذف والإضافة كأن نستبدل كلمة بأخرى أو رقم برقم،[4] والتغيير المعاقب عليه في هذه الحالة هو التغيير الذي ثم على غير إرادة من حرر المستند أو المحرر، فلو تم بناء على اتفاق بين الموقعين دون المساس بحق الغير، فلا عقاب عليه، كذلك لا تقوم جريمة التزوير إذا لم يتم على التغيير حصول اختلاف في مضمون

بطاقات مزورة، واستعملا لهه البطاقات لسحب مبلغ مالية من أرصدة العملاء/ مقال منشور على الموقع الالكتروني: www.alitihad-ae/détails.plp?gy=2008 384 تاريخ الإطلاع على الموقع: 2017/03/17.

[1]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الثاني، ص420.

[2]- فوزية عبد الستار، المرجع السابق، ص261.

[3]- عبد الفتاح بيومي حجازي، التزويد في جرائم الكومبيوتر والانترنت، المرجع السابق، ص210.

[4]- نفس المرجع، ص211.

المحرر نفسه، إلا إذا تضمن ذلك مخالفة قواعد معينة نص عليها للقيام بتحرير المستند أو ما به من بيانات على نحو مخالف الحقيقة.[1]

وعن إمكانية وقوع التزوير المعلوماتي بهذه الطريقة، فهو أمر ممكن ذلك أن جهاز الحاسب الآلي حين يتلقى البيانات والمعلومات ضمن نطاقه المعلوماتي، فإنه يقوم بمعالجة هذه البيانات والمعلومات في ضوء طلبات وحاجات الجهة العامة أو الخاصة مستخدمة الحاسب الآلي، وذات العمل يقوم به الحاسب حتى ولو تلقى النص المكتوب من شبكة الانترنت، إذ يتم معالجة النص لمعرفة الحاسب الآلي، ثم يظهر بعد ذلك مادياً في صورة مخرجات لهذا الحاسب وخلال مرحلة المعالجة يمكن التغيير في النص المعالج بالإضافة أو الحذف أو التعديل على النحو السابق بيانه ومن ثم يتحقق التزوير الالكتروني بهذه الطريقة.[2]

كما قد يحدث التزوير عن طريق تغيير أمر التحويل المصرفي، خاصة عند ما يعتبر التحويل الالكتروني للأموال وسيلة قانونية لإجراء المعاملات المصرفية بالنص على ذلك تشريعا، ويتم التحويل المصرفي الالكتروني للأموال بوسائل الكترونية متعددة،[3] ويتم التحويل إما فيما بين المصارف أو بواسطة الوسائل التكنولوجية الحديثة في التحويل المالي وأهمها الصراف الآلي، ومراكز الخدمة الهاتفية والبنك الناطق، البطاقات الذكية، نقاط البيع، جهاز الحاسب الشخصي المرتبط بحاسوب المصرف، ويقع التزوير في أمر التحويل المصرفي الالكتروني إن لم يكن صادراً عن العميل، وذلك بحصول الجاني على بيانات العميل ورقمه السري، واستعمالها من طرفه لإجراء تحويلات الكترونية.[4]

---

[1]– فوزية عبد الستار، المرجع السابق، ص262.

[2]– عبد الفتاح بيومي حجازي، التزوير في جرائم الكومبيوتر والانترنت، مرجع سابق، ص211.

[3]– أحمد خليفة الملط، المرجع السابق، ص467.

(*)– من أمثلة ذلك قيام مشرف تشغيل الحاسب في أحد البنوك باستخدام برنامج ساعد لزيادة أرصدة حسابات العديد من أصدقائه، يتم سحب هذه الأموال من طرفهم ثم قام بتفريق إيصالات السحب، ولكن بحلول موعد المراجعة الدورية لحاسبات البنك، اكتشف المراجعون هذه العمليات لأنه تم تسجيلها بواسطة نظام أمن سري حيث كان يقوم بتسجيل كل العمليات على الحاسب الموجود في أحد فروع البنك ولم يكن المجرم على علم بهذا النظام الأمني/عن: حسن طاهر داود، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، 2000، ص246.

[4]– حازم نعيم الصمادي، المسؤولية في العمليات المصرفية الالكترونية، الطبعة الأولى، دار وائل، الأردن، بدون سنة نشر، ص62 وما بعدها.

ويرى بعض الفقهاء أن عملية التزوير في المحررات الالكترونية أبسط بكثير من التغيير في المحددات الورقية لأنه لا يحتاج إلى إزالة باستخدام الأدوات والمواد الكيمياوية لتغيير معاني الكلمات، ويحتاج فقط إلى إدخال كلمات أو تغيير معاني كلمات بالحذف أو بالإضافة أو التعديل عليها عن طريق الحاسب الآلي.[1]

3- الاصطناع:

يعرف الاصطناع بأنه خلق محرر بأكمله ونسبته إلى غير محرره،[2] ويتحقق الاصطناع بخلق محرر لم يكن له وجود من قبل ونسبته زوراً إلى غير محرره بشرط أن يكون المحرر المصطنع له مظهر قانوني، أي متضمنا لواقعة تترتب عليها آثار قانونية وصالحة لأن يحتج به في الإثبات.[3]وبهذه الطريقة يقوم الجاني بخلق وثيقة معلوماتية أو محرر الكتروني لم يكن موجوداً من قبل بمحتوى غير صحيح مثل اصطناع شهادة إدارية بالوفاة، أو شهادة إدارية لمؤهل علمي معين، أو شهادة بعدم الملكية أو غيرها.[4]

وكثيراً ما يقترن التزوير بالاصطناع بطريقة وضع إمضاء أو ختم مزور، والغالب أن يحدث الاصطناع في المحررات الرسمية، كمن يصطنع صورة حكم وينسب صدوره لمحكمة معينة أو كمن يصطنع شهادة ميلاد حررها بنفسه ووضع عليها إمضاءات مزورة باسم ضابط الحالة المدنية.[5]

ويقوم التزوير الواقع بطريق الاصطناع ولو كان مضمون المحرر مطابقا للحقيقة، إذ يكون التغيير متحققا بنسبة المحرر زوراً إلى سلطة لم يصدر المحرر عنها.

وللاصطناع صورتان إحداهما أن يخلق المتهم محرراً لم يكن موجوداً من قبل، أما الصورة الثانية فهي أن يخلق محرراً آخر وذلك بعد التعديل من شروط أو بدون تعديل منها.[6]

---

[1]- عبد الله بن سعود محمد السيبراني، المرجع السابق، ص56.

[2]- محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص،ص239.

[3]- عبد الله بن سعود محمد السيبراني، المرجع السابق، ص56/أنظر أيضا: عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، المرجع السابق، ص188.

[4] -Cour de cassation, chambre criminelle ; 22 octobre2003.

[5]- أحسن بوسقيعة، الوجيز في القانون، الجزائي الخاص، الجزء الثاني، المرجع السابق، ص420.

[6]- عبد الفتاح بيومي حجازي، التزوير في جرائم الكومبيوتر والانترنت، المرجع السابق، ص226.

وهناك فارق بين التقليد والاصطناع، ففي الاصطناع لا يهم الجاني مدى التشابه بين خطه وخط الغير عكس التقليد، وذلك لأنه يصنع محررا جديداً بكامله، بينما التقليد يعالج جزءاً من المحرر، وغالبا يوقع على المحرر المصطنع بتقليد مزور، كي يستمد قيمته القانونية من هذا التزوير، ولكن ليس هناك تلازم بين الطريقتين فكليهما طريقة مستقلة للتزوير.[1]فالتقليدُ في جريمة التزوير هو صناعة الشيء على مثال شيء آخر، وقد ينصب التقليد على المحرر بأكمله وقد يقتصر على عبارة أو كلمة أو إمضاء، فالتقليد لا يشترط أن يكون بنفس درجة إتقان المحرر الأصلي بل يكفي أن يكون تقليده على نحو من شأنه أن ينخدع به الغير حيث يوهمهم بأن المحرر هو الأصلي.[2]

وتزوير المحرر الالكتروني بطريقة الاصطناع هو أمر وارد، إذ يمكن للجاني أن يدخل ما يريد من معلومات أو بيانات إلى جهاز الحاسب الآلي بوصفها منسوبة إلى ذلك الشخص أو تلك الجهة، ولذلك فتزوير النقود الورقية بطريقة الحاسب الآلي تعد من طرق الاصطناع، كما هي من طرق التقليد، وذلك لأن الاصطناع هو خلق محرر بأكمله ونسبته إلى غيره.[3]

ب- التزوير المعنوي:

إن التزوير المعنوي يتحقق بتغيير حقيقة معنى المحرر ومضمونه دون المساس بمادته أو شكله لذلك فهو لا يترك أثرا يمكن إدراكه بالحواس، فإن كان التزوير المادي يتم غالباً بعد تدوين المحرر، فالتزوير المعنوي لا يقع إلا عند تدوين المحرر ابتداء، وممن يقوم بذلك التدوين.[4]

و يتحقق التزوير المعنوي بتغيير الحقيقة في محتوى المحرر، أي في جوهر وظروف التصرف بحيث لا يترك أي علامة ظاهرة تدل عله، لأن الكتابة لم تعدل ولم تغير أو تزيف، بل كتب على المحرر كتابة كاذبة منذ البداية، ويتضح من ذلك أن التغيير المعنوي يتم أساساً بالتعاصر مع كتابة المحرر أو أثناءه.[5]

---

[1]- محمود نجيب حسني، شرح قانون العقوبات-القسم الخاص- مرجع سابق، ص239.

[2]- هدى حامد قشقوش، الحماية الجنائية للتوقيع الالكتروني، بحث مقدم لمؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004، ص585.

[3]- عبد الفتاح بيومي حجازي، التزوير في جرائم الكومبيوتر والانترنت، مرجع سابق، ص.ص226، 227.

[4]- فوزية عبد الستار، المرجع السابق، ص258.

[5]- الهام بن خليفة، المرجع السابق، ص105.

فالاعتداء على المحرر لا يقع على المحرر، ولكن على مضمونه، حيث ما يذكر من بيانات فيها لا تتفق مع الحقيقة،[1] وهذا يعني أن تزوير المحرر بهذه الطريقة لا يتم إلا من طرف القائم على تحريرها أثناء انتشائها، ومن ثم لا يتصور ارتكاب التزوير بها في محرر رسمي من فرد عادي كما هو الحال في التزوير المادي، لأن المحرر الرسمي إنما يكتبه دائما موظف عمومي، ومن ثم ففاعل التزوير لا يمكن أن يكون إلا موظفاً.[2]

وبالرجوع إلى نصوص التزوير تجد أن طرق التزوير المعنوي والمحددة قانونا تتمثل في جعل اتفاقات أو أقوال غير التي صدرت من الأطراف، وجعل واقعة كاذبة في صورة واقعة صحيحة، إضافة إلى جعل واقعة غير معترف بها في صورة واقعة معترف بها أو وقعت في حضوره.

وأيا كانت طرق التزوير المعنوي، فهو تزوير يؤدي إلى تغيير في مضمون المحرر أو في ظروفه وملابساته لا في مادته أو شكله، لذلك فهو غالباً يق عند إنشاء المحرر، كذلك فإنه لا يترك أثراً ظاهراً ينجم عنه ويمكن للحس إدراكه، وكذلك فهناك صعوبة في إثباته على عكس التزوير المادي الذي يثبت من فحص المحرر نفسه، أما التزوير المعنوي فهو يثبت من أمور أخرى تتيسر أحيانا وتتعذر في أخرى.[3]

والسؤال الذي يطرح هنا هو:**ما مدى إمكانية تصور وقوع التزوير الالكتروني بإحدى طرق التزوير المعنوي؟.**

قبل الإجابة عن هذا التساؤل نبين أولا طرق التزوير المعنوي والمتمثلة في :

1- تدوين اتفاقات أو أقوال غير التي صدرت أو أمليت من الأطراف:

يتحقق التزوير بهذه الطريقة عندما يكلف الجاني بكتابة المحرر وفقا للبيانات والشروط التي طلب صاحب الشأن إثباتها بالمحرر، فيكتب بيانات أو شروطاً أخرى مغايرة لما طلبه.[4]ويمكن أن

[1]- عبد الفتاح بيومي حجازي، التزوير في جرائم الكومبيوتر والانترنت، مرجع سابق، ص199

[2]- براهمي حنان، المرجع السابق، ص213.

[3]- عبد الفتاح بيومي حجازي، التزوير في جرائم الكومبيوتر والانترنت، مرجع سابق، ص288.

[4]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، المرجع السابق، ص421.

يتحقق التزوير بهذه الطريقة إذا أدلى أحدهم بيانات كاذبة أمام الموظف الذي كتبها الموظف، وإنما وقع ممن أملى الإقرارات الكاذبة.[1]

من خلال ما سبق يتضح أن الفاعل في تزوير المحرر الرسمي بالطريق المعنوي دائما موظف عام، وهذا ما يجيب على التساؤل الخاص بإمكانية وقوع التزوير الالكتروني بهذه الطريقة في ظل ما نشهده من توغل الحواسب الآلية العملية واليومية سواء في عمليات الدفع، الفواتير و طلبات، البضائع وجميع عمليات البنوك والشركات والمؤسسات أيا كان حجمها.[2]

وعليه يمكن وقوع التزوير الالكتروني، خاصة أن أغلب الشركات والمؤسسات التابعة للقطاع العام أو الخاص، أصبحت تعتمد على تقنية المعلومات في كافة أعمالها كعدد العمال ورواتبهم وكمية الإنتاج وتوزيعها والميزانية والأرباح والخسائر، وعادة ما توضع هذه الحسابات والأعمال بيد موظف خبير في مجال الحاسب الآلي ليعالجها آليا، وأثناء إدخاله للبيانات يمكنه كتابه غير الأمر الذي طلب إليه رصده في الجهاز، وأيضا فالمتعاقدان المتباعدان مكانياً يمكنهم إثباته تصرفهم في عقد الكتروني رسمي وأثناء إملاء أحدهم على الموثق البيانات يقوم هذا الأخير بإدخالها على المحرر مغلوطة في الحاسب.[3]

2- جعل واقعة مزورة في صورة واقعة صحيحة:

يقصد بهذه الطريقة كل إثبات لواقعة على غير حقيقتها، وعلى ذلك فكل تشويه أو تحريف أيا كان يدخله كاتب المحرر على الوقائع التي يثبتها فيه عندئذ وفيه للمحرر، يعد تزويراً معنوياً بهذه الطريقة.[4]وتستوعب هذه الطريقة كل تقرير لواقعة على غير حقيقتها، ومن هذا المنطلق تشمل هذه الطريقة مجمل طرق التزوير المعنوي وتحويلها، فهي تشمل التزوير الواقع بطريقة تدوين اتفاقات أو

[1]- الهام بن خليفة المرجع السابق، ص105.

[2]- عبد القادر القهوجي، المرجع السابق، ص61.

[3]- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، المرجع السابق، ص.ص270،266.

[4]- محمود نجيب حسني، المرجع السابق، ص232.

أقوال غير التي صدرت من المتعاقدين، كما تشمل أيضا جعل واقعة غير معترف بها في صورة واقعة معترف بها.[1]

وعليه تعد طريقة تقرير الوقائع الكاذبة في صورة وقائع حقيقية هي أشمل طرق التزوير وتتسع لعدة طرق، إذ أن الطريقة الأولى الوارد شرحها لا تعدو كونها جعل وقائع كاذبة في صورة وقائع صحيحة، كما أن طريقة الشهادة كذباً بأن وقائع قد اعترف بها أو أوقعت في حضوره، وأيضا طريقة الشهادة كذباً بأن وقائع قد اعترف بها أو أوقعت في حضوره، وأيضا طريقة إسقاطه أو تغييره عمداً للإقرارات التي تلقاها والتي يسميها بعض الفقه حالة الإغفال.[2]

فالموظف العام القائم على تحرير الوثائق الرسمية الإدارية عندما يقوم بمعالجتها آليا بإدخال البيانات اللازمة لجهاز الحاسب الآلي، قد يقوم في مرحلة الإدخال بالتلاعب في البيانات حيث يقوم بتغييرها، كما في المثال السابق أو تغيير بيانات فاتورة الهاتف أو بيانات معاملة بنكية عند إنشاء الوثيقة المتعلقة بها عن طريق الحاسب الآلي، باعتبار هذا الجهاز أصبح يمثل عصب الحياة في حياتنا اليومية في المحاكم والوزارات والمدارس والجامعات والمواصلات وغيرها.[3]

ولا محال من وقوع التزوير في المحررات الالكترونية بطريقة جعل واقعة مزورة في صورة واقعة صحيحة بمختلف تطبيقاتها طالما أن كل القطاعات العامة والخاصة والأفراد يتجهون إلى التعامل بكل ما هو الكتروني، فتزوير المحرر الالكتروني أثناء إنشائه في مضمونه أو جوهره وظروفه أمر وارد.

وتجدر الإشارة هنا إلى أن الصلة جد وثيقة بين التزوير المعنوي والجريمة الالكترونية، ذلك أن النظام الالكتروني الذي ترتكب الجريمة من خلاله عبارة عن معلومة تتدفق بطريقة غير مرئية، وهذه المعلومة والتي تعكس معنى معين يمكن التحكم في دلالتها عن طريق البرمجة.[4]فإمكانية وقوع التزوير الالكتروني بالطرق المعنوية وراد بصورة أكبر من التزوير المادي والسبب في ذلك أن جوهر أو حقيقة التزوير المعنوي والذي يتحقق بتشويه المعاني كان يجب أن يعبر المحرر عنها، فهو تزوير مادي

[1]– أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، المرجع السابق، ص422.

[2]– أحمد فتحي سرور، الوسيط في قانون العقوبات،القسم الخاص،الطبعة الخامسة،دار النهضة العربية،مصر،2013، ص597.

[3]– نفس المرجع، ص209.

[4]– عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، مرجع سابق، ص222.

يؤدي إلى تغيير مضمون أو دلالة المحرر ذاته، فضلا أنه لا يتضمن آثاراً مادية تشير بجلاء إلى العبث بالمحرر ولذلك لا يستدل عليه إلا إذا تم التوصل إلى حقيقة ما كان يجب إثباته وذلك للوصول إلى أن ما تم مخالف للحقيقة، هذا فضلاً عن أن التزوير المعنوي مصاحب لإنشاء المحرر ذاته.[1]

وتجدر أيضا إلى أن إن الطرق المذكورة للتزوير الالكتروني ليست مذكورة على سبيل الحصر، ذلك أن التكنولوجيا الحديثة في تطور مستمر، وبشكل سريع ولذلك لا يناسب الصيغة التشريعية في تجريم تزوير المحررات الالكترونية أن تكون دالة على حصر طرق التزوير فيها فكلما أنتجت تقنية حديثة، كما اكتشف المزور طرقاً حديثة وجديدة يرتكب بها التزوير لم تكن معهودة من قبل.،

الفرع الثاني: الركن المعنوي

لا تكتمل جريمة التزوير إلا إذا توافر الركن المعنوي إلى جانب الركن المادي على غرار باقي الجرائم، وتعتبر هذه الجريمة من الجرائم العمدية، حيث لابد من توافر القصد الجنائي، غير أنه لا يكفي وجود القصد العام فقط وإنما لابد من توافر القصد الجنائي الخاص.

وعليه فلا بد من ضرورة توافر القصد الجنائي العام الذي يقوم على ضرورة توافر عنصري العلم والإرادة، إضافة إلى القصد الجنائي الخاص والمتمثل في اتجاه نية الجاني إلى استعمال المحرر فيما زور من أجله، وهذا ما سنبينه في العناصر الآتية:

أولاً- القصد العام:

يقوم القصد الجنائي العام في جريمة التزوير إذا انصرفت إرادة الجاني إلى تغيير الحقيقة في المحرر بإحدى الطرق التي بينها القانون مع توقعه احتمال حدوث ضرر مادي أو أدبي نتيجة لهذا الفعل، فالقصد العام يقوم على عنصري العلم والإرادة، فلا بد أن يدرك الجاني أنه يقوم بتحريف مفتعل للحقيقة في صك أو مخطوط أو مستند، وإجمالاً بمحرر وذلك بإحدى الطرق المادية أو المعنوية المنصوص عليها قانوناً.[2]

[1]- نفس المرجع والصفحة.

[2]- نهلا عبد القادر المومني، المرجع السابق، ص147.

ولابد أن يكون الجاني مدركاً أن هذا التزوير سيترتب عليه ضرر محقق أو احتمالي، أي لابد من أن يكون الفاعل على علم بجميع عناصر التزوير، لكن علم الجاني وحده لا يكفي لقيام جريمة التزوير، بل لابد من أن تتجه إرادته إلى القيام بالركن المادي المكون لجريمة التزوير.

والإرادة اللازمة في جريمة التزوير الالكتروني هي تلك التي تتجه لتحقيق الواقعة الإجرامية بسيطرتها على السلوك المادي وتوجيهه نحو تحقيق النتيجة، أي أن تتجه إرادة المزور إلى ارتكاب فعل تغيير الحقيقة في محرر وإلى تحقيق نتيجة وهي اشتمال المحرر على بيانات تخالف الحقيقة تسبب في إحداث ضرر[1] .

وزيادة على إرادة تغيير الحقيقة يقتضي القصد العام توافر علم الفاعل ببقية عناصر الجريمة، والقاعدة أن انتقاء العلم بأحد هذه العناصر ينفي القصد سواء كان راجعاً إلى غلط في الوقائع أو في القانون طالما كان هذا الغلط بعيداً عن نص التجريم ذاته.[2]فالعلم بالشيء هو إحاطة الذهن به وإدراك حقيقته وهو أبرز ما يميز العمد عن الخطأ ويشترط فيه أن يكون شاملاً لكل عناصر الجريمة وأن يكون معاصرة لارتكابها.[3]

والعلم المتطلب في جريمة التزوير أن يعلم الجاني وقت ارتكاب الجريمة أنه يغير الحقيقة وأن فعله هذا ينصب على محرر ورقي أو الكتروني، وأنه ترتكبه بطريقة ما سواء تلك التي ذكرتها القوانين أو غيرها، وأن فعله يترتب عليه ضرر حال أو احتمالي.

كما ينبغي أن يعلم الجاني أن فعله يسبب ضرراً فعلياً أو محتملاً للغير، فإذا انتفى ذلك انتفى القصد أيضاً.[4]

فالقصد الجنائي العام بعنصريه العلم والإرادة يجب توافره حتى يمكن نسبة التزوير الالكتروني إليه، حيث يجب أن يكون عالماً بأن إدخال المعلومات والبيانات إلى مضمون المحررات أو محو تلك

---

[1]– فوزية عبد الستار، المرجع السابق، ص305.

[2]– احسن بوسقيعة، الوجيز في القانون الجنائي الخاص، المرجع السابق، ص415.

[3]– محمد نجيب حسني، شرح قانون العقوبات، القسم الخاص وفقا لأحدث التعديلات التشريعية، المرجع السابق، ص310.

[4]– فتوح الشادلي، عفيفي كامل عفيفي، المرجع السابق، ص258.

المعلومات أو تحويلها وإتلافها أو القيام بأية أفعال أخرى من شأنها أن تؤدي إلى التأثير على المجرى الطبيعي لمعالجة البيانات، فإذا كان جاهلا بأن الفعل الذي يرتكبه غير مشروع فلا يتحقق القصد.[1]

وإذا كان عنصر الإدارة لا يثير أية إشكالات، فإن عنصر العلم يثير عدة إشكالات ولعلها أهمها هو الأشكال المتعلق بالغلط، فإذا كان العلم ينبغي بالجهل فهل ينتفي العلم بالغلط والشك؟وهنا نطرح التساؤل التالي: هل الجهل بقواعد التزوير في القوانين العقابية ينفي القصد الجنائي؟

ذهب الرأي الراجح في الفقه والمعمول به في القضاء أن الجهل بالقانون الجنائي لا ينفي العمد، وبهذا تقع جريمة التزوير ممن يغير الحقيقة جاهلاً بأن القانون يعاقب على تغييرها متى اكتملت العناصر الأخرى للجريمة.[2]

وهناك رأي في الفقه يرى أنه يجب توافر علم الجاني بأن المحرر موضوع التزوير قد توافرت فيه صلاحيته للإثبات وترتيب الآثار القانونية، ويجب أن يحيط علما فيما إذا كان المحرر رسميا أو عرفياً.[3] غير أنه متى كان من شأن تغيير الحقيقة إحداث ضرر محتمل بمن يحتج عليه بالمستند طبقاً لمجرى الأمور العادي، افترض علم الفاعل بذلك ولو لم يكن به فعلاً.[4]

ثانياً- القصد الخاص:

القصد الخاص هو نية إضافية أو قصد إضافي يتكون من اتجاه نية الجاني إلى استعمال المحرر المزور فيما زور من أجله، ويتوافر هذا القصد حتى ولو لم يستعمل هذا المستند المزور فعلاً.[5]فلا يكفي لقيام الركن المعنوي توافر القصد العام، بمعنى أنه لا يكفي توافر الإرادة والعلم بمكونات الجريمة، بل لابد أن تكون نية الجاني قد اتجهت وقت ارتكاب هذا الفعل إلى استعمال المحرر المزور فيما زور من أجله، أي الاحتجاج به على اعتبار أنه صحيح.[6]

---

[1]- نزيه عبد اللطيف، التزوير المعلوماتي، htpp:/Nazih abdelatif.blogspo.com، تاريخ الإطلاع على الموقع: 2017/04/15 الساعة00:18.

[2]- فوزية عبد الستار، المرجع السابق، ص306.

[2]- أحمد فتحي سرور، المرجع السابق، ص626.

[4]- أحمد محمود خليل، المرجع السابق، ص114.

[5]- علي عبد القادر القهوجي، الحماية الجنائية لبرنامج الحاسب الآلي، المرجع السابق، ص152.

[6]- إيهاب فوزي السقا، المرجع السابق، ص59.

وعليه فالقصد الخاص هو نية إضافية تتمثل في اتجاه نية الجاني إلى استعمال هذا المحرر المزور، فإذا تخلفت هذه النية انتفى القصد الجنائي، ومتى توافر للقصد الجنائي عناصره فلا عبرة بالبواعث التي تدفع الجاني على ارتكاب التزوير، فقد يكون الباعث شريف في ذاته ولكنه لا يحول مع ذلك دون توافر القصد الجنائي ومثال ذلك حالة من يصطنع مستنداً لإثبات حق متنازع عليه ولا سبيل لإثباته إلا بالدليل الكتابي.[1]

وقد ثار جدل فقهي حول تحديد القصد الخاص وهل يكفي لوقوع جريمة التزوير القصد العام وحده أم لابد من ضرورة توافر القصد الخاص؟.

فقد ذهب رأي في الفقه الايطالي إلى أنه يكفي لوقوع جريمة التزوير في المحررات الرسمية أن يتوافر القصد الجنائي العام بخلاف جريمة التزوير في المحررات العرفية، فإنه يجب أن يتوافر القصد الخاص.[2]

في حين ذهب الفقه في مصر وفرنسا إلى ضرورة توافر القصد الخاص في، جميع أنواع التزوير(*)، واستقر على أن القصد الخاص المتطلب لقيام الركن المعنوي للتزوير هو اتجاه نية المزور–لحظة ارتكاب فعل تغيير الحقيقة–إلى استعمال المحرر المزور فيما زور من أجله، ذلك أن التزوير لا يشكل خطراً اجتماعياً يقتضي تدخل القانون الجنائي لتجريمه إلا إذا ارتكب بنية استعمال المحرر بعد تزويره، فإذا لم تتوافر تلك النية لحظة الفعل، ولو توافرت بعد ذلك فلا تزوير، لأنه يلزم معاصرة القصد للفعل كقاعدة لقيام كل الجرائم بما فيها التزوير.[3]

وتعبر صيغة النص الجنائي الفرنسي في تجريم التزوير من الصيغ الواضحة في تطلب هذا القصد، حيث يشير النص إلى ضرورة وقوع التزوير بنية الغش، أي أن تكون نية الجاني من التزوير

---

[1]– أمين طعباش، مرجع سابق، ص102.

[2]– الهام بن خليفة، المرجع السابق، ص136.

(*)– يرى جانب من الفقه الفرنسي، إلى أن القصد الخاص في جريمة التزوير هو قصد الإضرار بالغير، أي أن عنصر الضرر مرتبط بالركن المعنوي، في حين يرى جانب آخر من الفقه إلى أن القصد الخاص في جريمة التزوير هو نية الاحتجاج بالمحرر المزور كدليل مخالف للقانون وهذا الرأي يربط القصد الخاص بفكرة الإثبات./ للمزيد أنظر: أحمد فتحي سرور، المرجع السابق، ص ص628،627 وعوض محمد، المرجع السابق، ص266،265، وأيضا الهام بن خليفة المرجع السابق، ص136، وما بعدها.

[3]– محمد زكي أبو عامر، المرجع السابق، ص319.

التأثير في إثبات حق أو واقعة لها أثار قانونية، ويعني ذلك أن المشرع الفرنسي، يتطلب في الجريمة توافر قصد عام لدى الجاني، كما تطلب أيضا توافر قصد خاص قوامه غرض الجاني التأثير في إثبات حق أو واقعة قانونية.[1]

وباعتبار جرائم التزوير في المحررات هي جرائم عمدية فإن المبدأ العام فيها هو الباعث أو الدافع لا تأثير له على قيام الجريمة ولا عبرة بالباعث الذي دفع بالمجرم إلى ارتكاب الجريمة سواء كان هذا الدافع نبيلاً وشريفا كالتزوير من أجل إحقاق الحق، كاستعمال المحرر لنشر فضيحة أو إنقاذ صديق أو قريب من مأزق خطير، سواء أكان غير نبيل أو مشروع كتحقيق الإثراء بلا سبب أو قد يكون لمجرد انتقام...[2]

ومما سبق نخلص إلى أن الركن المعنوي لجريمة التزوير في نطاق المعاملات الالكترونية هو اتجاه إرادة الجاني إلى تزوير مستندات معلوماتية مع نية مسبقة في استعمال المستندات المزورة في الغرض التي يتم تزويرها من أجله وأن يؤدي هذا الفعل إل حصول ضرر فعلي أو احتمالي لم ارتكب ضده، فمتى توافر الركن المادي والمعنوي قامت جريمة التزوير واستحق مرتكبها العقوبة.

الفرع الثالث: الركن الشرعي:

لقد استقر الفقه التقليدي في تحليله للواقعة الإجرامية على أنها تتكون من ركنين؛ ركن مادي يمثل المظهر المادي لها، وركن معنوي يتخذ إما صورة قصد جنائي عمدي من علم وإرادة، وإما صورة قصد جنائي خاص ولكن الفقه الألماني والإيطالي أضافا ركنا ثالثاً وهو الركن الشرعي والذي يقصد به توفر نص التجريم الواجب التطبيق على الفعل، وهذا يعني وجوب خضوع التزوير لنص يجرمه ووجوب ألا يخضع الفعل المجرم بنص قانوني لسبب من الإباحة التي تخرج الفعل من دائرة التجريم إلى دائرة الإباحة، وهذا يعني وجوب أن يخضع التزوير لمبدأ الشرعية إذ لا يخضع لعقوبة إلا بنص، فلمواجهة الجريمة الالكترونية لابد من وجود نصوص خاصة، ويطرح الركن الشرعي عدة إشكالات قانونية هامة منها ما يتعلق بالموقع أي مكان هذه الجرائم، حيث ترددت العديد من الدول في اختيار

[1]– أشرف توفيق شمس الدين، المرجع السابق، ص115.

[2]– محمد زكي أبو عامر، المرجع السابق، ص260.

التقنية التشريعية المناسبة، وكذا إشكالية الطريقة أو المصطلحات التقنية والتي تعتبر غريبة عن لغة القانون[*1].

وعليه سنحاول من خلال هذا الفرع التطرق إلى الصيغ التشريعية في تجريم التزوير الالكتروني، ثم التطرق إلى مدى تطبيق نص التزوير التقليدي على التزوير الالكتروني وهذا على النحو التالي:

أولاً- الصيغ التشريعية في تجريم التزوير الالكتروني:

لقد اعتمدت بعض الدول نهجاً معينا في تجريم التزوير الالكتروني بصفة عامة حيث تم توسيع نصوص قانون العقوبات ليشمل هذا النوع التزوير، ومن هذه الدول نجد فرنسا حيث سارعت إلى إحداث تعديلات على نصوص التزوير ليشمل التزوير المستحدث[1]، أما صيغ بعض القوانين العربية كالقانون المصري والقانون الإماراتي فتعتمد على تحديد مفهوم التزوير الالكتروني في قوانين مستقلة، كقانون التوقيع الالكتروني المصري والقانون الاتحادي الإماراتي لجرائم تقنية المعلومات الذي يعتبر من القوانين العربية السابقة في مكافحة الجرائم الالكترونية[2].

أ- صيغة التجريم في التشريع الفرنسي من خلال قانون العقوبات الفرنسي:

إن المشرع الفرنسي كان قد نظم الجرائم الالكترونية أو المعلوماتية بقانون خاص رقم 88/19 المؤرخ في 5 يناير 1988، حيث نص في المادة 462 في فقرتها 5 على:

¨Quin conque aura procédé a la falsification de documents informatisés quelle que soit leur forme, de mature a causer un préjudice a autrui, sera puni

2- وهنا يقتضي الأمر وجود نصوص قانونية خاصة لمواجهة الجريمة الالكترونية، ووعياً بخطورة الوضع، أصدر المجلس الأوروبي سنة 1989 توصية لتشجيع الدول الأعضاء على تبني نصوص جديدة للحد من هذه الظاهرة، وترددت العديد من الدول في اختيار التقنية التشريعية المناسبة، بأن يدرج هذه النصوص في إطار العقوبات التقليدي أم لابد من قانون جنائي مستقل يدخل في إطار القانون الجنائي التقني؟ وهذه هي إشكالية الموقع أو المكان، والمقصود من ذلك هل يوجد مكان لهذه الجرائم في القانون الجنائي التقليدي؟ أي هل يمكن دمج النصوص الجديدة ضمن نصوص القانون الجنائي التقليدي؟ أي هل يمكن دمج النصوص الجديدة ضمن نصوص القانون الجنائي التقليدي؟ أم أن الأمر يحتاج إلى قانون خاص؟.

2- توسع المشرع الجنائي الفرنسي في تجريم التزوير ليمتد إلى الوثيقة المعلوماتية في القسم الأول ضمن الكتاب الرابع من قانون العقوبات تحت عنوان "الاعتداءات ضد الثقة العامة، وهذا في المادة 441 في فقرتها الأولى والمعادلة في 14 ماي 1993.

emprisonnent d an a cinq ans et d une amende de 20.000 Frans a 2,000,000 Frans¨. وعليه فهذا النص يجرم تزوير المستند الالكتروني المعالج آليا مهما كان شكلها إذا سبب ذلك ضرراً للغير، وبالتالي كان منهج المشرع الجنائي الفرنسي هو إفراد نص مستقل في قانون العقوبات لمواجهة تزوير المستندات المعالجة آلياً،[1] وقد اعتبر الفقه الفرنسي هذه المواد مكملة للمادة 150 الخاصة بتزوير المحررات، وبذلك اعتبرت جريمة تزوير المحرر الالكتروني مستقلة من جريمة تزوير المحررات.[2]

ولكن بعد تعديل قانون العقوبات الفرنسي لم يأخذ المشرع بالمادتين 462 فقرة 5 وكذلك الفقرة 6 المتعلقتين بتزوير المستندات المعالجة آلياً وكذا استعمالها على اعتبار أن المادة 441 فقرة قد وسعت من مفهوم المستند المزور، كما أن هاتين المادتين لاقتا اعتراضات في مجلس الشيوخ عند مناقشة هذا القانون، نظرا لما يترتب عليها من مساواة بين المعطيات المعلوماتية بصفة عامة وبين المحررات من حيث القيمة القانونية.[3]

لذلك غير المشرع الجنائي الفرنسي خطة تجريم المستندات الالكترونية(*)، باعتبار أن المصلحة المحمية في جرائم المساس بالمعالجة الآلية للمعطيات والبيانات مختلفة عن تلك المتعلقة بجرائم التزوير في المحررات التي تتعلق بحماية الثقة العامة فيها، وبذلك اختفت جريمتا تزوير المستندات المعالجة آليا واستعمالها من الباب الثالث (المتعلق بالجرائم المعلوماتية) وأضافها إلى جريمة التزوير العادية بعد تطويع نصوصها بما يتلاءم وتلك المستندات.

كما لم يحدد المشرع الفرنسي في المادة 441 طرق معينة لارتكاب التزوير وهذا يعني استخدام شتى الطرق والأساليب المعلوماتية أيا كانت لارتكاب الفعل الإجرامي والمتمثل في تزوير المستندات المعلوماتية.[4]

(*)– يعرف هذا القانون بـ loi Grodfrain نسبة إلى النائب الذي تقدم به (Jacaque God Frain).

[1]– براهمي حنان المرجع السابق، ص167.

[2]– أشرف توفيق شمس الدين، مرجع سابق، ص108.

[3]– براهمي حنان، المرجع السابق، ص168.

[4]– على عبد القادر القهوجي، المرجع السابق، ص49.

إذن فبعد صدور القانون الفرنسي الجديد في 1992/12/16 قرر المشرع الفرنسي عدم ضرورة الإبقاء على التجريم الخاص بتزوير المستندات المعالجة آليا واستعمالها والاكتفاء بإضافة إلى جريمة التزوير العادية، وقد تم تعديل المادة 441 من الكتاب الرابع من قانون العقوبات لكي تفي بهذا الغرض.[1]

وبذلك يكون المشرع الفرنسي قد حسم الجدول الذي كان قائما من خلال المادة 441 فقرة 1 من قانون العقوبات، كما قطع كل خلاف حول مفهوم المحرر الذي به أصبح ينصرف إلى المحرر المكتوب والمحرر الالكتروني الذي عبر عنها بلفظ "أي دعامة أخرى"، حيث ينصرف هذا التعبير إلى كافة الأشكال المقررة التي يمكن أن يكون وعاء للتعبير عن فكرة يمكن أن ينتج عنها دليل على حق أو واقعة ذات آثار قانونية،[2] وبذلك يكون المشرع الفرنسي ومن خلال المادة 441 من قانون العقوبات قد حقق هدفين، يتمثل الهدف الأول في استيعاب هذا النص حالات التزوير التقليدي في المحررات إلى جانب تزوير المحررات الالكترونية، أما الهدف الثاني فهو خروج جريمتي تزوير المستندات المعالجة آليا واستعمالها من بين جرائم الاعتداء على نظم المعالجة الآلية للمعطيات.

ب- الصيغ التشريعية في تجريم التزوير الالكتروني على المستوى العربي:

لقد اختلفت خطة التشريعات حول موضع النص على جريمة التزوير الالكتروني، فهناك من ذهب إلى إحداث تعديلات على نصوص التزوير في قانون العقوبات كالمشرع الفرنسي-كما رأينا- وأيضا المشرع التونسي.[3]

وهناك اتجاهات تشريعية جرمت التزوير الالكتروني بنصوص خاصة تجرم كل الاعتداءات على تقنية المعلومات أي تنص الجرائم المعلوماتية منها التشريع المصري والإماراتي،والتي سوف نتطرق إليها فيما يلي، كما سندرس خطة التشريع الجزائري وذلك على النحو التالي:

1- صيغة التجريم في التشريع المصري:

لقد تناول المشرع المصري التزوير في المحررات في المواد من 211 إلى 227 من قانون العقوبات المصري ضمن الباب السادس عشر من الكتاب الثاني.

---

[1]- عبد الفتاح بيومي حجازي، الدليل الجنائي في جرائم الكومبيوتر والانترنت، مرجع سابق، ص143.

[2]- عبد الفتاح بيومي حجازي، التجارة الالكترونية، المرجع السابق، ص165.

[3]- أنظر: نهلا عبد القادر المومني، المرجع السابق، ص151 وأشرف توفيق شمس الدين، المرجع السابق، ص540.

وإزاء ضيق نطاق النصوص التقليدية للتزوير بشأن مواجهة التزوير الذي تقع في مجال المعالجة الالكترونية للبيانات وحماية للثقة الواجب توافرها في المستندات المعالجة الكترونيا خاصة مع نظام الاعتماد على السندات تلك في تسيير شؤون المجتمع الحديث، تدخل بعض الفقه المصري بلزوم التدخل التشريعي عن طريق إفراد قانون خاص لهذه الإشكالية على خطى الاتجاه الدولي والأخذ بالمفهوم الموسع للمحرر ليشمل المحرر الالكتروني بل ويتعداه إلى ما يشمل المحرر الالكتروني بل ويتعداه إلى ما يستجد من المحررات دون اشتراط أن تكون مدونة على خامة معينة أي سواء من الورق أو مكتوبة بخط اليد، ونتيجة لذلك شرع المشرع المصري نحو إسباغ الحجية القانونية للمحررات الالكترونية مثلها مثل المحررات التقليدية وذات الحال على التوقيع الالكتروني لمنحه نفس حجية التوقيع العادي.[1]

لذا فقد جرم المشرع المصري فعل التزوير في المحررات الالكترونية في قانون التوقيع الالكتروني وإنشاء هيئة تنمية صناعية تكنولوجيا المعلومات، إذ جاء في المادة 23 الفقرتين "ب" و "ج" أنه يعاقب كل من يزور محرراً الكترونيا بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر، وكل من يستعمل محرراً الكترونيا مزوراً مع علمه بذلك.

ويرى الفقه في مصر أن المشرع أحسن فعلا عند نصه على التزوير المستحدث في قانون منفصل ولم يخضعه لنصوص التزوير في قانون العقوبات، لأن المساس بمحتوى المستند الالكتروني يكون أشد صعوبة من المساس بالمستند الورقي على أساس اعتماد المعاملات الرقمية على تكنولوجيا التشفير وتأمين البيانات، كما أن اِكتشافه يكون صعباً، وطرق تزويره لا ينبغي تحديدها لأنه أمر غير ممكن لتعدد صور تغييره الحقيقة واختلافها وتجددها ما لا يمكن معه حصرها.[2]

كما جرم المشرع المصري في قانون الأحوال المدنية تزوير الوثائق الرسمية ذات الطبيعة المعلوماتية المخزنة كالكومبيوترات الموجودة بمراكز الأحوال المدينة من خلال المادة 72 التي تنص على:" في تطبيق أحكام هذا القانون وقانون العقوبات تعتبر المسجلة بالحسابات الآلية وملحقاتها بمراكز معلومات الأحوال المدينة ومحطات الإصدار الخاصة بها المستخدمة في إصدار الوثائق وبطاقات تحقيق الشخصية بيانات ورادة في محررات رسمية.

[1]– محمد إبراهيم غازي، المرجع السابق، ص521.

[2]– محمد أمين الرومي، المستند الالكتروني، المرجع السابق، ص88.

فإذا وقع تزوير في المحررات السابقة أو غيرها من المحررات الرسمية تكون العقوبة الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات".

وعليه فإن هذا النص خاص بالتزوير الواقع على المعلومات التي تتضمنها الحواسيب الخاصة بمصلحة الأحوال المدنية، لكن مع ذلك يسرى هذا النص على التزوير الذي يرتكب عن طريق شبكة الإنترنت في هذه المعلومات وتلك الوثائق، إذا كان استخدامها هو الوسيلة للوصول إلى الحاسبات الآلية الخاصة بمصلحة الأموال المدنية.[1]

2- صيغة التجريم في التشريع الإماراتي:

نظراً لضيق نطاق النصوص التقليدية للتزوير وعجزها حسب الراجح في الفقه والقضاء عن مواجهة التزوير الذي يقع في مجال المعالجة الالكترونية للبيانات وحماية للثقة الواجب توافرها في المستندات المعالجة الكترونيا، خاصة بعد تعاظم الاعتماد عليها في تسيير شؤون المجتمع الحديث، اتجه المشرع في العديد من الدول إلى ادخل هذه النوعية المستحدثة من التزوير في دائرة التأثيم بموجب نصوص سنت لهذا الغرض.

وكان للمشرع الإماراتي وقفة تشريعية مميزة في هذا الجانب من خلال القانون الاتحادي لمكافحة جرائم تقنية المعلومات.[2]

وقد سبق هذا القانون الاتحادي القانون 2002/02،[3] المتضمن القانون الخاص بالمعاملات والتجارة الالكترونية والذي يبين مفهوم المستند الالكتروني في المادة 02 منه حيث اعتبره: "كل" مستند يتم إنشاؤه أو تخزينه أو استخراجه أو انسخه أو إرساله أو إبلاغه أو استلامه بوسيلة الكترونية، على وسيط الكتروني آخر، ويكون قابلا للاسترجاع بشكل تمكن فهمه:.

إذا فقد جرم المشرع الإماراتي في القانون الاتحادي الخاص بجرائم تقنية المعلومات بعد الأفعال التي تتصل بالأنظمة المعلوماتية أو باستخدام جهاز الكومبيوتر ومن بينها فعل التزوير في مستند من

---

[1]- أشرف توفيق شمس الدين، مرجع سابق، ص108.

[2]- القانون 2006/02 المؤرخ في 30 يناير 2006، المتعلق بمكافحة جرائم تقنية المعلومات الجديدة الرسمية، عدد 442، الصادرة في 31 يناير 2006، ص55 وما بعدها.

[3]- القانون 2002/02 المؤرخ في 12 فبراير 2002، بشأن المعاملات والتجارة الإلكترونية، الجريدة الرسمية، عدد277، الصادرة في 16 فبراير 2002، منشور على الموقع (www.arab elaw.com).

مستندات الحكومة الاتحادية وبالتحديد في المادة 04 منه حيث نصت على:" يعاقب بالسجن المؤقت كل من زور مستندا من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية المعترف بها قانوناً في نظام معلوماتي، وتكون العقوبة الحبس أو الغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير فيما عدا ذلك من المستندات إذا كان من شأن ذلك إحداث ضرر، ويعاقب بالعقوبة المقررة بجريمة التزوير حسب الأحوال من استعمل المستند المزور مع علمه بتزويره".

والملاحظ على نص هذه المادة أن المشرع الإماراتي شدد العقوبة المقررة إذا كان التزوير في مستند من مستندات الحكومة الاتحادية أو المحلية أو المؤسسات العامة الاتحادية والمحلية المعترف بها قانوناً في النظام القانون وهي السجن المؤقت، في حين تكون العقوبة الحبس أو الغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير في مستند غير صادر عن هذه الجهات أخذ باتجاه اتفاقية بودابست المتعلقة بالإجرام المعلوماتي.

وكما سبقت الإشارة يعد القانون الاتحادي بشأن جرائم تقنية المعلومات من القوانين العربية السابقة في مكافحة الجرائم المعلوماتية وفي تبني نظام الحكومة الالكترونية ساعية إلى تحويل الخدمات والمعاملات الحكومية من الشكل الورقي إلى الشكل الالكتروني.

لكن الملاحظ على المشرع الإماراتي من خلال المادة 04 أعلاه أنه لم يضع صيغة تشريعية واضحة في التجريم، حيث لم يتطرق إلى أركان هذه الجريمة فلم يبين ولا نوع القصد الجنائي المطلوب مكتفيا بعنصر الضرر الذي ذكره فقط عند تجريم تزوير المستند غير الحكومي، وهذا ما يطرح التساؤل عما إذا كان عنصرا الضرر ينبغي توفره فقط في هذا النوع من التزوير؟.

3- صيغة التجريم في التشريع الجزائري:

في الجزائر هناك محاولات جادة لتطوير المنظومة القانونية وإصدار تشريعات تواكب التطور الحاصل في المجال التكنولوجي خاصة ما تعلق منها بتكنولوجيا الإعلام والاتصال ثم تغيير حتى اسم الوزارة المعنية لتأخذ اسم وزارة البريد وتكنولوجيات الإعلام والاتصال كمؤشر على النية الحقيقية في خوض عمار الالتحاق بمصاف الدول الآخذة بناصية هذه التقنية، وهذا ما يؤكد المساعي الجادة لتعديل وتكييف المنظومة القانونية مع المعطيات الدولية خاصة بعد انضمام الجزائر إلى الاتفاقيات

الدولية خاصة المتعلقة بالملكية الفكرية ذات العلاقة بالتجارة والمسماة تريبس (trips)،[1] والتي بموجبها تصبح الجزائر ملزمة ببسط الحماية على الملكية الصناعية وبراءات الاختراع والعلامات الصناعية والتجارية، وكذلك اتفاقية برن للمصنفات الإدارية والفنية.[2] وهذا بهدف بلوغ مستوى التشريعات الدولية في مجاراة مصطلحات جديدة فرضها واقع جديد في مجال الاتصالات والمعلوماتية بظهور التجارة الالكترونية وما صاحبه ذلك من مفاهيم كالعقد الالكتروني، البطاقات الالكترونية، الفواتير الالكترونية، المفتاح الالكتروني....

كما أنه وفي إطار الجهود الدولية والإقليمية المتعلقة بترقية ودعم سياسة مكافحة الجرائم الالكترونية، عمد المشرع الجزائري على مسايرة النسق التشريعي، لأجل البقاء على اتصال بأحدث الحلول التشريعية الخاصة بهذه الجرائم، خاصة وأن الجزائر تعرف مؤخرا وفي السنوات الأخيرة تعميم خدمة الربط بشبكة الانترنت، ودعم الجهات الحكومية بتقنيات المعلوماتية، وهو ما تولد عنه ارتفاع محسوس في معدلات الجريمة الالكترونية، وهي المعطيات التي دفعت بالمشرع الجزائري إلى التدخل من أجل رسم الخطط القانونية والعملية، لتنفيذ سياسة وقائية ورعية ضد الجرائم الالكترونية، وقد كان أول تشريع خاص بهذا المجال بصدر القانون 04/ المؤرخ في 2004/11/10 المعدل والمتم لقانون العقوبات الجزائري واستحداث قسم خاص معنون بقسم جرائم المساس بأنظمة المعالجة الآلية للمعطيات والذي حمل بين طياته نصوص المواد من 394 مكرر إلى 394 مكرر 7، والتي تضمنت في فحواها صور الجرائم المعلوماتية إضافية إلى تحديد العقوبات المناسبة لها.

غير أن هذا الجهد لم يكن كافياً لتفعيل سياسة مكافحة الإجرام المعلوماتي بسبب تعارض أحكام قانون العقوبات وقانون الإجراءات الجزائية لاسيما فيما يتعلق بمسائل الاختصاص النوعي والإقليمي، مما استدعى تدخل المشرع الجزائري بموجب القانون 22/06 المؤرخ في 2006/12/20 المعدل والمتهم لأحكام قانون الإجراءات الجزائية الجزائري والذي عدل من نصوص المواد من 45 إلى 47 والتي تحدد قواعد الاختصاص النوعي والمحلي وكذا قواعد التفتيش.

ولم يكتف المشرع الجزائري بهذا فحسب بل أضاف في هذا الصدد القانون 09-04 المؤرخ في 2009/08/05 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والذي يعتبر قانوناً

[1]- صادقت عليها الجزائر بمقتضى الأمر، رقم 02/75 المؤرخ في 09جانفي 1975.

[2]- انضمت إليها الجزائر بمقتضى المرسوم الرئاسي رقم 97-341 المؤرخ في 13 سبتمبر 1997.

نموذجياً خاصة بمكافحة الجرائم المعلوماتية على اعتبار أنه قانون يتضمن نصوصاً خاصة في هذا الشأن.[1]

وعليه فالمشرع الجزائري أطلق على الجرائم المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وأورد تعريفاً لها في المادة 02 فقرة –أ– على أنها(...جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية).

ومن خلال المادة المذكورة أعلاه نجد أن الجرائم المعلوماتية المنصوص عليها هي جريمة الدخول أو البقاء بغش في النظام وجريمة الاعتداء العمدي على سلامة المعطيات ،وجريمة التعامل في معلومات غير مشروعة ،وكذلك أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية،وهنا يقصد المشرع أي جريمة لم تحدد في هذه المادة ويمكن أن تحدث في بيئة معلوماتية،وهذا ما ينطبق على جريمة التزوير الالكتروني طبقا لمبدأ الشرعية بطابعه المرن والمستحدث.

كما أنه نصوص التزوير في قانون العقوبات لم تتضمن إشارة بإمكانية تطبيق هذه النصوص على التزوير الالكتروني في ظل الاعتراف بالقيمة االثبوتية للمحرر الالكتروني بموجب تعديل القانون المدني، وهنا يستلزم على المشرع أن يعدل في نصوص التزوير يستوعب حتى العقاب على التزوير المحرر أو المستند الالكتروني، خاصة وأن هذه الجرائم تتميز بالطابع الدولي والتقني بالقدر الذي تستطيع أجهزة العدالة من خلاله تطبيق الإجراءات المنصوص عليها في هذا القانون من جهة، وتفعيل آليات التعاون الدولي لمواجهة مثل هذه الجرائم من جهة أخرى.

ثانياً– مدى تطبيق نص التزوير التقليدي على التزوير الالكتروني:

سبقت الإشارة أن التشريعات الجنائية في مختلف الدول تجرم التزوير سواء كان المحرر عرفياً أو رسمياً وهذا حماية للثقة العامة، إلا أن خطة التشريعات اختلفت حول موضع النص الذي يجرم التزوير، لذلك ثار الأشكال في مدى انطباق نص التزوير التقليدي على التزوير الالكتروني كون أن

1–القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،الجريدة الرسمية للجمهورية الجزائرية،المؤرخة في 25 شعبان 1430 الموافق ل 16 غشت 2009 ،ص 9.

فكرة المحرر الالكتروني لا تتلاقى مع فكرة المحرر العادي، مما يؤدي بالضرورة إلى مناقشة مدى إمكانية انطباق معنى المحرر على المعلومات المعالجة آليا والتي تثبت حقاً أو مركزا قانونياً معينا.

وهناك اتجاهات بهذا الصدد، جانب يرى عدم تطبيق نص التزوير التقليدي على التزوير الالكتروني، في حين يرى جانب آخر من الفقه إمكانية تطبيق نص التزوير التقليدي على التزوير الالكتروني، وهذا ما سنوضحه في الآتي:

أ- عدم تطبيق نص التزوير التقليدي على التزوير الالكتروني:

قبل صدور القوانين التي تجرم التزوير في المحررات الالكترونية، أثيرت مشكلة مدى إمكانية تطبيق نصوص التزوير التقليدية على التزوير الالكتروني، حيث انقسم الفقه الفرنسي إلى اتجاهين، حيث يرفض الاتجاه الأول تطبيق نصوص التزوير التقليدية بحجية أنها تتطلب بأن يقع التزوير أولاً في محرر ورقي مكتوب ومن غير الممكن قياس المحررات الالكترونية على المستند الورقي، وثانياً تفترض إمكانية القراءة البصرية لمحتويات المحرر وهذا غير متحقق مع المحرر الالكتروني، لأن البيانات المحتواة فيه غير مقروءة، ولا يمكن إدراكها بالعين البشرية، كما أنها لا تعتبر عن فكرة بشرية وإنما تعبر عن فكرة آلية، وبالتالي استوجب مواجهة هذا النوع الجديد عن الجرائم بتشريعات مستقلة.[1]

ويؤكد هذا الاتجاه على عدم إمكانية تطبيق النصوص المتعلقة بالتزوير على تغيير الحقيقة في المعلومات المبرمجة كونها لا تعتبر محرر من حيث أنه لا تمكن مشاهدة المعلومات المخزنة على وسائط التخزين الخاصة بها عن طريق النظر، وبالتالي فهي ليست مقروءة ولا يمكن للمعنى الذي تحمله عن طريق العين المجردة.[2]

ولذلك فإنه في إطار نص التزوير التقليدي لا يمكن مد هذا النص ليشمل التزوير في المحرر أو المستند ذو الطبيعة الالكترونية لسببين:[3]

- جمود النص الجنائي مما يصعب معه التأويل، لعدم وجود أي إشارة إلى الأشكال المستحدثة من الوثائق، طالما هناك ربط بين الوثيقة المعلوماتية والكتابة التي لها مدلول ورقي غالباً.

---

[1]- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2009، ص111.

[2]- نائلة عادل محمد فريد قورة ،جرائم الحاسب الآلي الاقتصادية،دار النهضة العربية،2004 ص584، 585.

[3]- براهمي حنان، مرجع سابق، ص175.

– التلازم بين قيام جريمة التزوير وشرط وجود محرراً أو وثيقة لها قيمة ثبوتية يقتضي الرجوع إلى قوانين الإثبات وكيفية تنظيمها للدليل المكتوب، فإذا كانت هذه النصوص جامدة بحيث ترتبط الكتابة بالشرط الورقي، أولا تمكن التوسع في تفسيرها فإن هذا سيغلق الباب أمام تفسير النص الجنائي وبالتالي لا يمكن تطبيقه على الوثيقة ذات الطبيعة المعلوماتية باعتبار أن مفهوم الكتابة لا يشملها.

وأخذا بهذا الاتجاه تعتمد بعض التشريعات إلى عدم إمكانية تطبيق نصوص التزوير التقليدية على الإجرام الالكتروني المستحدث لاختلاف الجريمتين، خاصة وأن الثانية جريمة ذات طابع دولي مرتكبيها لهم مميزات خاصة.

ب– إمكانية تطبيق نص التزوير التقليدي على التزوير الالكتروني:

يؤيد هذا الاتجاه فكرة تطبيق نصوص التزوير التقليدية بحجة أن الكتابة وإن كانت متطلباً تقليدياً في جرائم تزوير المحررات، إلا أنه بالإمكان تغليب روح النصوص على الألفاظ واعتبار ما يظهر على شاشة الحاسب الآلي شكل مستحدث للكتابة، وأن وجود المحرر هو شرط مفترض في جريمة التزوير، إلا أن القضاء لا يفرق بين محرر منسوخ أو مختزل، وأنه لا يوجد ما يمنع من الاعتماد على المحررات الالكترونية في الإثبات طالما أن هناك علاقة بين التزوير والإثبات وعليه تمكن تطبيق النصوص التقليدية، وبالتالي تمكن تطبيق النصوص التقليدية لمواجهة التزوير في المحررات الالكترونية.[1]

وعليه فيرى هذا الجانب من الفقه إمكانية تطبيق نص التزوير التقليدي على التزوير القائم على المحرر أو المستند الالكتروني، وهو ما حصل في فرنسا قبل صدور قانون الغش المعلوماتي السابق ذكره، حيث أيد البعض فكرة تطبيق النص التقليدي لجريمة التزوير كل تلاعب أو تغيير في الوثيقة المعلوماتية معتمداً في ذلك على التطبيق والتفسير القضائي وكذا نصوص قانون الإثبات.[2]

وقد أخذت العديد من التشريعات بإمكانية تطبيق نصوص التزوير التقليدية على التزوير الالكترونية على أساس أن كل المحررين متمثلان، خاصة فيما يترتب عليهما من آثار قانونية، وبالتالي أدخلت تعديلات على النصوص العقابية القائمة على نحو يؤدي إلى استيعاب صور التزوير

[1]– محمود أحمد عبابنة، المرجع السابق، ص111.

[2]– Marc Segonds, faux, juris–chasseur ;art441/1–12 Fase 20,20011,p3.

المستحدثة، أو تفرد قوانين خاصة لبعض الموضوعات مثل الاتصالات والتوقيع الالكتروني، كما سبق الإشارة في ذلك.[1]

فالمشرع الفرنسي قد حسم الجدل في قانون العقوبات الفرنسي لسنة 1992 والمعمول به منذ عام 1994 وذلك في المادة (1/144)، كما سبقت الإشارة- منه التي توسعت في مفهوم المحرر الذي يقع عليه التزوير، حيث أصبحت تشمل إلى جانب المحرر بشكله التقليدي كل وسيط آخر للتعبير عن فكرة- ويشمل ذلك بطبيعة الحال الأقراص الممغنطة والأسطوانات المدمجة وغيرها من وسائط تخزين المعلومات، ويشترط القانون أن يكون من الممكن استخدام المحرر أو الوسيط الذي تم تزويره لممارسة حق تصرف أو أن يصلح لإثبات حق أو تصرف له آثار قانونية.[2]

أما فيما يتعلق بالتشريع الهولندي والنرويجي والسويدي، فلقد اعتبرت جميعها المحررات الالكترونية مساوية للمحررات في مفهومها التقليدي متى كان من الممكن قراءتها عن طريق الأجهزة الالكترونية اللازمة لذلك.[3]

وتجدر الإشارة إلى أن توصية المجلس الأوروبي الخاصة بالجرائم المعلوماتية تضمنت الإشارة إلى جريمة التزوير الالكتروني واقترحت التوصية على الدول الأعضاء نموذجاً تشريعياً يتم مقتضاه تجريم كل إدخال أو تعديل أو محو أو إعاقة لمعلومات داخل الأنظمة المعلوماتية، حيث يشكل هذا السلوك تزويراً وفقا لقوانين الدولة مشيرة إلى أن الحماية الجنائية يجب أن تمتد إذا تمت طباعة هذه المعلومات لاستعمالها فيها زورت ممن أجله أو ظلت داخل الحاسوب لاستخدامها مباشرة بين الأنظمة المعلوماتية.[4]

المطلب الثاني: أنواع جرائم التزوير الالكتروني

لقد شهد العالم منذ منتصف القرن العشرين بداية ثورة المعلومات والاتصالات والتكنولوجيا الرقمية المعتمدة على الحاسب الآلي، حيث استعملت هذه التكنولوجيا في البداية في مجالات مهمة وحساسة، ليشع نطاقها ليشمل مختلف مجالات الحياة يلمس هذا التطور الإدارة العامة لتتحول

[1]- أشرف توفيق شمس الدين، مرجع السابق ص487.

[2]- نهلا عبد القادر المومني، مرجع سابق، ص150.

[3]- نائلة قورة، المرجع السابق، ص09.

[4]- نهلا عبد المومني، المرجع السابق، ص151.

معاملتها تدريجياً من البيئة الورقية إلى البيئة الافتراضية بهدف تقليص النفقات والوقت وكذا الحد من التضخم الورقي، وتحسين أداء الخدمة، إلا أنه في الوقت نفسه الوقت حمل معه مخاطر الاعتداءات على هذا النوع من المحركات التي أصبحت تشكها جسما كبيراً يهدد الثورة ليس بالنسبة للأفراد فقط، بل أعلى مستوى واسع وفي فضاء دولي مفتوح خاصة في التطور المتزايد للمعلوماتية وقد صاحب ذلك من ارتفاع نسبة الغش المعلوماتي، ومن أخطر صوره التزوير في المحررات الالكترونية.

وتأتي جريمة التزوير في المحررات على أنواع ثلاث أنواع، فقد يرد على المحررات الرسمية أو العمومية، كما قد ينصب على المحررات التجارية أو المصرفية أو العرفية، ويرد التزوير أيضا على بعض الوثائق أو الشهادات الإدارية وسنحاول في هذا المقام التطرق لهذه الأنواع على النحو الآتي بيانه:

الفرع الأول: التزوير في المحررات الالكترونية الرسمية أو العمومية:

يقتضي التزوير في المحررات العمومية أو الرسمية المنصوص والمعاقب عليها في المواد 214 إلى 216 فضلا عن الأركان المشتركة لكل صور التزوير، أن يقع التزوير على محرر عمومي أو رسمي وأن يتم التزوير بإحدى الطرق المادية أو المعنوية المبينة في المواد من 214 إلى 216 من قانون العقوبات الجزائري.

وسنحاول من خلال هذا الفرع التطرق إلى تعريف المحررات الرسمية أو العمومية،وكذا عناصر المحرر الرسمي،إضافة إلى نطاق رسمية المحررات، وهذا على النحو الآتي:

أولا: تعريف المحرر الرسمي أو العمومي:

بوجه عام يمكن تعريف المحرر العمومي أو الرسمي بأنه كل محرر يصدر أو من شأنه أن يصدر من موظف ومن يشبهه مختص بمقتضى وظيفته بتحريره وإعطائه الصيغة الرسمية أو يتدخل في تحريره أو التأشير عليه وفق ما تقتضيه القوانين واللوائح التنظيمية التي تصدر إليه من جهته الرئيسية.[1]

[1]– أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، المرجع السابق، ص416.

فالمحرر أو السند العمومي أو الرسمي هو كل وثيقة تحررها وتصدرها السلطات العمومية المتمثلة في إدارة رئيس الدولة والوزارات وفروعها سواء في الإدارة المركزية أو الإقليمية، ومن شأنها إثبات أي حق من الحقوق أو إثبات حالة قانونية.[1]

لكن السؤال الذي يثار في هذا الصدد هو ما الفرق بين المحررات العمومية والمحررات الرسمية، وهل أن المحرر الرسمي هو نفسه المحرر العمومي أم لا؟.

إن قانون العقوبات الجزائري لم يحدد معنى عبارة العمومية، ولا معنى عبارة المحررات الرسمية، وهما مصطلحات يستعملان للتفريق بين نوعين من الوثائق حسب مصدر وكل نوع منها، فإذا كان مصدر المحرر المزور هو شخص مكلف بخدمة عامة أو ضابط عمومي أمكن وصف المحرر بأنه محرر عمومي، وإذا كان مصدر الدولة أو أحد فروعها جاز وصف المحرر بأنه محرر رسمي.[2]

وعلى خلاف ذلك احتوت المادة 324 من القانون المدني تعريفا شاملاً للمحرر الرسمي بقولها:" المحرر الرسمي هو العقد الذي يثبت فيه موظف عام، أو ضابط عمومي، أو شخص مكلف بخدمة عام، ما تم لديه أو ما تلقاه من ذوي الشأن وذلك طبقا للأشكال القانونية وفي حدود سلطاته واختصاصاته".

وبالتالي فالمحرر العمومي هو كل ما يصدر عن أي ضابط عمومي أو شخص مكلف بخدمة عامة، مثل المحرر الصادر عن الموثق أو عن المحضر القضائي أو عن المترجم وشاملاً للمحرر الرسمي الصادر عن السلطة التنفيذية كالقوانين والمراسيم والقرارات الوزارية، أو عن السلطة القضائية أو السلطات الإدارية المحلية أو الإقليمية؛ مثل الوثائق التي تصدرها البلديات والولايات كرخص البناء ورخص السياقة وغيرها.

وأمام عدم تحديد التشريعات العقابية لمعنى المحررات الرسمية ولا معنى المحررات العمومية إلا أن بعض الفقه يرى أن المحررات العمومية هي تلك التي تحررها موظف عام في حدود ما استند إليه قانونياً من اختصاص، في حين أن المحررات الرسمية هي تلك المحررات التي يقيد فيها الضابط

[1]– عبد العزيز سعد، المرجع السابق، ص14.

[2]– نفس المرجع، ص16.

العمومي–كالموثقين والمحضرين القضائيين ومحافظي البيع بالمزاد العلني وكل التصرفات أو العقود ويجري فيها لتختلف الإثباتات، على سبيل المثال التبليغ الذي يعد من المحضر القضائي.

وعلى الرغم من محاولات التفريق بين المستندات أو المحررات العمومية، وبين المحررات أو المستندات الرسمية من حيث المظهر أو المصدر، إلا أن قانون العقوبات الجزائري قد وحد بينهما في العقوبة وفرق بين عقوبة تزوير المحررات العمومية وبين عقوبة تزوير المحررات الرسمية، هذا وإذا كان قانون العقوبات قد فرق وميز بين وسائل ارتكاب جرائم التزوير المنصوص عليها في المادة 215 من قانون العقوبات فإنه لا يتضمن معياراً حقيقياً للتفريق بين المحررات الرسمية والمحررات العمومية وهو ما يجعلنا نميل إلى تبني التعريف الذي تضمنته المادة 324 من القانون المدني.

وقد أجمع الفقه والقضاء على تقسيم المحررات الرسمية إلى أربعة أنواع:

1- المحررات السياسية:

وهي المحررات التي تصدر عن السلطتين التشريعية والتنفيذية ومثالها القوانين وأوامر رئيس الجمهورية بقوانين والمراسيم التنفيذية والقرارات الوزارية والمعاهدات،[1] غير أن هذه المحررات لا يمكن المخاصمة بها بطريقة التزوير لأن تزويرها مستبعد ونادر الوقوع.

2- المحررات القضائية:

وهي تلك المحررات التي تصدر عن السلطات القضائية بمعرفة أعضائها سواء كانوا قضاة وأعضاء نيابة عامة وسواء كانت تلك المحررات صادرة أثناء التحقيق أو السماع القضائي أو بعد صدور الحكم أو كانت صادرة عن معاونيهم مثل أعوان الضبط القضائي، ومن أمثلة هذا النوع من المحررات محاضر الجلسات أو التحقيقات ومحاضر الخبراء وتقاريرهم ومحاضر التفتيش، والتزوير في هذا النوع من المحررات يندر وقوعه أيضا وإن كان من المتصور حدوث التزوير في شهادة انحصار الورثة أو اصطناع كاتب الجلسة بإحلاله محل المحضر الأصلي.[2]

[1]– نبيل صقر، المرجع السابق، ص209.

[2]– علي محمد قاسم الطلي ،جريمة التزوير في المحررات الرسمية في القانون اليمني–دراسة مقارنة، دار النهضة العربية، مصر، ص.ص34،33.

3- المحررات الصادرة عن الموثقين والمختصين:

وهي المحررات التي يتم فيها إثبات إقرارات ذوي الشأن واتفاقاتهم وإضفاء صفة الرسمية عليها، ومنها العقود والتوكيلات الرسمية العامة والخاصة، إضافة إلى المحررات الصادرة عن كتاب الضبط والمحضرين القضائيين.

4- المحررات الإدارية:

وهي أكثر عدداً من سابقاتها وتشمل كل ما تصدر عن السلطات الإدارية المختلفة، وتذكر منها على سبيل المثال القرارات الولائية والبلدية ودفاتر عقود الحالة المدنية.

ولا يشترط القانون- كي تسبغ الرسمية على الورقة- أن تكون محررة على نموذج خاص، ذلك أن الصفة إنما يسبغها محررها لا طبعها على نموذج خاص، ومتى كانت الورقة عمومية أو رسمية فإن تغيير الحقيقية يعد تزويراً سواء حصل هذا التغيير في الورقة ذاتها أو في صورتها المطابقة لها.[1]

ومناط رسمية الورق أن يكون محررها موظفا عمومياً مكلفا بتحريرها بمقتضى وظيفته ومفاد ذلك أن المحرر الرسمي بالنسبة لجريمة التزوير يعتبر رسمياً في جميع أجزاه وتكتسب بياناته جميعاً الصفة الرسمية سواء ما أثبتها الموظف في المحرر ونسبها إلى نفسه باعتبار أنها حصلت منه أو وقعت بين يديه أو سواء ما تلقاه الموظف من ذوي الشأن من أقوال وبيانات وتقريرات في شأن التصرف القانون الذي تشهد به الورقة.[2]

ثانياً- عناصر المحرر الرسمي:

لكي نكون بصدد محرر رسمي يجب أن يكون هذا المحرر تضمن شروطاً ثلاثة:هي الصفة والاختصاص والشكل، وبجانب ذلك لابد أن يصدر المحرر عن الدولة أو أحد الأشخاص المعنوية العامة، وأن يتم تدوينه وفقا للأوضاع والإجراءات التي يحددها القانون.[3]

فالدولة كشخص معنوي عام تستعين في أداء مهامها بمجموعة من الأشخاص يعبرون عن إرادتها، ولهم الصفة في تمثيلها، وهؤلاء الأشخاص هم الموظفون العموميون وتكون للمحررات التي

---

[1]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الثاني، المرجع السابق، ص417.

[2]- نبيل صقر ، المرجع السابق، ص209.

[3]- علي محمد قاسم الطلي، المرجع السابق، ص28.

تصدر عنهم صفة الرسمية، وعلى ذلك لابد أن يصدر المحرر من موظف عام ويكون مختصاً بإصدار المحرر من حيث الموضوع أو المكان،[1] وبمفهوم المخالفة فإن المحررات التي تصدر من غير الموظف العام لا تعد محررات رسمية، ومثال ذلك المحررات التي تصدر عن الشركات أو البنوك بمختلف أنواعها لا تعد محررات رسمية، ولا تعد محررات عرفية.

أما بالنسبة للعنصر الثاني من عناصر المحرر الرسمي فهو يجب أن يكون تدوينه وفقاً للأوضاع والإجراءات التي تحددها القوانين واللوائح، وبمقتضى ذلك يعد المحرر رسميا إذا كان الموظف العام مكلفاً بتدوينه وإثبات جميع البيانات فيه، أو قد يقتصر دور الموظف العام بإثبات ما يملئ عليه أو التدخل من خلال المراجعة أو التأشير على المحرر دون أن يقوم بتحرير في الأصل أي أن يقتصر دوره على مراجعة المحرر فقط.[2]

ومن خلال ذلك يتضح لنا أن اختصاص الموظف العام بتحرير الرسمي لا يقتصر فقط على القوانين واللوائح المنظمة لذلك، بل إنه وإلى جانب ذلك يستمد الموظف العام اختصاصه من أوامر رؤسائه فيما لهم أن يكفلوه به في حدود القانون، كما أن المحرر قد يستمد رسميته من ظروف إنشائه أو من جهة مصدره أو بالنظر إلى البيانات التي يتضمنها وتلزم الموظف بالتدخل لإثباتها وإقرارها.

ثالثاً- نطاق رسمية المحرر:

إن نطاق رسميته المحرر هي أن يكون كاتب المحرر الرسمي موظفاً عاما مختصاً، وفي الواقع أن فكرة المحرر الرسمي تدور مع فكرة الموظف العام ومن حكمه وجوداً وعدماً، غير أن الاهتداء إلى هذا النطاق لا يكفي لحل صعوبة البحث فيما إذا كان المحرر رسمياً أم غير رسمي، لأنه لازال من المتعين الاهتداء كذلك إلى حقيقة مدلول هذا النطاق نفسه، ذلك أنه يتفرع عن هذا القول ارتباط فكرة المحرر الرسمي بالموظف العام أنه لتحرير صفة المحرر المزور يجب البدء ببحث ما إذا كان الشخص المختص بتحريره في العادة هو موظف أم لا؟

[1]- إبراهيم حامد طنطاوي، المرجع السابق، ص154.

[2]- علي محمد قاسم الطلي، المرجع السابق، ص28.

فجريمة التزوير في المحررات الرسمية أو العمومية قد ترتكب من موظف عام أو من في حكمه أثناء تأديته وظيفته، وقد يرتكبها عامة الناس، حيث يترتب على اختلاف صفة الجاني اختلاف العقوبات، لذا كان من الضرورة الوقوف عند هذه المسألة.

كما أن الفقه والقضاء الجنائيان توسعا في تحديد معنى الرسمية إلى مدى يتجاوز حدود الرسمية في نصوص الإثبات وذلك بإدراجها لفكرتي اصطناع محرر رسمي وكذا المحرر الرسمي الأجنبي، لذا كان من الضروري الوقوف عند هذه المسألة أيضا.

أ- صفة الجاني في جريمة تزوير المحررات الرسمية أو العمومية:

سبقت الإشارة أن التزوير في المحررات الرسمية أو العمومية، لا تمكن أن يرتكب من موظف عام أو من في حكمه فحسب، بل يمكن أن يرتكب عن عامة الناس وهذا ما نبحثه في النقاط التالية:

1- صفة الموظف العام أو من في حكمه:

بالرجوع إلى المادتين 214 و215 من قانون العقوبات الجزائري نجدها تنص على أن جريمة التزوير في المحررات الرسمية أو العمومية تتطلب ضرورة أن تتوافر في الجاني صفة الجاني أو من في حكمه.[1]

ومن خلال هاتين المادتين يتضح أن أهم عناصر أو أركان قيام جريمة التزوير في المحررات الرسمية أو العمومية هو عنصر الوصف الوظيفي، وذلك بأن يكون المتهم إما قاضياً بإحدى المحاكم أو بأحد المجالس القضائية سواء ضمن سلك العادي أو ضمن سلك القضاء الإداري أو القضاء

---

[1]- تنص المادة 214 من قانون العقوبات على أنه:" يعاقب بالسجن المؤبد كل قاض أو موظف أو قائم بوظيفة عمومية ارتكب تزويراً في المحررات العمومية أثناء تأدية وظيفته:

1- إما بوضع توقيعات مزورة،

2- وإما بإحداث تغييرات في المحررات أو الخطوط أو التوقيعات،

3- وإما بانتحال شخصيته أو الحلول محلها،

4- وإما بالكتابة في السجلات أو غيرها من المحررات العمومية أو بالتغيير فيها بعد إتمامها أو اقفالها".

كما تنص المادة 215 من قانون العقوبات الجزائري على أنه:" يعاقب بالسجن المؤبد كل قاض أو موظف أو قائم بوظيفته قام أثناء تحريره محررات من أعمال وظيفته بتزييف جوهرها أو ظروفها بطريق الغش وذلك إما بكتابة اتفاقات خلاف التي دونت أو أمليت من الأطراف أو تقريره وقائع يعلم أنها كاذبة في صورة وقائع صحيحة أو بالشهادة كذبا بأن وقائع قد اعترفت بها أو وقعت في حضوره أو بإسقاطه أو تغييره عمداً الإقرارات التي تلقاها".

العسكري، وإما أنه يقوم بخدمة عامة في إطار قانون الدولة وبرخصة منها مثل الموثقين والمحضرين للقضائيين والمترجمين، ويعرف الموظف العام في القانون الأساسي العام للوظيفة العمومية في المادة 04 منه بأنه:" كل عون في وظيفة عمومية دائمة ورسم في السلم الإداري".[1]

أما الموظف العمومي في نظر القانون الجنائي، فهو ما جاءت به الفقرة ب من المادة 02 من القانون رقم 01/06 المتعلق بالوقاية من الفساد[2] ومكافحته بأنه:" يقص بالموظف العمومي:- كل شخص يشغل منصباً تشريعياً أو تنفيذياً أو إدارياً أو قضائياً أو في أحد المجالس الشعبية المحلية المنتخبة سواء كان معيناً أو منتخباً دائماً أو مؤقتاً، مدفوع الأجر أو غير مدفوع الأجر بصرف النظر عن رتبته أو أقدميته.

- كل شخص آخر يتولى ولو مؤقتاً وظيفته أو وكالة بأجر أو بدون أجر ويساهم بهذه الصفة في خدمة هيئة عمومية أو مؤسسة عمومية، أو أية مؤسسة أخرى تملك الدولة كل أو بعض رأسمالها، أو أية مؤسسة تقدم خدمة عمومية.

- كل شخص آخر معرف بأنه موظف عمومي أو من في حكمه طبقاً للتشريع والتنظيم المعلوم بهما.

وهو تعريف مستمد من المادة 02 الفقرة - أ- من اتفاقية الأمم المتحدة لمكافحة الفساد المؤرخة في 31 أكتوبر 2003، ويختلف تماما عن تعريف الموظف العمومي الوارد في الأمر 06-03 المتضمن القانون الأساسي العام للوظيفة العامة، ويشمل كل من الموظف العام في القانون الإداري سواء كان معيناً أو منتخباً، ومن في حكمه كالضابط العمومي ومن يقوم كخدمة عامة.[3]

---

[1]- صدر هذا القانون بموجب الأمر 03/06 المؤرخ في 19 جمادى الثانية عام 0427، الموافق لـ15 يوليو 2006، الجريدة الرسمية عدد 496 الصادرة بتاريخ 20 جمادى الثانية 1427 الموافق لـ 16 يوليو 2006، ص3.

[2]- القانون 01/06. المؤرخ في 20 فبراير 2006، المتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية العدد 14، الصادرة بتاريخ 08 مارس 2006 والذي جاء نتيجة مصادقة الجزائر على اتفاقية الأمم المتحدة لمكافحة الفساد في 19 أفريل 2004، بموجب المرسوم الرئاسي 04-128.

[3]- أما موقف المشرع الفرنسي بخصوص فكرة الموظف العام فكانت أوضح وأشمل حيث لم يذكر في نص الفقرة 4 من 441 من قانون العقوبات عبارة الموظف العام، بل أورد عمارة ممثل ع السلطة العامة والتي تشمل بدورها الموظف العام والضابط العمومي وكذا المكلف بخدمة عامة وهذا بقولها:"...يعاقب على التزوير المرتكب في كتابة عمومية أو رسمية أو تسجيلات تأمر بها السلطة العامة...إذا ارتكب التزوير بواسطة شخص مؤتمن من السلطة العامة أو مكلف بمهمة في مرفق عام أثناء القيام بوظيفته أو مهمته فتكون العقوبة 15 سنة سجن وغرامة مالية تقدر بـ 22500 يورو".

2- التزوير الذي يقع من غير الموظف أو من في حكمه:

لقد نصت المادة 216 من قانون العقوبات الجزائري على معاقبة كل شخص عدا من ذكرتهم المادة 215، ارتكب تزويراً في محررات عمومية أو رسمية بإحدى الطرق الآتية:

1- إما بتقليد أو تزييف الكتابة أو التوقيع.

2- إما باصطناع اتفاقيات أو نصوص أو التزامات أو مخالصات بإدراجها في هذه المحررات فيما بعد.

3- وإما بإضافة أو بإسقاط أو بتزييف الشروط أو الإقرارات أو الوقائع التي أعدت هذه المحررات لتقليها أو لإثباتها.

4- وإما بانتحال شخصية الغير أو المحلول محلها.

في حين نصت المادة 212 من قانون العقوبات المصري على أن:" كل شخص ليس من أرباب الوظائف العمومية ارتكب تزويراً ما هو مبين في المادة السابقة يعاقب بالسجن المشدد أو بالسجن المشدد أو بالسجن مدة أكثرها عشر سنين".

والمقصود بالجاني غير موظف عام هو كل شخص ليس م أرباب الوظائف العمومية، وعلى ذلك يعد الفرد العادي مرتكبا لجريمة تزوير في محرر رسمي وكذلك الموظف يعد مرتكباً تزويراً في محرر رسمي إذا كان بعيداً عن دائرة اختصاصه فوصل إلى المحرر بطريقة غير مشروعه.[1]

وكل هذه الطرق تدخل ضمن طرق التزوير المادي أو المعنوي، وإذا كان الظاهر من نص المادة 216 أنه يطبق على عامة الناس فحسب ولا يسري على الموظفين ومن في حكمهم، فإنه في حقيقة الأمر لا يسري على الموظف ومن في حكمه إذا واقع التزوير أثناء تأديته لوظيفته ويسري عليه في الحالات الأخرى.

ب- مناسبة التزوير:

يجب أن يكون التزوير قد وقع أثناء تأدية الجاني لوظيفته، وبالرجوع للتزوير المعنوي المنصوص عليه في المادة 215 من قانون العقوبات، فلا يمكن تصوره إلا مع توافر هذا الشرط،

[1]- شريف الطباخ، المرجع السابق، ص.ص166،167.

ذلك أن التزوير المعنوي يقع أثناء تحرير المحرر، ولكي يكون المحرر رسميا هنا يجب أن يقوم بتحريره موظف مختص، فالفاعل الأصلي في التزوير المعنوي في محرر رسمي لا يكون إلا الموظف المختص، أما غيره فلا يرتكب التزوير وإنما يكون شريكا فيه، وعندئذٍ يعاقب بالعقوبة المقررة بجريمة الموظف وفقا للمادتين 42 و215 عقوبات.

أما بالنسبة للتزوير المادي الذي يقع من الموظف المختص فإنه نادراً ما يحصل أثناء تحرير المحرر، والمنصوص عليه في المادة 214 من قانون العقوبات،[1] فغالباً ما يتم بعد تحرير المحرر بالمحو أو بالإضافة أو الاصطناع.[2]

فالتزوير المادي فقد يقع أثناء التحرير أو بعده، وعليه فالأمر لا يتوقف على أن يرتكب هذا التزوير الموظف بتحريره، بل قد يرتكبه موظف آخر أثناء تأديته عمله ولكنه غير مختص بكتابته.

الفرع الثاني: جرائم التزوير في المحررات الأخرى

علاوة على تزوير المحررات الرسمية أو العمومية، نص قانون العقوبات على صور أخرى للتزوير تتمثل في التزوير في بعض الوثائق الإدارية والشهادات إضافة إلى التزوير في المحررات العرفية أو التجارية أو المصرفية.

لذا سنقسم الدراسة إلى قسمين نخصص الأول لبيان التزوير في بعض الوثائق الإدارية والشهادات، في حين نخصص القسم الثاني للتزوير في المحررات العرفية أو التجارية أو المصرفية.

أولاً- جرائم التزوير في بعض الوثائق الإدارية والشهادات

تنص المواد من 222 إلى 228 من قانون العقوبات الجزائري[3(*)] على صور مختلفة لتزوير الوثائق الإدارية والشهادات، وقد اعتبر القانون هذه الأفعال جنحا وقرر لها عقوبات أخف من عقوبة

---

[1]- نصت على ذلك المادة 214 بقولها:<<...أثناء تأدية وظيفته>>.

[2]- أحسن بوسقعية، الوجيز في القانون الجزائي الخاص، الجزء الثاني، المرجع السابق، ص425.

[3]- تنص المادة 222 من قانون العقوبات الجزائري على أن:" كل من قلد أو زيف رخصا أو شهادات أو كتابات أو بطاقات أو نشرات أو إيصالات أو جوازات سفر أو أوامر خدمة أو وثائق سفر أو تصاريح مرور أو غيرها من الوثائق التي تصدرها الإدارات العمومية بغرض إثبات حق أو شخصيته أو صفة أو منح إذن يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من 20،000 إلى 100.000 دج".

التزوير في المحررات الرسمية، وهذا ما سنراه لاحقا مع أن بعضها تنطبق عليه صفات التزوير في المحررات الرسمية، ومع ذلك خطورة التزوير في هذه الأحوال أقل خطورة من الأحوال الأخرى.

وقد نصت المادة 222 من قانون العقوبات الجزائري على إصدار عقوبة الحبس والغرامة على كل من قلد أو زيف أو زور رخصاً أو شهادات وغيرها من الوثائق التي تصدرها الإدارات العمومية.[2]

ولتوضيح ذلك سنحاول بيان معنى الوثائق الإدارية والشهادات، وكذا عناصر قيام جريمة التزوير فيها.

1- تحديد معنى الوثائق الإدارية والشهادات:

إن المشرع الجزائري لم يضع تعريف محدد للوثائق الإدارية واكتفى فقط بالإشارة إلى بعض منها. فعلى سبيل المثال المادة 222 بقوله ...أو غيرها من الوثائق التي تصدرها الإدارات العمومية بغرض إثبات حق أو شخصية أو صفة أو منح إذن.....[1].

أشارت المادة 222 إلى بعض الوثائق على سبيل المثال:

- الرخص: ومنها رخص القنص والصيد وحمل السلاح وكذا رخصة السياقة.
- الشهادات: وتتسع هذه العبارة لتشمل كل الوثائق التي تصدرها الإدارات العمومية بالشهادات الطبية.
- الدفاتر: ومنها الدفتر العائلي والدفتر العسكري.
- البطاقات: وأهمها بطاقة التعريف الوطنية.
- النشرات: ومن هذا القبيل نشرة الأحوال الجوية ونشرة الأنباء، والنشرة الطبية وكذا مذكرة -إرسال وبيان الأمتعة وبيان إبداع وبيان الشخص وبطاقة الانتخاب.
- الإيصالات: وهي أوراق تثبت فيها الإدارة توصلها بوثائق من صاحبها.
- جوازات السفر: سواء كانت العادية أو البيومترية.
- أوامر المهمة ويقصد لها أوامر المهمة الصادرة عن الإدارات والمؤسسات العمومية.

ولهذا يمكن القول أنه ليس من الصعب أن نقتبس من هذه المادة تعريفا مناسبا لما يسمى بالوثائق الإدارية، فنقول أن الوثائق الإدارية هي تلك الوثائق التي تصدر عن السلطات الإدارية

[1]- /للمزيد أنظر أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الثاني، المرجع السابق، ص426،427، وأنظر أيضا" جمال نجيمي، المرجع السابق، ص 433.

المركزية أو الإقليمية، ويكون الغرض من إصدارها إثبات حق أو شخصية، أو صفة أو تثبت منح إذن مثل جواز مثل جواز السفر، وبطاقة التعريف الوطنية والدفتر العائلي.[1]

وأما بالنسبة لتحديد معنى الشهادة ومدلولها فإنه يمكن القول أنها تعني كل الشهادات التي تصدر عن السلطات القضائية مثل شهادة الجنسية وشهادات الطعن بالاستئناف أو بالنقض في الأحكام والقرارات، كما تعني تلك الشهادات التي تصدرها السلطات الإدارية المركزية أو المحلية مثل شهادة الإعفاء من الضريبة أو شهادة الميلاد ومثلها الرخص التي تمنح للغير مثل رخصة السياقة...كما تعني أيضا الشهادات التي تمنحها الأطباء لإثبات مرض أو التعافي منه أو غيرها، وشهادات الإقامة أو الإطعام في المحلات المعدة لذلك مثل الفنادق والمراكز الجامعية وما يشابهها.[2]

وفيما يتعلق بطبيعة الإدارة التي تصدر عنها الوثائق الإدارية فإن المادة 222 من قانون العقوبات الجزائري لم تحدد طبيعة هذه الإدارة، كذلك الأمر بالنسبة لقانون العقوبات الفرنسي، إلا أنه وبالرجوع للقضاء الفرنسي فإن الغرفة الجنائية لمحكمة النقض أصدرت في عدة قرارات لها بأنه لا يراد منها الإدارة العامة الوطنية فحسب، بل كذلك الأجنبية وأكثر من ذلك قررت أنه ليس فحسب الإدارة المتعلقة بالدولة والتي تؤخذ بعي الاعتبار بل كذلك الإدارة العامة المستقلة ذاتياً.[3]

وعنصر القصد الجنائي يعتبر من المسائل الموضوعية التي تدخل في سلطة تقرير قاضي الموضوع ولا تخضع لرقابة المحكمة العليا التي تعتبر محكمة قانون فإن انتقاء قيام أحد هذه العناصر أو إغفاله سهواً أو عمداً أو جهلاً يؤدي حتما إلى انتقاء قيام الجريمة ويجعلها كأن لم تكن.[4]

وعليه فلقيام الركن المعنوي في هذه الجريمة فلا بد من توفر القصد الجنائي العام الذي يقوم على إرادة التزوير مع العلم أنه يرتكب على وثائق محمية قانوناً ويتسبب بضرر ممكن.[5]

---

[1]– عبد العزيز سعد، المرجع السابق، ص40.

[2]– عبد العزيز سعد، ص41.

[3]– cass,crim,22mai 1997,n°=96-82,080, voir: Marc segonds, faux juris classeur art 441/1-12, la signature électronique, première réaléserions après la publication de la directive du 13/12/1999 et la loi de Mars 2000, Gaspal 19-20 juillet 200,200,n°=12,520.

[4]– عبد العزيز سعد، المرجع السابق، ص43.

[5]– الهام بن خليفة، المرجع السابق، ص171.

2- عناصر قيام جريمة التزوير في الوثائق والشهادات:

من خلال قراءة المادة 222 من قانون العقوبات الجزائري يمكن اِستخراج العناصر الأساسية لقيام هذه الجريمة والمتمثلة في:

أ- عنصر أو ركن الفعل المادي:

يعتبر الركن المادي من أبرز العناصر المكونة للجريمة ويتحقق هذا العنصر لمجرد قيام المتهم بمباشرة أي فعل من أفعال التقليد أو التزوير أو التزييف لإحدى الوثائق المذكورة على سبيل المثال.[1]

ب- عنصر كون الوثائق أو الشهادات صادرة عن الإدارة:

لقيام هذه الجريمة يجب أن تكون الوثيقة أو الشهادات المزورة صادرة عن مؤسسة إدارية عامة أو جهة لها صلاحية في إصدار الشهادة محل التزوير.

ج- عنصر المصلحة:

بالرجوع إلى الفقرة الأولى من المادة 222 من قانون لا العقوبات نجد أنه يستلزم لقيام هذه الجريمة أن يكون الغرض من أفعال التزوير بواسطة التقليد أو التزييف أو التزوير هو الحصول على حق أو إثبات شخصيته أو صفة، أو منح إذن.

د- عنصر القصد الجنائي:

إن عنصر القصد أو العمد في جريمة تزوير الوثائق والشهادات يتطلب إثبات إرادة المتهم في تغيير الحقيقة، مع علمه بأن ما يقوم به من تغيير، وأن تتجه إرادة الفاعل إلى تغيير هذه الحقيقة

[1]- التقليد يكون بإنشاء وثيقة إدارية أو شهادة غير صحيحة وغير حقيقية تشبه وتماثل تماماً وثيقة إدارية أو شهادة في شكلها وفي مضمونها بحيث ينخدع بها الشخص العادي ويعتقد أنها وثيقة صحيحة، في حين التزييف هو كل عمل يؤدي إلى وضع بيانات ووقائع كاذبة مكان وقائع صحيحة وصادقة، أما تزوير الوثائق الإدارية والشهادات المشار إليها في المادة 222 من قانون العقوبات فيعني كل تغيير مادي أو معنوي بأية طريقة من الطرق بحيث يحول الوثيقة أو الشهادة من الشخص أو الغرض القانوني الذي وضعت من أجله إلى غرض آخر أم إلى شخص آخر/ عبد العزيز سعد، المرجع السابق، ص42.

بإحدى الطرق المبنية في القانون، وبالتالي تتجه إرادة الجاني إلى استعمال الوثيقة أو الشهادة فيما زور من أجله.[1]

وتجدر الإشارة إلى أنه وبالرجوع إلى نص المادة 222 من قانون العقوبات الجزائري وكذلك الفقرة 2 من المادة 441 نجد أنها جاءت بصياغة عامة فلم تحدد صفة مرتكب الجريمة، كما لا تتحدث عن الضرر الناتج من التزوير وهنا يثور التساؤل هنا عن مدى إمكانية تطبيق النص العام للتزوير الذي يحدث ضرراً عن تزوير الوثائق الإدارية؟

لقد اكتفى القضاء الفرنسي بضرورة تحقق الضرر أو احتماله تحققه في جريمة تزوير جواز السفر، أما باقي الوثائق فتزويرها لا ينجم عنه ضرر،[2] ويرى أغلب الفقه الفرنسي أن كل الجرائم ضد الثقة العامة ينتج عنها ضرر وأن تنص عليه المادة 441 في فقرتها الثانية إلا أنه يستنتج بطريقة ضمنية، ولقد أخذ القضاء بما ذهب إليه الفقه في عدة قرارات له.[3]

3- تزوير الوثائق الالكترونية:

إن الوثائق الالكترونية غير محصورة باعتبار أنها مرتبطة بالتطور التكنولوجي، والعالم الرقمي الذي يشهد تطور مستمراً.وتتخذ البطاقات الالكترونية أشكالاً متعددة ووظائف مختلفة، كما أنها قد تصدر عن جهات حكومية أو مؤسسات مالية خاصة من أجل المبادلات التجارية أو الاستفادة من بعض الخدمات ومن بينها البطاقات البنكية أو المصرفية.

وسنحاول التطرق إلى نماذج فقط من هذه الوثائق والتي يتم تداولها بكثرة في المعاملات الالكترونية كجواز السفر الالكتروني وبطاقات الشفاء الالكترونية، وذلك ببيان مدى تجريم تزويرها وذلك في النقاط التالية:

أ- تزوير جواز السفر الالكتروني:

يعد جواز السفر الالكتروني وثيقة تعريف وسفر عالية الأمان تحمل صورة وبصمات رقمية وخصائص بيومترية لصاحبها مخزنة ضمن شريحة الكترونية، حيث تسمح هذه الشريحة بقراءة الجواز

[1]- علي محمد قاسم الطلي، المرجع السابق، ص42.

[2]- Mare segonds, op,cit,p21.

[3]- Loc,cite,méne page.

الكترونيا وبشكل سريع للتعرف على هوية الشخص عند السفر، كما تسمح بالتأكد من صحة البطاقة كونها تتضمن المعطيات الشخصية مثل الاسم وتاريخ الميلاد ورقم الجواز وغيرها.[1]

ويعتبر جواز السفر البيومتري هو ذاته جواز السفر المنصوص عليه في المادة 222 من قانون العقوبات الجزائري السابق ذكرها، وقد عرفته المادة 02 من القانون 03/14/4 المتعلق بسندات ووثائق السفر[2] بأن جواز السفر الذي يلزم بحمله كل مواطن يسافر إلى الخارج هو جواز سفر من نوع بيومتري الكتروني/ أو قابل للقراءة بالآلة.[3]

ويثار التساؤل هنا حول مدى تجريم تزوير هذه الوثيقة وما هو القانون المطبق؟

بالرجوع إلى قانون العقوبات وتحديداً المواد من 394 مكرر إل 394 مكرر 8 ضمن القسم السابع مكرر والتي تعاقب على كل إدخال بطريق الغش في نظام المعالجة الآلية وإزالة بطريق الغش للمعطيات التي يتضمنها.[4]

وعليه فمن خلال هذه المواد نستنتج أن التزوير الذي يقع على النظام البيومتري أو الالكتروني تطبق عليه الأحكام والعقوبات المنصوص عليها في قانون العقوبات والواردة في المواد أعلاه.

وهذا ما أكدته المادة 17 من القانون 03/14 المتعلق بسندات ووثائق السفر إذ تعاقب على كل تزوير أو التحريف أو إتلاف لوثيقة عقوبات منصوص عليها في قانون العقوبات لا سيما المنصوص عليها في المواد 394 مكرر إلى 394 مكرر.

---

[1]– براهمي حنان، المرجع السابق، ص103.

[2]– القانون 03/14 المؤرخ في 24 ربيع الثاني 1435 الموافق لـ 24 فبراير 2014 المتعلق بسندات ووثائق السفر، الجديدة الرسمية، العدد 16، الصادر بتاريخ 21 جمادى الأول 1435 الموافق لـ 23 مارس 2014، ص04 وما بعدها.

[3]– تنص المادة 03 من 03/14 على أنه:<<يجب على كل مواطن يسافر إلى الخارج أن يكون حاملاً لإحدى سندات السفر الآتية:جواز سفر، جواز سفر، جواز دبلوماسي، جواز سفر المصلحة، إن جوازات السفر المذكور في الفقرة الأولى أعلاه هي من نوع بيومتري الكتروني/ أو قابل للقراءة بالآلة...>>.

[4]– تنص المادة 394 مكرر على أنه:" يعاقب بالحبس من ثلاثة أشهر (3) إلى سنة (1) وبغرامة من 20،000 إلى 200،000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذ ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة".

والملاحظ على هذه المادة أن المشرع من خلال هذا القانون ميز بين التزوير في المحررات الالكترونية والتزوير الرافع على البيانات المخزنة على النظام البيومتري الالكتروني، فأحال التزوير الذي يقع على تزوير السفر البيومتري إلى نصوص التزوير، أما التزوير الواقع على النظام البيومتري الالكتروني فتطبق بشأنه العقوبات المنصوص عليها في المواد من 394 مكرر إلى 394 مكرر8.[1]

لكن بالرجوع إلى نص المادة 18 من القانون 03/14 نجدها تحيل كل من يتخذ من وثيقة سفر أو يقوم بمحاولة الاستعمال المزور لجواز سفر الغير يتعرض إلى العقوبات المنصوص عليها في المادتين 222 و223 من قانون العقوبات.[2]

وهنا نستشف الغموض وعدم دقة هذه النصوص، فالمادة 17 لم تبين المقصود من جواز السفر هل تقصد به جواز السفر باعتباره محرر رسمي أو عمومي أم أنه وثيقة صادرة عن إدارة عمومية؟ وبطبيعة الحال هنا يختلف القانون المطبق، فتطبق أحكام المواد من 214 إلى 216 في الحالة الأولى، في حين نطبق أحكام المادتين 222،223 في الحالة الثانية كما أن الفقرة 02 من ذات المادة اعتبرت أن الفعل يعتبر مساساً بنظام المعالجة الآلية للمعطيات وتحيلنا إلى تطبيق العقوبات المنصوص عليها في قانون العقوبات لا سيما تلك المنصوص عليها في المواد 394 مكرر 1 إلى 394 مكر 8 وبالتالي فهذه بالنصوص غير واضحة وغير دقيقة ويتعين على المشرع وضع حد لازدواجية النصوص في مثل هذه النصوص.

---

[1]– تنص المادة 17 من القانون 14–03 على مايلي:" كل شخص يزور أو يقلد أو يحرض أو يتلف عمداً سنداً أو وثيقة سفر أو يستعمل عمداً سنداإص أو وثيقة سفر مزورة أو محرقة يتعرض إلى العقوبات المنصوص عليها من قانون العقوبات".

وإذا مست الأفعال المذكورة أعلاه البيانات المخزنة في النظام البيومتري الالكتروني فتطبق العقوبات المنصوص عليها في قانون العقوبات لا سيما للمنصوص عليها في المواد 394 مكرر 1 إلى مكرر 8...".

[2]– تنص المادة 18 من القانون 03/14 على مايلي:<<كل شص يتخذ من أي سند أو وثيقة السفر حالة مدنية غير حقيقية أو يستعمل سنداً أو وثيقة سفر مسلمة تحت حالة مدنية غير حالته المدنية أو يستعمل حالة مدنية أخرى غير حالته المدنية أو يقوم بمحاولة الاستعمال المزور لجواز سفر الغير، يتعرض إلى العقوبات المنصوص عليها في المادتين 222 و223 من قانون العقوبات".

ب- تزوير بطاقة الشفاء الالكترونية:

كل المواطنين المؤمنين اجتماعياً تمكنهم الحصول على بطاقات الضمان الاجتماعي الالكترونية الصادرة عن الإدارة العامة ومسلمة من هيئات الضمان الاجتماعي.

وقد نظم هذه البطاقات القانون 01/08 المعمم للقانون 1/83 المتعلق بالتأمينات الاجتماعية.[1]

وقد عالج القانون 01/08 مسألة تزوير بطاقات الشفاء الالكترونية وهذا في المادة 93 مكرر 3 كل من يقوم بطريق العش بتعديل أو حذف كلي أو جزئي للمعطيات سواء التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعياً.[2]

كما نصت المادة 93 مكرر 04 على التزوير بطريق النسخ أو الصنع أو الحيازة بطريقة غير مشروعة للبطاقات الالكترونية للمؤمن له اجتماعيا.

ثانياً- جرائم التزوير في المحررات العرفية أو التجارية أو المصرفية:

نصت المادة 219 من قانون العقوبات على التزوير في التجارية أو المصرفية ونصت المادة 220 على التزوير في المحررات العرفية، وتتفق هاتان الصورتان من صور التزوير مع تزوير المحررات الرسمية أو العمومية في طرق التزوير، حيث اشترطت المادتان 219 و220 أن يتم التزوير فيهما بإحدى الطرق المنصوص عليها في المادة 216 وهو النص المتعلق بالتزوير في المحررات الرسمية أو العمومية المرتكب من غير الموظفين ومن في حكمهم. ولتفصيل ذلك سنتطرق إلى التزوير في المحررات التجارية أو المصرفية في الجزء الأول، في حين تخصص الجزء الثاني لبيان التزوير في المحررات العرفية وهذا على النحو الآتي:

---

[1]- تنص المادة 06 مكرر من القانون 01/08 المؤرخ في 15 محرم 1429 المواقف لـ 23 يناير 2008، المتمم للقانون 11/83 المؤرخ في 21 رمضان 1403 الموافق لـ 02 يوليو 1983 المتعلق بالتأمينات الاجتماعية على أنه:<<تثبت صفة المؤمن له اجتماعيا ببطاقة الكترونية...>> أنظر الجريدة الرسمية للجمهورية الجزائرية، العدد 04 المؤرخة في 19 محرم عام 1429هـ- الموافق لـ 27 يناير 200، ص4 وما بعدها.

[2]- تنص إلى 93 مكرر 3 على أنه:<< دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين (2) 'لى خمس (5) سنوات، وبغرامة من 50.000دج إلى 100.000 دج كل من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية/ أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعياً أو في المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهني الصحة...>>.

1- التزوير في المحررات التجارية أو المصرفية:

إن معنى أو مفهوم المحررات التجارية أو المصرفية يصدق على كل الوثائق المتبادلة بين التجار وبين المصارف أو البنوك، سواء من أجل دفع مبالغ مالية أو سحبها أو تحويلها، ويعتبر من المحررات التجارية أو المصرفية جميع أنواع الشيك والسفتجة والكمبيالة والدفاتر التجارية، وكل ما يتعلق بوثائق وسندات الشخص والتفريغ والإخراج من الميناء وشهادات التخزين.[1]

كما قضي في فرنسا بأن المحررات المتعلقة بالتجارة التي يصدرها أو يتبادلها التجار فيما بينهم كالمراسلات بما فيها من طريق التلغرام تعد محررات تجارية.[2]

ويخضع التزوير في هذه المحررات إلى الأركان العامة للتزوير، فأول عنصر يتطلب القانون توفره لقيام هذه الجريمة هو فعل تغيير الحقيقة في هذا المحرر وإحداث تزوير فيه سواء بتزوير التوقيع نفسه أو بوضع شيء كاذب مكان آخر صحيح مع اشتراط أن يقع التزوير وفقا لإحدى الطرق المنصوص عليها في المادة 216 من قانون العقوبات الجزائري.

كما أن من أهم عناصر قيام الجريمة المنصوص عليها في الفقرة الأولى من المادة 219 من قانون العقوبات هو كون المحرر محل الجريمة هو محرر تجاري أو مصرفي وليس محرراً عمومياً أو رسمياً ولا وثيقة من الوثائق الإدارية أو الشهادات.[3]

إلا أن أهم ما يميز هذه الجريمة هو أنها قد ترتكب من الأفراد العاديون ومن بينهم الموظفون خارج مجال عملهم والتجار والشركات التجارية سواء التابعة للقطاع العام أو القطاع الخاص، وقد ترتكب من طرف البنوك و المصارف بمختلف أنواعها.[4]

إضافة إلى هذا لابد من توفر عنصر القصد أو النية الجريمة المستخرج عادة من توجه المتهم ومن إرادته للفعل مع علمه أن ما يقوم بتزويره هو وثيقة تجارية أو مصرفية، ويعد من المسائل التي

---

[1]- عبد العزيز سعد، المرجع السابق، ص52.

[2]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الثاني، المرجع السابق، ص434.

[3]- تنص الفقرة الأولى من المادة 219 على أنه:" كل من ارتكب تزويراً بإحدى الطرق المنصوص عليها في المادة 216 في المحررات التجارية أو المصرفية أو شرع في ذلك يعاقب بالحبس من سنة إلى 5 سنوات وبغرامة من 20.000 إلى 100.000 دينار...".

[4]- جمال نجيمي، المرجع السابق، ص426.

يكون لقاضي الموضوع سلطة تقديرية في استخلاصه وإثبات توفره÷ وبدوه تكون العناصر الجرمين ناقصة.[1]

ويجوز فضلا عن ذلك، رفع عقوبة الحبس إلى عشر سنوات إذا كان مرتكب الجريمة أحد مجال المصارف أو مدير شركة وعلى العموم أحد الأشخاص الذين يلجئون إلى الجمهور بقصد إصدار أسهم أو سندات سواء كانت لشركة أو مشروع تجاري أو صناعي، مع الملاحظة أن وصف الجريمة يبقى دائما وصفاً جنحياً حتى ولو تجاوزت العقوبة الحد الأقصى للجنحة وأصبحت عقوبة جنائية.[2]

أما بخصوص الأوراق أو المحررات التجارية المنصوص عليها في القانون التجاري الجزائري والمتمثلة في السفاتج والسندات الأمر وسندات السحب وسندات التخزين وعقود تحويل الفواتير، وكذا الشيكات فإن تقديمها يكون قد يكون ماديا، كما قد يكون الكترونيا بأي وسيلة تبادل الكترونية محددة في التشريع المعمول به.[3] وبالتالي فكل هذه السندات قد تكون الكترونية وتعد هي أيضا أداة للوفاء وانتقال المال إلا أنها تختلف تماما عن الأولى، إذ أن هذه الأخيرة وهي الكتابة الرقمية قد تتم في شكل رموز أو بيانات يتم إنشاؤها وتخزينها وإرسالها عن طريق وسائط الكترونية.[4]

كما قد أتاحت شبكة الأنترنت طرقا عديدة بخصوص الدفع والأداء للثمن ومنها الدفع الفوري عند الاستلام أو استخدام البطاقات البنكية، البطاقات الذكية النقود الرقمية والبطاقات البلاستيكية أو المغناطيسية التي تخزن بها البيانات الخاصة بالعميل وبالتالي إحلال العمولات الالكترونية محل

---

[1]– عبد العزيز سعد، المرجع السابق، ص54.

[2]– نصت على هذا الفقرة من المادة 219 قانون العقوبات الجزائري بقولها:" ويجوز أن يضاف الحد الأقصى للعقوبة المنصوص عليها في الفقرة الأولى وإذا كان مرتكب الجريمة أحد رجال المصارف أو مدير شركة وعلى العموم أحد الأشخاص الذين يلجئون إلى الجمهور بقصد إصدار أسهم أو سندات أو حصص أو أية سندات سواء كانت لشركة أو مشروع تجاري أو صناعي".

[3]– ثم قبول التعامل بالوسائل الالكترونية بموجب القانون 02/05 المؤرخ في 06 فبراير 2005 المعدل والمتمم للأمر 59/75 المؤرخ في 26 سبتمبر 1975 المتضمن للقانون التجاري الذي يعدل نص المادة 414 والتي أصبحت تنص على مايلي:<<...يعتبر التقديم المادي للسفتجة لغرفة المقاصة بمثابة تقديم للوفاء، يمكن أن يتم هذا التقديم أيضا بأي وسيلة تبادل الكترونية محددة في التشريع والتنظيم المعمول بها...>>، الجريدة الرسمية للجمهورية الجزائرية، العدد 11، المؤرخة في 30 ذي الحجة 1425 الموافق لـ09 فبراير 2005، ص8.

[4]– زبيحة زيدان، المرجع السابق، ص36.

العملات التقليدية في الممارسة التجارية في شكل محفظة الكترونية (بطاقة ذكية) يمكن تثبيتها على الحاسوب الشخصي أو قرص مرن يتم إدخاله في فتحه القرص المرن في الحاسوب الشخصي ليتم نقل القيمة المالية منه وإليه عبر شبكة الأنترنت.[1]

أما بخصوص التزوير الواقع على هذه الأوراق، فنطبق عليه الأحكام الخاصة بالتزوير، فمثلا بخصوص التزوير الواقع على الشيكات فقد أفرد له قانون العقوبات الجزائري نصاً خاصاً بموجب المادة 375 التي تعاقب على كل من زور أو زيف شيكاً، كما تعاقب كل من استلم شيكاً مزوراً أو مزيفاً وهو عالماً بذلك.[2]

كما أن البطاقات البنكية الالكترونية للدفع أو السحب كإحدى وسائل الدفع الالكترونية المستحدثة في القانون التجاري الجزائري قد تكون محلاً لبعض الأفعال الإجرامية، حيث تكون محلاً لارتكاب أفعال التزوير، وبالتالي تسري عليها أحكام تزوير المحررات العرفية المصرفية على البطاقات البنكية دون حرج وذلك بعد التعديلات التي ادخلها المشرع الجزائري على ترسانته القانونية منذ 2004 في قانون العقوبات وكذا القانون المدني والقانون 04/15 المتعلق بالتوقيع الالكتروني، وبالتالي أقر بمبدأ التعامل الوظيفي بين المحررات التقليدية وتلك الالكترونية وساوى بينهما في حجة الإثبات.[3]

2- التزوير في المحررات العرفية:

المحررات العرفية هي الأوراق التي يحررها أصحاب الشأن من ذات أنفسهم دون أن يتدخل الموظف العام في تحريرها، بعكس المحررات الرسمية التي يتولى تحريرها الموظف العام، وبعبارة أكثر توضيح فإن المحرر العرفي هو كل محرر لا تنعقد له صفات المحرر الرسمي.[4]

---

[1]- نفس المرجع، ص،ص39،38.

[2]- تنص المادة 375 من قانون العقوبات الجزائري على أنه:<يعاقب بالحبس من سنة إلى عشر سنوات وبغرامة لا تقل عن قيمة الشيك أو النقص في الرصيد:

1- كل من زور أو زيف شيكاً.

2- كل من قبل استلام شيك مزور أو مزيف مع علمه بذلك>>.

[3]- بن حديد سامية، الحماية الجنائية لبطاقات الدفع من جرائم التزوير في القانون الجنائي الجزائر، مجلة دراسات، جامعة الأغواط، الجزائر، 2017، العدد57، ص220.

[4]- علي محمد قاسم الطلي، المرجع السابق، ص37.

فالمحرر العرفي هو كل محرر ليست له الصفة الرسمية، أي كل محرر لا يقوم بتحريره موظف مختص بذلك بمقتضى القوانين واللوائح،[1] ويعتبر المحرر عرفيا ولو نعته صاحبه كذباً بأنه محرر رسمي وأسند صدوره إلى موظف عام مادام الظاهر من عباراته أنها لم تصدر منه أو إنها خرجت من اختصاصه.

ويعد من المحررات العرفية المحررات التي يحررها الأفراد أي القرارات والمخالصات والتصرفات والعقود والوصايا، كما يعتبر المحرر عرفيا حتى ولو اجتمع في ورقة واحدة مع محرر رسمي، حيث يبقى لكل منهما حكمه ووضعه الخاص به.[2]

تنقسم المحررات العرفية إلى قسمين: محررات عرفية محددة للإثبات: وهو تلك التي تصدر من ذوي الشأن وتكون موقع من قبلهم كالأوراق المعدة لإثبات التصرفات القانونية من بيع وإيجار، وهناك المحررات العرفية غير المعدة للإثبات والتي غالبا لا تكون موقع عليها من قبل ذوي الشأن، ومع ذلك لها حجية في الثبات كدفاتر التجار والدفاتر والأوراق المنزلية والرسائل والبرقيات

ولا يشرط القانون صفة خاصة في المحرر العرفي لكي يعتبر تزويراً فإذا ما توفرت بقي شروط التزوير من حيث ترتيب الضررً أو احتماله و القصد الجنائي الذي يتحقق بتغيير الحقيقة في هذا المحرر تغييراً يؤدي إلى حدوث ضرر وأن يكون هناك قصدا مسبقا لاستعمال هذا المحرر فيما أعدله.[3]

والتزوير في المحررات العرفية هو الفعل المنصوص والمعاقب عليه في المادة 220 من قانون العقوبات الجزائري،[4] وتتمي هذه الصورة عن باقي صور التزوير الأخرى من حيث محل الجريمة إذ ينصب التزوير في هذه الصورة على محرر عرفي.

---

[1]– شريف الطباخ، المرجع السابق، ص170.

[2]– رؤوف عبيد، المرجع السابق، ص156.

[3]– محمد علي قاسم الطلي، المرجع السابق، ص37.

[4]– تنص المادة 220 من قانون العقوبات الجزائري على أنه:<< كل شخص ارتكب تزويراً بإحدى الطرق المنصوص عليها في المادة 216 في محررات عرفية أو شرع في ذلك يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 20.000إلى 100.000 دينار...>>.

فالمحرر العرفي هو كل محرر لا يعد محرراً عمومياً أو رسمياً ولا محرر تجارياً أو مصرفياً ولا شهادة أو وثيقة إدارية تثبت حقا أو شخصية أو تمنح إذنا،[1] ولا يتطلب القانون في هذه الصورة صفة خاصة في المحرر، كما لا يشترط أن يكو المحرر صالحاً لإثبات حق أو تخالص أو صفة أو حالة قانونية، فالتوقيع بإمضاء مزور على شكوى أو رسالة يعد من قبيل التزوير في محررات عرفية.[2]

وهناك أيضا المحررات العرفية الالكترونية التي تستخدم عادة في إثبات العقود المدنية التي تبرم عن الطريق الالكتروني وكذا عقود التجارة الالكترونية، سواء كانت تحمل توقيعا الكترونيا مؤمن ومصادق عليه بشهادة الكترونية والتي تكون محمولة على أشرطة ممغنطة أو ميكروفيلم أو قرص صلب أو مرن، وسواء أكان عبر موقع الكتروني مثل رسائل البريد الالكتروني غير الموقعة، إذ لا يمكن التحقق من هوية المرسل ولا سلامة المضمون، إذ تمكن في نصوص الإثبات إثبات التصرفات المدنية بها إذا كانت أقل من 100،000دج، وكذلك إثبات التصرفات التجارية بها.[3]

المبحث الثاني: القواعد الموضوعية لجريمة التزوير الالكتروني على مستوى العقاب

نظراً لخطورة الجرائم الالكترونية بصفة عامة، والتزوير الالكتروني بصفة خاصة قامت التشريعات الوطنية والدولية بفرض عقوبات على كل من يقترفها للحيلولة دون وقوعها، حيث قامت بتجريم مراحل متقدمة يمر بها الجاني قبل أن يصل إلى المرحلة النهائية وارتكاب الجريمة كاملة، ومن الأفعال التي جرمها المشرع وقرر العقاب على مرتكبيها، الاتفاق الجنائي على التحضير والإعداد لارتكاب هذه الجرائم، ونفس الأمر بالنسبة للشروع، كما نص المشرع الجزائري على مساءلة الأشخاص المعنوية في ارتكابهم لمثل هذه الجرائم، والهدف من العقاب على هذه الجرائم هي حماية المصالح المحمية نظراً لتعلقها بالمصلحة العامة فشدد العقوبة إلى ضعف العقوبة للشخص الطبيعي فضلاً عن العقوبات الأصلية التي قررها المشرع لهذه الجرائم كما قرر عقوبات تكميلية.

كما وضعت التشريعات المقارنة نصوصاً خاصة لقمع وعقاب جريمة التزوير الالكتروني الوارد بينها فيما سبق كقانون التوقيع الالكتروني المصري وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري، وكذا قانون المعاملات الالكتروني لإمارة دبي، والتي تبنت مبدأ المسؤولية

[1]– عبد العزيز سعد، المرجع السابق، ص52.

[2]– أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الثاني، المرجع السابق، ص435.

[3]– الهام بن خليفة، المرجع السابق، ص165.

الجنائية عن ارتكاب جرائم التزوير الالكتروني للأشخاص الطبيعية وكذا المعنوية. وهذا ما سنتناوله بالتفصيل في المطالب الآتية:

ومن هنا ارتأينا تقسيم هذا المبحث إلى مطلبين،نخصص المطلب الأول إلى بيان العقوبات المقررة لجريمة التزوير الالكتروني في التشريع الجزائري أما المطلب الثاني نتطرق فيه إلى بيان العقوبات المقررة لجريمة التزوير الالكتروني في التشريعات المقارنة.

المطلب الأول: العقوبات المقررة لجريمة التزوير الالكتروني في التشريع الجزائري

لقد ساير المشرع الجزائري الركب المعلوماتي من خلال تبني نصوص تشريعية حديثة تعالج بعض الجرائم التي قد تمس بنظام المعالجة الآلية للمعطيات بصفة مباشرة، هادفاً من وراء ذلك إلى حماية المكونات المعنوية لهذا النظام، إلا أنه لم يوفق في الإحاطة الشاملة بكل الجرائم الالكترونية، ولعل من أهم هذه الجرائم جريمة التزوير الالكتروني، وإن كانت تكتسي أهمية قصوى .

وفي مجال التزوير الالكتروني، فبالرغم من أن المشرع قد أضفى على الكتابة الالكترونية نفس القيمة الثبوتية للمحررات الورقية، إلا أنه لم يدخل أي تعديل في نصوص التزوير تستوعب تغيير الحقيقة في المحررات الالكترونية ما يحيلنا إلى تناول العقوبات الناشئة عن ارتكاب جريمة التزوير الالكتروني إلى نصوص التزوير التقليدية بالرغم ما تميز به الجريمة الالكترونية من خصوصية تختلف عن الجرائم التقليدية.

وسنحاول من خلال هذا المطلب تحليل العقوبات المقررة لجريمة التزوير الالكتروني بهدف الوصول إلى السياسة العقابية التي انتهجها المشرع الجزائري لمواجهة والحد من هذه الجريمة، سواء كانت هذه العقوبات مقررة للشخص الطبيعي أو المعنوي، وهذا على النحو الآتي:

الفرع الأول: العقوبات المقررة للشخص الطبيعي

سبقت الإشارة إلى أن المشرع الجزائري بخصوص الجزاء المترتب عن تزوير المحررات الالكترونية أحالنا إلى نصوص التزوير في قانون العقوبات، وعليه فإن دراسة هذه الجزاءات ستقودنا لا محالة إلى العقوبات المنصوص عليها نصوص تزوير بعض الوثائق الإدارية والشهادات، وكذا تزوير المحررات العرفية أو التجارية أو المصرفية وهذا على النحو الآتي:

أولاً- العقوبات المقررة لجريمة تزوير الوثائق والشهادات

تعد الوثائق الالكترونية من أهم وسائل المعاملات القانونية المختلفة في وقتنا هذا سواء تلك الصادرة عن الجهات الحكومية أو عن المؤسسات المالية، وتم التطرق فيما سبق إلى أهم نماذج هذه الوثائق والتي يتم تبادلها بكثرة في المعاملات الالكترونية والمتمثلة في جواز السفر الالكتروني أو البيومتري وكذا بطاقات الشفاء الالكترونية، وسنتناول العقوبات المقررة لتزوير هاتين الوثيقتين في النقاط التالية:

أ- العقوبات المقررة لجريمة تزوير جواز السفر الالكتروني

يعتبر جواز السفر البيومتري أو الالكتروني هو ذاته جواز السفر المنصوص عليه في المادة 222 من قانون العقوبات الجزائري، وعليه فإن المشرع الجزائري أحال العقاب على التزوير الواقع على جواز السفر البيومتري إلى نصوص التزوير العامة والمتمثلة في المادتين 222 و223 من قانون العقوبات.

ومن هنا يمكننا أن نقول أن المشرع الجزائري قد قرر لجريمة تزوير جواز السفر الالكتروني عقوبتين أحدهما أصلية والثانية تكميلية، وبالإضافة إلى هذا فقد عاقب على الشروع في هذه الجريمة- وعقوبة مستقلة أيضا تتعلق بمباشرة استعمال مثل هذه الوثائق المزورة.

1- العقوبات الأصلية:

قرر المشرع الجزائري عقوبة بدنية والمتمثلة في الحبس لكل متهم ثبتت إدانته بتهمة ارتكاب جريمة التزوير الواقعة على الوثائق الإدارية ومنها جواز السفر الالكتروني لمدة ما بين ستة أشهر(06) إلى ثلاث(3) سنوات وعقوبة مالية تتراوح ما بين20،000 إلى 100،000 دينار جزائري.

2- العقوبات التكميلية:

بالنسبة للعقوبات التكميلية أو الإضافية، قرر المشرع الجزائري في الفقرة 02 من المادة 222 من قانون العقوبات جواز الحكم على المتهم المدان بالحرمان من حق أو أكثر من الحقوق الوارد

ذكرها في المادة 14 وبالمنع من الإقامة من سنة على الأقل إلى خمس سنوات على الأكثر، أي لمدة لا تقل عن سنة ولا تزويد عن خمس سنوات.[1]

وفيما يتعلق بالحرمان من الحقوق المنصوص عليها في المادة 14 من قانون العقوبات الجزائري، فهي تتمثل في الحرمان من حق أو أكثر من ممارسة الحقوق الوطنية والمدنية والعائلية والتي حصرتها المادة 09 مكرر 01،[2] وذلك بعزل المحكوم عليه وطرده من بعض الوظائف السامية في الدولة وكذا الخدمات التي لها علاقة بالجريمة، إضافة إلى الحرمان من الحقوق السياسية كحق الانتخاب والترشح وحمل الأوسمة وعدم الأهلية لتولي مهام محلف أو خبير أو شاهد أمام القضاء، إضافة إلى الحرمان من الحق في حمل السلاح وتولي مهام في سلك التعليم، وكذلك عدم الأهلية لتولي مهام الوصاية كلها أو بعضها.

وتسري هذه العقوبة من يوم انقضاء العقوبة الأصلية أو الإفراج على المحكوم عليه، كما وضع المشرع عقوبة إضافية أو تكميلية أخرى طبقا لنص المادة 222 والمتمثلة في المنع من الإقامة، وذلك بالحظر المؤقت على المحكوم عليه أن يوجد في أماكن محددة، وذلك لمدة سنة على الأقل وخمس سوات على الأكثر، يبدأ سريانها من يوم الإفراج عل المحكوم عليه وبعد تبليغه قرار المنع من الإقامة.

3- الشروع في ارتكاب جريمة تزوير جواز السفر الالكتروني:

لقد نصت المادة 222 في فقرتها الثالثة على أنه يعاقب على الشروع في جرائم تزوير الشهادات والوثائق بما فيها جواز السفر البيومتري يمثل ما يعاقب على الجريمة التامة.[3]

---

[1]- تنص المادة 14 من قانون العقوبات الجزائري على أنه:<< يجوز للمحكمة عند قضائها في جنحة، وفي الحالات التي يحددها القانون، أن تحظر على المحكوم عليه ممارسة حق أو أكثر من الحقوق الوطنية المذكورة في المادة 9 مكرر 01، وذلك لمدة لا تزيد عن خمس (5) سنوات...>>.

[2]- تنص المادة 9 مكرر 01 من قانون العقوبات الجزائرية على أنه:<< يتمثل الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية في:

1- العزل أو الإقصاء من جميع الوظائف والمناصب العمومية التي لها علاقة بالجريمة.

2- الحرمان من حق الانتخاب أو الترشح ومن حمل أي وسام.

[3]- تنص الفقرة 03 من المادة222 من قانون العقوبات الجزائري على أنه:<<...ويعاقب على الشروع بمثل ما يعاقب به على الجريمة التامة...>>.

ولكن هذه المادة لم تبين متى وكيف يحصل الشروع في أفعال التقليد أو التزوير في الوثائق الإدارية والشهادات فلا مناص من الرجوع إلى القواعد العامة التي تحكم الشروع وتنظيمه.

وبالرجوع إلى المادة 30 من قانون العقوبات نجد أن الشروع هو كل فعل جرمي يؤدي مباشرة إلى تنفيذ أفعال لم تقف ولم يخب أثرها إلا نتيجة لظروف مستقلة عن إدارة المتهم تعتبر كالجريمة التامة،[1] وهذا يعني أن كل فعل جرمي يشرع المتهم في انجازه، ثم يغيب فعله ولم يصل إلى النتيجة التي كان يرغب في حصولها بسبب خارج عن إرادته يعتبر مدينا ويمكن معاقبته بنفس العقوبة المقررة للفعل التام.

وتجدر الإشارة أنه وبالرجوع لنص المادة 31 من قانون العقوبات في فقرتها الأولى نجد أن المشرع لا يعاقب على المحاولة في الجنحة إلا بناء على نص صريح في القانون، وبما أن جريمة التزوير في الوثائق والشهادات تأخذ وصف الجنحة، فإنه لا يمكن العقاب على الشروع فيها إلا إذا نص على وجوب ذلك.[2]

ب- العقوبات المقررة لجريمة تزوير بطاقات الشفاء الالكترونية:

بعد صدور القانون 01/08 المتمم للقانون 11/83والمتعلق بالتأمينات الاجتماعية والذي جاء بدوره منظما لبطاقات الشفاء الالكترونية، والذي عالج مسألة تزوير هذه البطاقات وذلك في المادة 93 مكرر 03 والتي تعاقب على كل من يقوم بطريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية المدرج في هذه البطاقة.[3]

---

[1]- تقضي المادة 30 من قانون العقوبات الجزائري بأنه:<<كل المحاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ وبأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية ذاتها إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إدارة مرتكبها حتى ولو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها>>.

[2]- في حي تنص المادة 31 من قانون العقوبات على أنه:<< المحاولة في الجنحة لا يعاقب عليها إلا بناء على نص صريح في القانون...>>.

[3]- تنص المادة 93 مكرر 03 من القانون 01/08المتمم للقانون 11/83 المتعلق بالتأمينات الاجتماعية على أنه:<<...دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين إلى (02) إلى خمس (05) سنوات وبغرامة من 500،000 دج إلى 1،000،000 دج كل من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية /أو الإدارية المدرجة في البطاقة الالكترونية...>>.

أما العقوبات التي قررتها هذه المادة فهي الحبس من سنتين إلى خمس سنوات وبغرامة مالية 500،00 دج إلى 1،000،000دج، وهذا دون الإخلال بالعقوبات المنصوص عليها في قانون العقوبات.

وقد جاءت العقوبة المقررة في المادة أعلاه أشد من العقوبات المنصوص عليها في المادتين 222 و223 من قانون العقوبات.

وقد نصت الفقرة الأخيرة من المادة 93 مكرر03 على أنه تطبق نفس العقوبة على كل محاولة لارتكاب هذه الجنحة.

وإضافة للمادة 93 مكرر03 فقد نصت المادة 93 مكرر04 على عقوبة الحبس من سنتين (02) إلى خمس (05) سنوات، وكذا الغرامة المالية من 50،000 إلى 100،000دج لكل من يفسخ أو يصنع أو يحوز أو يوزع هذه البطاقات الالكترونية بطريقة غير مشروعة.[1]

ثانياً- العقوبات المقررة لجريمتي التزوير في المحررات التجارية أو المصرفية والعرفية:

بالرجوع إلى نصي المادتين 219،220 نجد أن المشرع قد وضع عقوبات على جريمتي تزوير المحررات التجارية أو المصرفية، وكذا العرفية، تطبق على مرتكبها سواء أتمها أو شرع فيها وهذا ما سنوضحه فيمايلي:

أ- العقوبات المقررة لجريمة التزوير في المحررات التجارية أو المصرفية:

لقد نص المشرع الجزائري في المادة 219 على جريمة التزوير في المحررات التجارية والعرفية، ووضح عقوبات لكل من قام بتزويرها، تنوعت هذه العقوبات التجارية والعرفية، ووضع عقوبات لكل من قام بتزويرها، تنوعت هذه العقوبات بين العقوبات الأصلية والتبعية، كما عاقب على كل محاولة لارتكاب مثل هذا الجرم، وهذا ما سنبينه في العناصر الآتية:

[1]- تقضي المادة 93 مكرر 4 من القانون 01/08 المتمم للقانون 11/83 المتعلق بالتأمينات الاجتماعية بأنه:<<دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين (02) إلى خمس (05) سنوات وبغرامة من 50،000 إلى 100،000 دج كل من يفسح أو يصنع أو يحوز أو يوزع بطريقة غير مشروعة البطاقة الالكترونية...>>.

1- العقوبات الأصلية:

لقد عاقبت المادة 219 في فقرتها الأولى كل من ارتكب تزوير بإحدى الطرق المنصوص عليها في المادة 216 في المحررات التجارية أو المصرفية بالحبس من سنة إلى خمس سنوات وبغرامة من 20،000 إلى 100،000 دينار جزائري.

كما شددت الفقرة 3 من ذات المادة العقوبة وضاعفت الحد الأقصى لها إذ كان مرتكب الجريمة أحد رجال المصارف أو مدير شركة أو أحد الأشخاص الذين يلجئون إلى الجمهور بقصد إصدار أسهم أو سندات أو حصص أو أية سندات كانت سواء لشركة أو مشروع تجاري أو صناعي.[1]

وبناءً على ذلك تصبح العقوبة عشر سنوات سجن وغرامة تقدر بـ 200،000 دج، وفي هذه الحالة فإن وصف الجريمة يتحول من جنحة إلى جناية وهذا طبقا لنص المادة 29 من قانون العقوبات والتي تقضي بتغير نوع الجريمة إذا نص القانون على عقوبة تطبق أصلا على نوع آخر أشد منها نتيجة لظروف مشددة.[2]

2- العقوبات التكميلية:

بالنسبة للعقوبات التكميلية أو التبعية، فقد قرر المشرع الجزائري في الفقرة 03 من المادة 219 جواز الحكم على الجاني الحرمان من حق أو أكثر من الحقوق الواردة في المادة 14، وكذا المنع من الإقامة من سنة إلى خمس سنوات على الأكثر،[3] والتي سبق التطرق إليها.

---

[1]- تنص هذه على أنه:<<...ويجوز أ يضاعف الحد الأقصى للعقوبة المنصوص عليها في الفقرة الأولى إذا كان مرتكب الجريمة أحد رجال المصارف أو مدير شركة وعلى العموم أحد الأشخاص الذين يلجئون إلى الجمهور بقصد إصدار أسهم أو سندات أو حصص أو أية سندات كانت سواء لشركة أو مشروع تجاري أو صناعي...>>.

[2]- تنص المادة 219 من قانون العقوبات الجزائري على أنه:<<يتغير نوع الجريمة إذا نص القانون على عقوبة تطبق أصلاً على نوع آخر أشد منها نتيجة لظروف مشددة>>.

[3]- تنص الفقرة 3 من المادة 219 على مايلي:<<...ويجوز علاوة على ذلك أن يحكم على الجاني بالحرمان من حق أو أكثر من الحقوق الواردة في المادة 14 وبالمنع من الإقامة من سنة إلى خمس سنوات على الأكثر...>>.

3- الشروع في ارتكاب جريمة التزوير في المحررات التجارية أو المصرفية:

بما أن المشرع الجزائري لا يعاقب على المحاولة أو الشروع في الجنحة، إلا بناءاً على نص صريح في القانون، لأن المادة 219 من قانون العقوبات نصت على الشروع وعليه فإن القانون يعاقب من بدأ في تنفيذ الجريمة ولم يحقق النتيجة المقصودة بنفس العقوبة المقررة للجريمة التامة.

ب- العقوبات المقررة لجريمة التزوير في المحررات العرفية:

باستقراء المادتين 219 و220 من قانونا العقوبات، نجد أن المشرع يعاقب على جريمتي التزوير في المحررات التجارية أو المصرفية والعرفية بنفس العقوبة إذ تطبق على الجاني عقوبات أصلية، إضافة إلى العقوبات التكميلية وهنا ما سنبينه فيما يلي:

1- العقوبات الأصلية:

تتمثل العقوبة الأصلية لجريمة التزوير في المحررات العرفية في الحبس من سنة إلى خمس سنوات إضافة إلى غرامة مالية تتراوح ما بين 20،000 إلى 100،000دج.[1]

2- العقوبات التكميلية:

تتمثل العقوبات التكميلية لجريمة التزوير في المحررات العرفية، في الحكم على الجاني بالحرمان من حق أو أكثر من الحقوق الواردة في المادة 14 إضافة إلى المنع من الإقامة من سنة إلى خمس سنوات على الأكثر،[2] والتي سبق بيانها.

3- عقوبة الشروع في ارتكاب جريمة التزوير في المحررات العرفية:

نصت الفقرة الأولى من المادة222 على الشروع في ارتكاب جريمة التزوير في المحررات العرفية بنفس العقوبة المقررة للجريمة التامة، سواء. أتم الجاني جريمته أو شرع فيها.

---

[1]- وهذا ما نصت عليه الفقرة 1 من المادة 220 بقولها:<<كل شخص ارتكب تزويراً بإحدى الطرق المنصوص عليها في المادة 216 في محررات عرفية أو شرع في ذلك يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 20.000 إلى 100.000دج.>>.

[2]- وهذا ما أكدته الفقرة 2 من الماد 220 بقولها:<< ويجوز علاوة على ذلك أن يحكم على الجاني بالحرمان من حق أو أكثر من الحقوق الواردة في المادة 14 وبالمنع من الإقامة من سنة إلى خمس سنوات على الأكثر...>>.

الفرع الثاني: العقوبات المقررة للشخص المعنوي

إن التطور الاقتصادي والاجتماعي الحاصل في عصرنا هذا زاد من انتشار الأشخاص المعنوية، كما تعدد تنوع نشاطها وهي بذلك تحقق فوائد كبيرة لأفراد المجتمع، ومع ذلك فإنها تمكن أن تسبب أضراراً تعاقب عليها النصوص الجزائية، وهو ما يجعلها محل مساءلة جزائية عن الجرائم المرتكبة.

وقد أقر المشرع الجزائري بالمسؤولية الجزائية للشخص المعنوي وفقا للقواعد المقررة في القانون العام،[1] واعتبر قانون العقوبات الشخص المعنوي مسئولاً جزائيا عن جرائم التزوير،[2] وعليه تطبق على الشخص المعنوي العقوبات المقررة والمنصوص عليها في المادة 18 مكرر، وعند الاقتضاء تلك المنصوص عليها في المادة 18 مكرر 02 من هذا القانون، كما يتعرض لواحدة أو أكثر للعقوبات التكميلية المنصوص عليها في المادة 18 مكرر.

وسنتناول هذه العقوبات على النحو الآتي:

أولا- شروط تقرير المسؤولية الجزائية للشخص المعنوي:

تنص المادة 394 مكرر 04 من قانون العقوبات الجزائري على أنه:<< يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي>>.

فالأشخاص المعنوية تمكن أن يسألوا جنائيا عن الجرائم المنصوص عليها في هذا القسم وفي الحالات التي نص عليها القانون والتي ارتكبوها لحسابهم أو من طف أعضائهم أو ممثليهم.

والمسؤولية الجنائية للأشخاص المعنوية لا تستبعد الأشخاص الطبيعية فاعلين أو مساهمين الذين ارتكبوا نفس الوقائع.وحتى تمكن استناد التهمة للشخص المعنوي فعلى النيابة العامة أن تثبت أن الجريمة قد ارتكبت من طرف شخص طبيعي معين بذاته، وأن هذا الشخص له علاقة بالشخص

[1]- وهذا ما أكدته الفقرة الأولى من المادة 51 مكرر من قانون العقوبات بقولها:<<باستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام، يكون الشخص المعنوي مسئولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على لذلك...>>.

[2]- وهذا ما أكدته المادة 253 مكرر في فقرتها الأولى:<<يكون الشخص المعنوي مسئولا جزائيا عن الجرائم المحددة في هذا الفصل وذلك طبقا للشروط المنصوص عليها في المادة 51 مكرر من هذا القانون>>.

المعنوي، فشرط مساءلة الشخص المعنوي جزائياً يتمثل في أن يرتكب الفعل الإجرامي من طرف أجهزته أو ممثله القانوني.[1]

وحتى تقوم مسؤولية الشخص من جزائيا لابد من توافر الشروط:

- أن ترتكب الجريمة من أحد أعضاء الشخص المعنوي أو ممثليه.
- يجب أن ترتكب الجريمة لحساب الشخص المعنوي.
- ويسأل الشخص المعنوي بصفة فاعلاً أصليا أو مساهماً (متدخلاً).

وعليه فلا يمكن مساءلة الشخص المعوي إلا إذا أقر المشرع مسؤوليته جزائيا في نصوص جرائم معينة على سبيل الحصر، ويقصد بعضو أو ممثل الشخص المعوي الشخص الذي يمثل أهمية كبيرة في المؤسسة بالنظر إلى الوظيفة التي يحتلها والتي تؤهله لتسيير أمورها والتصرف والتعاقد باسمها ولحسابها والتي تتوقف اِستمراريته المؤسسة على إرادته، ويدخل في هذا المدلول مجموعة شركاء أو أعضاء مجلس الإدارة أو الجمعية العامة،[2] ويترتب على اشتراط أن تكون الجريمة مرتكبة ممن يملك زمام أمور الشخص المعنوي، ألا يسأل هذا الأخير عما يرتكبه من ليست له هذه الصفة حتى ولو ارتكب جريمة من الجرائم المحددة قانونياً، وكون ارتكاب الجريمة لحساب الشخص المعنوي يترتب عليها بمفهوم المخالفة عدم مسائلة الشخص المعنوي عن الجريمة التي تقع من ممثليه إذا ارتكبها لحسابه الشخصي أو لحساب شخص آخر أو وقعت إضراراً بمصالح الشخص المعنوي، إذ يؤاخذ الشخص الطبيعي عنها على أساس جريمة التعسف في استعمال الشركة أو الإفلاس.[3]

ولقد شدد المشرع العقوبة على الشخص المعنوي لأن الكثير من الأشخاص المعنوية تنشأ بغرض تحقيق الربح فتقوم بالمنافسة غير المشروعة لمنافسيها عن طريق ارتكاب هذا النوع من

---

[1]- عبد الرحمان خليفي، إسناد المسؤولية الجزائية للشخص المعنوي في جرائم الأموال، مراحله في إطار فعاليات الملتقى الوطني الأول حول جرائم المالية في ظل التحولات الاقتصادية والتعديلات التشريعية، وقسم العلوم القانونية والإدارية، جامعة 08 ماي 09465 قالمة، الجزائر، يومي 24،25 أفريل 2007.

[2]- Jean-Christophe, saint peau, la présomption d'imputation d une infraction aux organes ou répesrants d une personne morale, recueil , Dalloz,2007,p61/183.

المشار إليه في الهام حليفة، المرجع السابق، ص183.

[3]- محمد مزوالي، المسؤولية الجنائية للأشخاص المعنوية عن الجرائم الالكترونية في القانون الجزائري، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، الجزائر، العدد الأول، 2009،ص392.

الجرائم، حيث يتم الدخول إلى أنظمة الحاسبات المنافسة والاطلاع على ملفاتها وخططها ومنافستها بناء على ذلك، وقد يصل الأمر إلى حد التلاعب بمعطياتها وتزويرها.[1]

ثانياً- أنواع العقوبات المطبقة على الأشخاص المعنوية

إن العقوبة كانت من الحجج التي استند إليها المعارضون لمبدأ مسؤولية الشخص المعنوي، وذلك لأنهم رأوا أنه لا يمكن تطبيقها على هذا الأخير، خصوصاً الشخص المعنوي، وذلك لأهم لرأوا أنه لا يمكن تطبيقها على هذا الأخير، خصوصاً تبلك السلبية والمقيدة للحرية، ولكن وبعد اتساع عقوبة الغرامة وابتكار عقوبات جديدة تتلاءم وطبيعة الشخص المعنوي والتي نصت عليها المادة 18 مكرر من قانون العقوبات الجزائري.

أ- الغرامة:

والتي تساوي من مرة إلى خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة وهي العقوبة التي نصت عليها المادة 394 مكرر4.

وعندما لا ينص القانون على عقوبة الغرامة بالنسبة للأشخاص الطبيعيين سواء في الجنايات والجنح، وقامت المسؤولية الجزائية للشخص المعنوي كما حددته المادة 51 مرر فإن الحد الأقصى للغرامة فيما يخص الشخص المعنوي يكون 500،000 دج على اعتبار أن جريمة التزوير جنحة.[2]

والغرامة كعقوبة مالية تعتبر جزءا فعالاً بالنسبة للشخص المعنوي ذلك أن معظم الجرائم التي يرتكبها هذا الأخير يكون القصد منها تحقيق فائدة غير مشروعة، كما تعتبر هذه العقوبة الأكثر تطبيقاً

---

[1]- غنية باطلي، المرجع السابق، ص220.

[2]- وهذا ما بينته المادة 18 مكرر02 بقولها:<<عندما لا ينص القانون على عقوبة الغرامة بالنسبة للأشخاص الطبيعيين، سواء في الجنايات أو الجنح، وقام المسؤولية الجزائية للشخص المعنوي طبقاً لأحكام المادة 51 مكرر، فإن الحد الأقصى للغرامة المحتسب لتطبيق النسبة القانونية المقررة للعقوبة فيما يخص الشخص المعنوي يكون كالآتي:

- .2.000.000 دج عندما تكون الجناية معاقبا عليها بالإعدام أو السجن المؤبد.
- 1.000.000 دج عدما تكون الجناية معاقباً عليها بالسجن المؤقت.
- 500.000دج بالنسبة للجنحة>>.

وانتشاراً بالنسبة للشخص المعنوي كونها أكثر ردعاً وأقل ضرراً من الناحية الاقتصادية، إضافة إلى هذا سهلة التطبيق سواء من حيث التحصيل أو من حيث إجراءات التنفيذ.[1]

ب- العقوبات التكميلية:

تتمثل العقوبات التكميلية المقررة لجريمة التزوير في العقوبات المنصوص عليها والمطبقة على الشخص المعنوي في المادة 18 مكرر وذلك بتطبيق واحدة أو أكثر من العقوبات التالية:

1- حل الشخص المعنوي والتي تماثل عقوبة الإعدام بالنسبة للشخص الطبيعي، ولا توقع إلا بتوافر حالتين وهما:[2]

- أن يكون الشخص المعنوي قد وجد بغرض ارتكاب الجريمة وهذا يعني أن هناك غرضا رئيسيا لمؤسسي الشخص المعنوي وهو ارتكاب النشاط غير المشروع.

- خروج الشخص المعنوي عن الغرض الذي أنشأ من أجله ارتكاب النشاط الإجرامي.

2- غلق مؤسسة أو إحدى فروعها لمدة لا تتجاوز 5 سنوات وهذا يعني وقف الترخيص لمزاولة النشاط، وهذه المدة تقضي بغلق المؤسسة فلا يجوز بيعها ولا التصرف فيها طول مدة الغلق، وتعد من العقوبات المؤقتة خلافاً للحل الذي يعتبر الإنهاء الكلي لها.[3]

3- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5سنوات، وهذا بحرمان الشخص المعنوي من المساهمة في أي صفقة وهذا بإبقاء الهيبة للمال العام.

4- المنع من مزاولة نشاط مهني أو اجتماعي بشكل أو غير مباشر نهائياً، لمدة لا تتجاوز خمس سنوات، بشكل مؤقت أو دائم كما تمكن أن يكون هذا النشاط المحظور هو الذي وقعت الجريمة بمناسبته أو يعتري المنع أنشطة أخرى.[4]

---

[1]- محمد محدة، المسؤولية الجنائية للشخص المعنوي، مجلة المفكر جامعة محمد خيضر، العدد الأول، بسكرة، الجزائر، 200، ص،ص52،51.

[2]- محمد أبو العلا عقيدة، الاتجاهات الحديثة في قانون العقوبات الفرنسي الجديد، د.ون طبعة، دار النهضة العربية، مصر، 2004، ص78.

[3]- محمد محدة، المرجع السابق، ص54.

[4]- وتجدر الإشارة إلى أن المشرع الجزائري لم يحدد النشاط الذي يجوز منع الشخص من ممارسته على عكس المشرع الفرنسي الذي نص على تحديد ماهية ومفهوم الأنشطة التي تجوز منع الشخص من ممارسته/ للمزيد أنظر: محمد أبو العلا عقيدة، المرجع السابق، ص43.

5- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها وتتميز هذه العقوبة بأنها غير رضائية وأنها دون مقابل، وأيضا قضائية كونها تعني نزع ملكية المال من صاحبه جبراً عنه وإضافته إلى الخزينة العامة، والأهم من ذلك أن المصادرة بنوعيها تعتبر من العقوبات الفعالة كونها تصيب الشخص المعنوي بخسارة مالية.

6- تعليق ونشر قرار الإدانة وذلك بإعلانه حتى يصل إلى علم عدد كاف من الناس بأي وسيلة كانت سمعية أو بصرية.

7- الوضع تحت المراقبة القضائية لمدة لا تتجاوز 5سنوات والتي تنصب على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.[1]

وبالرجوع إلى المادة 394 مكرر06 من قانون العقوبات الجزائري نجدها قد استثنت المادة نفسها الغير حسن النية بحفظ حقوقه ونصت على مصادرة الأجهزة المستعملة والبرامج والوسائل المستعملة مع إلحاق ذلك بغلق المواقع وكذا أماكن الاستغلال شريطة أن تكون الجريمة قد ارتكبت بعلم مالك تلك المحلات.[2]

والواضح أن تطبيق هذا النص يثير إشكالات عديدة في الحياة العملية سيما بخصوص طرق التفتيش والتحري عن الجريمة من هذا النوع نظراً لطابعها التقني هذا فضلاً عما سوف يترتب عن ذلك أي عن اختراق المواقع من المساس بالحقوق الشخصية والتي يكفلها الدستور للأشخاص.[3]

وبمجرد الملاحظة البسيطة يتضح أن المشرع الجزائري حذا حذو التشريعات العربية والعالمية المتطورة والحديثة في مجال في العقوبات التكميلية مثل المصادرة إذ جاءت المادة 394 مكرر 6 على سبيل المثال متطابقة تماما مع ما نص عليه القانون الاتحادي للإمارات العربية المتحدة رقم 02 لسنة

---

[1]- محمد محدة، المرجع السابق، ص،ص55،56.

[2]- تنص المادة 394 مكرر06 على أنه:<< مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلاً لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذ كانت الجريمة قد ارتكبت بعلم مالكها>>.

[3]- زبيحة زيدان، المرجع السابق، ص104.

2006 [1] غير أن القانون الجزائري أورد النص في شكل قواعد عامة سواء بخصوص المصادرة أو غلق الواقع والمحلات.

إلا أنه لم يحدد القواعد الإجرائية كما أشرنا له وكما أوردته تشريعات أخرى مثل القانون التونسي الخاص بالمبادلات التجارية الالكترونية، وكذا القانون الفرنسي 1987/17 والخاص بالمعالجة الالكترونية للبيانات الاسمية والمدعم بقانون العقوبات الجديد 336/92 لسنة 1992.[2]

وتجدر الإشارة إلى أن القانون 10/08 المتمم للقانون 11/83 المتعلق بالتأمينات الاجتماعية نص على المسؤولية الجنائية للأشخاص المعنوية عن المرتكبة على هذه البطاقات من غش أو تعديل أو حذف كلي أو جزئي للمعطيات سواء التقنية أو الإدارية المدرجة في هذه البطاقات الالكترونية، حيث عاقبت المادة 93 مكرر 05 بغرامة تساوي خمس مرات المبلغ الأقصى للغرامة المقررة للشخص الطبيعي>>.[3]

وما يلاحظ على العقوبة المقررة للشخص المعنوي بمناسبة ارتكابه للتزوير في المحررات الالكترونية هي غرامة مشددة إذا ما قورنت بتلك العقوبة المقررة في المادة 18مكرر.

وعليه فالعقوبة المقررة للشخص المعنوي المرتكب لتزوير بطاقة الشفاء هي عقوبة خاصة لذا فالمشرع لم يورد بشأنها إحالة على قانون العقوبات، ولعل السبب في ذلك يرجع إلى خطورة التزوير

4- وهذه المادة تطابق المادة 25 من القانون 02 لسنة 2006 القانون الإماراتي الاتحادي بقولها:" مع عدم الإخلال بحقوق الغير النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في القانون أو الأموال المتحصلة منها، كما يحكم بإغلاق المحل أو المشروع الذي يكون محلا لارتكاب أيمن هذه الجرائم إذا كانت الجريمة قد ارتكبت بعلم مالها، وذلك إغلاقاً كلياً أو للمدة التي تقدرها المحكمة".

[2]- زبيحة زيدان، المرجع السابق، ص105.

[3]- تنص المادة 93 مكرر 3 على أنه:<< يعاقب كل شخص معنوي يرتكب إحدى الجنح المنصوص عليها في المادتين 93 مكرر 03 و93 مكرر04 أعلاه بغرامة تساوي 5 مرات المبلغ الأقصى للغرامة المقدرة للشخص الطبيعي>>.

وقد نصت المادة 93 مكرر 03 من ذات القانون على مايلي:<دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين (02) إلى خمس (05) سنوات وبغرامة من 500.000دج إلى .1.000000 دج كل من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية و/أو الإدارية المدرجة في البطاقة الالكترونية لمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهني الصحة>>.

في المحررات الالكترونية الذي يتطلب دراية وعلم بالتقنيات الحديثة، كما تتطلب ذكاء وخبرة وبراعة من جانب مرتكب الجريمة.[1]

المطلب الثاني: العقوبات المقررة لجريمة التزوير الالكتروني في التشريعات المقارنة

إن بيان العقوبات المقررة في جريمة التزوير الالكتروني في التشريعات المقارنة يقضي الرجوع إلى الصيغ المجرمة لفعل التزوير في المحرر الالكتروني، سواء كان هذا الفعل مجرماً بنصوص خاصة، أو من خلال قانون العقوبات.

ولقد انتهجت التشريعات المقارنة منهجاً معينا في تجريم التزوير الالكتروني فهناك من جرم هذا الفعل في قانون العقوبات كالمشرع الفرنسي، وهناك من جرمه في قوانين منفصلة.

ودراسة العقوبات لجريمة التزوير الالكتروني ستكون بناء على النصوص الواردة في هذه القوانين.

وسنحاول من خلال هذا المطلب بيان العقوبات المقررة لجريمة التزوير الالكتروني في التشريع الفرنسي، وكذا القانون المصري وأيضا القانون الاتحادي الإماراتي لجرائم تقنية المعلومات الذي يعتبر من القوانين العربية السباقة في مجال مكافحة الجرائم الالكترونية، وهذا على النحو الآتي بيانه.

الفرع الأول: العقوبات المقررة لجريمة التزوير الالكتروني في القانون الفرنسي

بعد صدور القانون الفرنسي الجديد في 1992/12/16 قرر المشرع الفرنسي عدم ضرورة الإبقاء على التجريم الخاص بتزوير المستندات المعالجة آليا واستعمالها، والاكتفاء بإضافته إلى جريمة التزوير العادي، وقد تم إعادة 441 من الكتاب الرابع من قانون العقوبات لكي تفي بهذا الغرض.

وتطبيقا لذلك صنف المشرع الفرنسي العقوبات المقررة لجريمة التزوير إلى أصناف تتناسب طرداً مع طبيعة المحرر المزور، حيث نظم المادة 441 من قانون العقوبات في عدة فقرات، وضعت فيها عقوبات تختلف باختلاف جسامة وخطورة كل نوع من أنواع التزوير، كما قرر عقوبات للشخص الطبيعي سواء أصلية أو تبعية، إضافة إلى العقوبات المقررة للشخص المعنوي وهذا ما سنوضحه في العناصر الآتية:

[1]– الهام بن خليفة، المرجع السابق، ص192.

أولاً- العقوبات المقررة للشخص الطبيعي

تنص الفقرة الرابعة من المادة 441 من قانون العقوبات الفرنسي على أنه:" يعاقب على التزوير المرتكب في كتابة عمومية أو رسمية أو في تسجيلات تأمر بها السلطة العامة[(*)1] بعشر سنوات سجن و150،000 يورو غرامة، وإذا ارتكب التزوير بواسطة شخص مؤتمن من السلطة العامة أو مكلف بمهمة في مرفق عام أثناء القيام بوظيفته أو مهمته فتكون العقوبة 15 سنة وغرامة قدرها 225.000يورو".

من خلال المادة أعلاه نجد أن العقوبة المقررة لجريمة التزوير والتي أقرها المشرع الفرنسي تختلف بحسب ما إذا كان المحرر محل التزوير رسمياً أو عرفياً، كما تختلف أيضا حسب صفة الشخص مرتكب التزوير.

وعليه ففعل التزوير لا يعد جريمة إلا إذا انصب على وثيقة لها قيمة قانونية ويتحقق ذلك دائما في حال كانت الكتابة عامة، فهذه الوثائق لها حماية خاصة باعتبارها صادرة عن جهة إدارية عامة، ولذلك تتفاوت العقوبات المقررة في حال تزويرها بحسب خطورة الآثار المترتبة على ذلك، باعتبار أن ذلك يؤدي إلى إضعاف الثقة العامة في مثل هذه الوثائق، وهي نتيجة خطيرة يجب مواجهتها بالعقوبة المناسبة على خلاف التزوير في المحررات العرفية، ولذلك شدد المشرع الجنائي الفرنسي العقوبة كلما اشتدت خطورة الفعل وذلك تبعا لنوع الوثيقة محل التزوير.[2]

ويطبق على ارتكاب التزوير في المحررات عقوبات أصلية عادية وأخرى مشددة.

[1](*)- أضافت هذه الفقرة إلى المحررات الرسمية أو العمومية التسجيلات التي تأمر بها السلطة العامة، وهذا تطبيقا لنص المادة 441 فقرة ، فهذه الفقرة تعتبر هذه التسجيلات من قبيل المحررات الرسمية أو العمومية وتشمل هذه التسجيلات الرئيسية والبصرية وكذا السمعية البصرية وتسجيلات التصنت الهاتفي.

[2]- Philipe Bluteau, la faux en écriture publiques, courrier des Maires, n°= 249, France,2011.

أ- العقوبات الأصلية المقررة للشخص الطبيعي:

نصت المادة 441 فقرة 04 في شقها الأول على العقوبة المقررة لجريمة التزوير في المحررات الرسمية أو العمومية والتسجيلات التي تأمر بها السلطة العامة والمتمثلة في الحبس لمدة سنوات إضافة إلى غرامة مالية تقدر بـ 150،000 يورو.[1]

وقد شدد المشرع الجنائي الفرنسي العقوبة بحسب صفة مرتكب التزوير، إذ رفع العقوبة في

حال ارتكاب جرم التزوير من طرف شخص يملك سلطة عامة أو مكلفة بتأدية خدمة عامة في إطار أدائه لوظائفه وهذا طبقا للفقرة 03 من المادة 4/441، إذ ترتفع العقوبة إلى 15 سنة سجن، كما ترتفع الغرامة إلى 225 ألاف أورو،[2] بحسب خطورة الفعل في هذه الحالة، ذلك أن السلطة التي يملكها هذا الشخص والتي خولها إياه القانون لتحرير مثل هذه الوثائق، تمكنه من ارتكاب التزوير، ويكون الأمر أيسر عندما تكون هذه الوثائق معلوماتية، حيث سيكون هذه الشخص من الأشخاص المرخص لهم قانوناً بالدخول إلى النظام المعلوماتي لمعالجتها آلياً.

كما تشدد العقوبة أيضا لتصل إلى 15 سنة سجنا إذا ارتكب الجريمة المنصوص عليها في المادة 47/441 قصداً بالارتكاب مع مجموعات مكونة وبالتالي تشكل فعلاً إرهابياً بهدف الإخلال بالنظام العام وهذا طبقا للفقرة 03 من المادة 4/441 من قانون العقوبات الفرنسي.

أما بالنسبة للعقوبات المقررة للتزوير في المحررات العرفية أو المصرفية أو التجارية فقد قررها المادة 1/4410 في فقرتها الثانية بالحبس لمدة ثلاث سنوات و غرامة تقدر 1/45،000 في فقرتها الثانية بالحبس لمدة ثلاث سنوات و غرامة تقدر بـ 45،000 يورو، ولم تنص هذه المادة على ظروف تشديد العقوبة.

---

[1]- la faux commis dans une écriture publique ou authentique on dans un enregistrement ordonné par l'autorité publique et puni de disc ans d'emprisonnement et de 150,000 euro demande.

[2]- Les peines sont portées a quinze ans de réclusion criminelle et a 225,000 euro d'amende lorsque le faux ou l'usage de faux et commis par une personne dépositaire de l'autorité publique ou chargée dune mission de service public agissant dans l'escrime de ses fonctions ou de sa mission.

في حين جاءت الفقرة 2من المادة 441 والتي تقرر العقوبات المفروضة عن التزوير في الوثائق الإدارية بعقوبات أشد من تلك المنصوص عليها في المادة 441 فقرة 01، حيث يعاقب بالحبس لمدة 05 سنوات وغرامة تقدر بـ 75،000 كل من ارتكب جرم التزوير في الوثائق الإدارية،[1] وذلك كون أن التزوير في هذه الحالة يتعلق بوثيقة تثبت حقا أو واقعة أو تمنح ترخيصاً، وهي صادرة عن جهة إدارية عامة وهذا ما جعل العقوبة مشددة وهذا حماية للثقة العامة التي تتمتع بها هذه الوثائق.

وبالرجوع للفقرة الثالثة من المادة 2/441 نجد أن المشرع النائي الفرنسي قد رفع العقوبة إلى 07 سنوات حبس و100،000 أورو غرامة إذا كان التزوير مرتكب من ممثل عن السلطة العامة أو مكلف بمرفق عام أثناء تأدية وظيفته.

وقد عاقب المشرع الجنائي الفرنسي على الشروع في الجرائم السابقة بنفس العقوبة المقررة للجريمة التامة سواء شكل التزوير جنحة أو جناية، وهذا طبقا للفقرة 9 من المادة 441، وعليه فتسلط العقوبة حتى ولو لم تتحقق النتيجة وهذا حفاظاً على المصلحة المحمية قانوناً، طالماً القصد الجنائي ثابت لدى الجاني.

ب- العقوبات التكميلية المقررة للشخص الطبيعي:

إضافة إلى العقوبات الأصلية المطبقة على الشخص الطبيعي، قرر المشرع الجنائي لفرنسي عدة عقوبات تكميلية، وتتمثل هذه العقوبات في المنع من الحقوق الوطنية والمدنية والعائلية، وهذا طبقا للمادة 10/441، إضافة إلى المنع من ممارسة الوظيفة العامة أو أي نشاط ذو طبيعة مهنية أو اجتماعية، وكذا الإقصاء من الصفقات العمومية، وأيضا مصادرة الشيء المستعمل في ارتكاب الجريمة.

كما نصت الفقرة 11 من المادة 441 على عقوبة المنع من دخول الإقليم الفرنسي بصفة نهائية أو لمدة 10 سنوات فأكثر على كل أنبي ارتكب أي جريمة من جريمة التزوير في المحررات.

[1]- Le faux commis dans un document délivré par une administration publique aux fins de constater un droit, une identité ou une qualité ou d'accorder une autorisation et puni de cinq ans d'emprisonnement et de 75,000 Euro d'amende.

ثانياً- العقوبات المقررة للشخص المعنوي

بالرغم من الخلاف الفقهي بين مؤيد ومعارض لقيام المسؤولية الجنائية للشخص المعنوي، إلا أنها أصبحت من الأمور المسلم بها، إذ أقرت بها كل التشريعات الجنائية، ولقد نص المشرع الفرنسي على المسؤولية الجنائية للشخص المعنوي عن كل جرائم التزوير وهذا من خلال المادة 12/441 من قانون العقوبات الفرنسي.[1]

وبناءاً على ذلك تمكن الأشخاص المعنوية أن يسألوا جنائياً عن جرائم التزوير وهذا في الحالات التي نص عليها القانون أو اللائحة عن الجرائم التي ارتكبوها لحساب أو من طرف أعضائهم أو ممثليهم، أما الجماعات المحلية والتجمعات التابعة لها لا يسألون جنائياً إذا كانت الجرائم التي ارتكبوها أثناء ممارسة نشاطهم والقابلة لأن تكون موضوعاً لا تفاق الخدمة العامة.

والمسؤولية الجنائية للأشخاص المعنوية لا تستبعد الأشخاص الطبيعية فاعلين أو مساهمين الذين ارتكبوا نفس الوقائع، ومن هنا يتضح أن المشرع الفرنسي أراد أن يشرك الأشخاص الطبيعية في المسؤولية مع الأشخاص المعنوية حتى لا يتحملوا وحدهم نتائج فعل مترتب عن الإرادة الجماعية.[2]

وبالرجوع للمادة 2/121 من قانون العقوبات الفرنسي نجدها قد حددت شروط مساءلة الشخص المعنوي، حيث تستثني الدولة ققي فقرتها الأولى، والجماعات المحلية في الفقرة الثانية من هذه المسؤولية، وهذه المسؤولية مقتصرة على الحالات التي نص عليها القانون، ويشرط لقيامها أن ترتكب الجريمة من احد أعضاء الشخص المعنوي.[3]

وعليه فإذا ارتكب الشخص المعنوي جريمة تزوير في وثيقة أو محرر الكتروني وتوافرت الشروط السابق ذكرها، فإنه يسأل جنائياً وتطبق عليه العقوبات المنصوص عليها في المواد 38/131 و131 فقرة 39 وفقا للمادة 441 فقرة 12 ولقد شدد المشرع العقوبة على الأشخاص المعنوية التي تنشأ

---

[1]- art 441/12 : "les personnes morales peuvent être déclarées responsables pénalement dans les condition prévues pas article 121/2 , des infractions au présent chapitre".

[2]- غنية باطلي، المرجع السابق، ص219.

[3]- Jean Francois Casile, code pénal a épreuve de la délinquance informatique, presse universitaire d'Aix, Marseille, France,2002, p107.

بغرض تحقيق الربح، فتقوم بالمنافسة غير المشروعة لمنافسيها عن طريق ارتكاب هذا النوع من الجرائم .

وقد قرر المشرع الجزائي الفرنسي للشخص عقوبات أصلية حددتها المادة 38/131 وأخرى تكميلية ذكرتها المادة 39/131 سنحاول إيجازها فيما يلي:

أ- العقوبات الأصلية المقررة للشخص المعنوي:

إن العقوبة كانت من الحجج التي استند إليه المعارضون لمبدأ مسؤولية الشخص المعنوي، وذلك لأنهم رأوا أنه لا يمكن تطبيقها على هذا الأخير، خصوصاً تلك السالبة أو المقيدة للحرية، ولكن بعد اتساع عقوبة الغرامة وابتكار عقوبات جديدة تتلاءم وطبيعة الشخص المعنوي، ومن بين العقوبات المطبقة على الشخص المعنوي المقررة في قانون العقوبات الفرنسي الغرامة وهذا وفقاً للمادة 38/131 والتي جاءت في فقرتها الأولى على أن الحد الأقصى للغرامة المطبقة على الأشخاص المعنوية يساوي خمس أضعاف الحد الأقصى للغرامة المقررة للأشخاص الطبيعية.

وتنص الفقرة 02 من ذات المادة على أنه:"...في حالة ما ارتكب الشخص المعنوي جريمة لم يقرر فيها القانون للشخص المعنوي عقوبة الغرامة، فإنه تسلط عليه غرامة 1،000،000 أورو....."

كما نص المشرع الفرنسي على عقوبة الغرامة في حالة العود، فرفع حدها الأقصى إلى عشر أضعاف ما هو مقرر للشخص المعنوي حسب ما قررته المادة 132/1-12 إلى المادة 15/132 من القانون الجنائي الفرنسي.

ب- العقوبات التكميلية المقررة للشخص المعنوي:

وقد قررت المادة 39/131 جملة من العقوبات التكميلية التي تمكن أن تطبق على الشخص المعنوي والمتمثلة في الحل، الحرمان من النشاط، الحرمان من الاكتتاب العام في الادخار، الإقصاء من الصفقات العمومية بطريقة نهائية أو لمدة سنوات أو أكثر.

الفرع الثاني: العقوبات المقررة لجريمة التزوير الالكتروني في نصوص خاصة

لقد اختلفت خطة التشريعات العربية حول النص على جريمة التزوير الالكتروني، فهناك من التشريعات من ذهب إلى إرساء تعديلات على النصوص التزوير في قانون العقوبات كالمشرع الفرنسي

الفرنسي، كما سبقت الإشارة إلى ذلك وهناك اتجاهات تشريعية جرمت التزوير الالكتروني في نصوص خاصة تجرم كل الاعتداءات الواردة على تقنية المعلومات كالتشريع المصري والإماراتي.

وبناء على هذا فإن بيان العقوبات المقررة لجريمة التزوير الالكتروني يقتضي الرجوع إلى الصيغ التشريعية المجرمة لهذا الفعل سواء بالرجوع إلى النصوص الخاصة أو إلى قانون العقوبات إذا اقتضى الأمر ذلك.

وموازاة مع ما تم دراسته في المبحث الأول سنبين العقوبات المقررة لجريمة التزوير الالكتروني في التشريع المصري والتشريع الإماراتي، وهذا على النحو الآتي بيانه:

أولاً- العقوبات المقررة لجريمة التزوير الالكتروني في التشريع المصري

إن المسؤولية الجنائية الشخصية تعني ألا يسأل جنائيا إلا الشخص الذي ارتكب الجريمة ويساهم في ارتكابها عن طريق وسائل الاشتراك من اتفاق أو تحريض أو مساعدة وقد أخذ المشرع الجنائي بهذا المبدأ.[1]

كما تبنى المشرع المصري مبدأ المسؤولية الجنائية للأشخاص المعنوية إلى جانب الأشخاص الطبيعية وهذا ما سنوضحه فيما يلي:

أ- المسؤولية الجنائية الشخصية عن جرائم التزوير الالكتروني:

إن المسؤولية الجنائية عن الجرائم الالكترونية بصفة عامة هي مسؤولية الشخص الطبيعي عن ارتكاب الجريمة ضد المعلومات سواء كان هذا الشخص الطبيعي مستخدماً أو متدخلاً أو مهنياً من العاملين على شبكة الانترنت وفقا لما هو وارد في القانون.[2]

وقد عاقب المشرع المصري على فعل تزوير المحرر أو المستند الالكتروني بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تتجاوز مئة ألف جنيه أو بإحدى هاتين العقوبتين، مع مراعاة تطبيق

[1]- ياسر محمد الكومي محمد أبو حطب، الحماية الجنائية والأمنية للتوقيع الالكتروني في التشريع المصري والتشريعات المقارنة، أطروحة دكتوراه كلية الحقوق، جامعة حلوان، مصر، 2013، ص175.

[2]- أحمد فتحي سرور، الوسيط في قانون العقوبات (القسم العام)، المرجع السابق، ص379.

العقوبة الأشد المنصوص عليها في قانون العقوبات أو أي قانون آخر وهذا طبقا لنص المادة 23 من قانون التوقيع الالكتروني.[1]

وما يلاحظ على نص هذه المادة أن المشرع الرسمي من خلال قانون التوقيع الالكتروني لم يفرق أو لم يميز بين المحرر الالكتروني الرسمي المزور والمحرر الالكتروني العرفي المزور،[2] فتزوير المحرر الالكتروني في وثيقة رسمية إدارية يعاقب عليه بعقوبة أشد، ومن ذلك التزوير الواقع في وثائق الأحوال المدنية ذات الطبيعة المعلوماتية، والتي اعتبرها المشرع المصري وثائق رسمية من خلال ما نص عليه في قانون الأحوال المدنية في المادة 72 منه، وإذا وقع تزوير في هذا المحررات أو غيرها من المحررات الرسمية تكون العقوبة الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات.[3]

وما يفهم من المادة 72 وكذا المادة 23 من قانون التوقيع الالكتروني أن العقوبة المقررة لتزوير المحرر الالكتروني قد تكون هي العقوبة المنصوص عيها في المادة 23 من قانون التوقيع الالكتروني، وقد تكون أشد إذ تصل إلى الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات، تبعا لطبيعة الوثيقة المزورة، وعليه فليس ثمة جنائيا واحداً يبين تدرج العقوبة حسب طبيعة المحرر المزور.

ولكن بالرجوع إلى نصوص المواد 211 و212 و213 من قانون العقوبات نجد أن التزوير في المحررات الالكتروني يشكل جناية، خاصة وأن المشرع المصري استهل نص المادة 23 بقوله:" مع عدم الإخلال بأي عقوبة أخرى منصوص عليها في قانون آخر...، وهنا يجب إعمال عقوبة الجريمة ذات الوصف الأشد، فمن المسلم به أن الأنظمة الجنائية تهتم عادة بتشديد العقاب على التزوير في

[1]– تنص المادة 23 من القانون 15 لسنة 2004 بشأن التوقيع الالكتروني على أنه:" مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في لأي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تتجاوز مئة ألف جنيه أو بإحدى هاتين العقوبتين كل من: الاصطناع أو التعديل أو التحوير أو بأي طريق آخر".

[2]– محمد أمين الرومي، المستند الالكتروني، مرجع سابق، ص87.

[3]– تنص المادة 72 من قانون الأحوال المدنية المصري:" في تطبيق أحكام هذا القانون وقانون العقوبات تعتبر البيانات المسجلة بالحسابات الآلية وملحقاتها بمراكز معلومات الأحوال المدنية ومحطات الإصدار الخاصة بها المستخدمة في إصدار الوثائق وبطاقات تحقيق الشخصية بيانات واردة في محررات رسمية، فإذا وقع تزوير في المحررات السابقة أو غيرها من المحررات الرسمية تكون العقوبة الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات".

المحرر الرسمي وذلك لطبيعة الصلة الوثيقة التي تربط الوضع الوظيفي من جانب والمحرر الرسمي من جانب آخر، وهذا ما أخذه به المشرع المصري في المادتين 212،213 من قانون العقوبات.

إلى جانب ذلك تنص المادة 212 من قانون العقوبات المصري على معاقبة كل شخص ليس من أرباب الوظائف العمومية ارتكب تزويراً ممن هو مبين في المادة السابقة بالأشغال الشاقة المؤقتة أو بالسجن مدة أكثرها عشر سنين[1] .

ومن خلال مطالعة ذلك النص لوحظ فيه عدم الدقة في الصياغة، فقد بين فيه المشرع صفة الفاعل فاشترط ألا يكون من أرباب الوظائف العمومية، وهذا القيد يوهم بأن حكم المادة يقتصر على الموظف العام ويقتصر كذلك على من عداه، وهذا يخالف مقتضى قصد المشرع ولو صح هذا الفهم لأفلت الموظف العام من العقاب إذا كان غير مختص بتحرير المحرر الذي ارتكب التزوير فه أو كان غير واقع منه أثناء تأدية وظيفته.[2]

ويفهم أيضا من نص المادة 212 من قانون العقوبات المصري أن المقصود بالعقاب هنا هو غير الموظف العام، ذلك أن الموظف العام قد قررت له عقوبة أخرى، خاصة وأن المادة تشير إلى الصياغة، حيث يفهم من صيغة هذه المادة أنها لا تنطبق إلا على أفراد الناس الذين ليس لهم صفة الموظف العام إطلاقا مع أنه يدخل في حكمها الموظف العام الذي يرتكب تزويراً مادياً في محرر رسمي في غير أعمال وظيفته، وكان يكفي لأداء هذا المعنى النص بالقول كل شخص ليس من ذكر في المادة السابقة،[3] ومع هذا يمكن الاعتذار عن صياغة النص بالقول أن عبارة "أرباب الوظائف العمومية" في باب التزوير لها معنى خاص هو أن يكون الموظف العام قد خوله القانون سلطة تحرير المحرر وإعطائه الصبغة الرسمية.[4]

---

[1]– تنص المادة 212 من قانون العقوبات المصري على أنه:" كل شخص ليس من أرباب الوظائف العمومية ارتكب تزويراً مما هو مبين في المادة السابقة يعاقب بالأشغال الشاقة المؤقتة أو بالسجن مدة أكثرها عشر سنين".

[2]– إبراهيم حامد طنطاوي، المسؤولية الجنائية عن جرائم التزوير في المحررات– فقها وقضاء، الطبعة الأولى، المكتبة القاهرية، مصر، 1995، ص177.

[3]– عوض محمد عوض، المرجع السابق، ص257.

[4]– رؤوف عبيد، المرجع السابق، ص153، أنظر أيضا: محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص391.

ب- المسؤولية الجنائية للأشخاص المعنوية عن جرائم التزوير الالكتروني:

كان المشرع المصري ملتزما بمبدأ المسؤولية الجنائية للشخص المعنوي، أما الفقه انقسم إلى فريقين مؤيد لإقرار المسؤولية الجنائية للأشخاص المعنوية وفريق آخر معارض لها، وكان المشرع المصري اعترف بهذا النوع من المسؤولية على سبيل الاستثناء وذلك في مجال الاقتصاد وبالتالي قبول مبدأ توقيع عقوبة الغرامة.[1]

وبصدور القانون 15 بسنة 2004 بشأن التوقيع الالكتروني حسم المشرع ذلك الأمر صراحة، حيث نص على مسؤولية الشخص المعنوي عن الجرائم التي تركت بالمخالفة لأحكام هذه القانون، وعليه يكون الشخص الاعتباري مسئولاً جنائيا ويعاقب بالعقوبات المقررة للجرائم الالكترونية أو المعلوماتية والمتمثلة في الحبس أو الغرامة أو أيهما، وبالغرامة فقط إذا كانت هي العقوبة الجنائية الوحيدة لهذه الجريمة، وذلك بشرط أن تكون الجريمة قد وقعت لأن المدير المسؤول لم يراع الواجبات المفروضة عليه والتي تقتضيها الإدارة.[2]

ومن ناحية أخرى فإن المشرع قد ألزم الشخص الاعتباري بالتضامن بالغرامات والتعويضات التي قد يقضي بها متى كانت الجريمة قد ارتكبها شخص طبيعي –باسم ولصالح- ذلك الشخص الاعتباري.

والحقيقة أن العقوبات المالية وكذلك التعويضات المقضي بها هي أمور تتفق وطبيعة الشخص الاعتباري، وسيما وأن الجريمة قد ارتكبت باسم ولصالح ذلك الشخص الاعتباري، وعليه فإن الأشخاص الاعتبارية العامة أو الخاصة قد ينسب إليها مخالفتها لأي حكم من أحكام هذا القانون، أو اللوائح التي صدرت بناء عليه ويتعين أن تكون هذه المخالفة والتي تمثل جريمة جنائية قد وقعت بناء

[1]- ياسر محمد الكومي محمد أبو حطب، المرجع الساق، ص185.

[2]- تنص المادة 24 من القانون 15 لسنة 2004 بشأن التوقيع الالكتروني على أنه:" يعاقب المسئول عن الإدارة الفعلية للشخص الاعتباري المخالف بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون إذا كان إخلاله بالواجبات التي تفرضها عليها تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك، ويكون الشخص الاعتباري مسئولا بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات إذا كانت المخالفة قد ارتكبت من أحد العاملين به باسم ولصالح الشخص الاعتباري".

على تصرف أو إهمال أو موافقة عضو مجلس إدارة أو مدير أنه أي موظف آخر لدى الشخص المعنوي.[1]

من خلال ما سبق يظهر أن المشرع المصري لم يستثنى من المسؤولية الجنائية عن تزوير المحرر الالكتروني الأشخاص المعنوية العامة خلافاً للمشرع الفرنسي والجزائري، حيث اشترط في مسؤولية أن ترتكب من أحد العاملين ولكن باسم ولصالح الشخص المعنوي.

وعليه فإن العقوبة المقررة للأشخاص المعنوية العامة أو الخاصة هي التضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات، حيث أن هذه العقوبات المالية والتعويضات أمور تتفق وطبيعة الشخص الاعتباري سيما وأن الجريمة قد ارتكب باسمه ولصالحه.[2]

كما قرر المشرع المصري عقوبات تكميلية وجوبية وهي نشر الحكم الصادر بالإدانة في جريدتين يوميتين واسعتي الانتشار، وعلى شبكة المعلومات الالكترونية المفتوحة على نفقة المحكوم عليه.[3]

ثانياً- العقوبات المقررة لجريمة التزوير الالكتروني في قانون مكافحة جرائم تقنية المعلومات الإماراتي

يعد القانون الاتحادي بشأن جرائم تقنية المعلومات من القوانين العربية السباقة في مكافحة الجرائم المعلوماتية، كون أن دولة الإمارات العربية المتحدة من الدول العربية الأولى في استخدام المعلوماتية وفي تبني نظام الحكومة الالكترونية وكان للمشرع الإماراتي وقفة تشريعية مميزة في مجال مكافحة الجرائم المعلوماتية من خلال القانون 2006/02 الخاص بمكافحة جرائم تقنية المعلومات.

وفي مجال التزوير الالكتروني فقد جرم المشرع الإماراتي في القانون الاتحادي الخاص بجرائم تقنية المعلومات فعل التزوير في مستندات الحكومة الاتحادية ووضع عقوبات لذلك، حيث نصت المادة 04 من القانون 02 لسنة 2006 على عقوبة السجن المؤقت كعقوبة أصلية، سواء تغلق الأمر وثيقة صادرة عن الحكومة الاتحادية أو المحلية، وذلك عندما استخدم عبارة معترف بها قانوناً.

---

[1]- ادوارد غالي الذهبي، المسؤولية الجنائية للشخص المعنوي، الطبعة الأولى، دار النهضة العربية، مصر، 1978، ص19.

[2]- نفس المرجع السابق ونفس والصفحة.

[3]- محمد حسين علي محمود، المرجع السابق، ص136.

وتعتبر عقوبة الحبس المؤقت كعقوبة سالبة للحرية من العقوبات الملائمة لطبيعة وجسامة جريمة التزوير، باعتبار أن هذه العقوبات من الجرائم المخلة بالثقة العامة، في حين تعد الغرامة كعقوبة مالية منصوص عليها في هذه المادة عقوبة اختيارية، حيث تمكن الحكم بها مع عقوبة الحبس إذا تعلق الأمر بتزوير وثيقة معلوماتية غير رسمية، وقد لا يحكم بها آخذا باتجاه اتفاقية بودابست المتعلقة بالإجرام المعلوماتي.

فضلا عن العقوبة الأصلية التي تسلط على مرتكب الجريمة فإن المادة 24 من القانون 2006/02 نصت على عقوبة المصادرة كعقوبة تكميلية وذلك بمصادرة الأجهزة والوسائل المستخدمة في ارتكاب الجرم، وكذا الأموال المتحصلة منها كما نصت على غلق المحل الذي ارتكبت فيه الجرائم كلياً أو لمدة تقدرها المحكمة.[1]

وتجدر الإشارة إلى أن المادة 26 من القانون لسنة 2006 قد أحال إلى فقانون العقوبات الاتحادي في تطبيق العقوبة متى كانت أشد من تلك الواردة فيه، وعليه يكون القاضي في جريمة

التزوير الالكتروني متمسكاً بالقانونين معاً لتطبيق العقوبة المقدرة على جريمة التزوير الالكتروني.[2]

[1]– تنص المادة 24 من القانون 02 لسنة 2006 على أنه:" مع عدم الإخلال بحقوق الغير حس النية يحكم في جميع الأحوال بمصادرة الأجهزة والبرامج أو الوسائل ألمستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة عنها، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم إذا كانت الجريمة فد ارتكبت بعلم مالكه، وذلك إغلاقا كليبا أو للمدة التي تقدرها المحكمة".

[2]– تنص المادة 026 من القانون 02–2006 بشأن مكافحة جرائم تقنية المعلومات على أنه: "لا يدخل تطبيق العقوبات المنصوص عليها في هذا القانون بأية عقوبة أشد ينص عليها في قانون العقوبات أو أي قانون آخر".

خلاصة الباب الأول

تعد جريمة التزوير الإلكتروني من الأنماط الإجرامية الحديثة التي فجرتها ثورة تقنية المعلومات، وقع التزوير على كل محرر الكتروني لإحدى الطرق المنصوص عليها قانونا ما من شأن ذلك إحداث ضرر للغير.

وتتميز جريمة التزوير الالكتروني بجملة من الخصائص المختلفة عن جريمة التزوير التقليدي ،لعل أهمها صعوبة إثباتها وطابعها الدولي العابر للحدود ،ناهيك عن تفرد شخصية المزور الالكتروني المتميزة .

ولعل الضمانة الأبرز لحماية المحرر الالكتروني ومكافحة جريمة التزوير الإلكتروني هو التدخل التشريعي ، وهذا بتجريم كل غش يقع عليها وتوقيع العقوبة على مرتكبيها لما تشكله هذه الجريمة من تهديد للثقة العامة التي يوليها الأفراد لهذه المحررات لاسيما مع ازدياد التعامل بالمحررات الالكترونية وحلولها محل المحررات الورقية.

ومن هنا حرصت التشريعات في مختلف دول العالم على تجريم التزوير الإلكتروني أما بتعديل نصوصها العقابية القائمة أو استحداث نصوص جديدة تتلاءم وطبيعة هذا الجرم ،وكذا وضع الجزاء الجنائي المترتب عن درجة خطورة هذا التزوير،وخطورة المجرم المزور في حد ذاته.

كما بادر المجتمع الدولي إلى تجريم التزوير الالكتروني وهذا من خلال إبرام العديد من الاتفاقيات الدولية في هذا المجال كاتفاقية بودابست لمكافحة أجرام الفضاء المعلوماتي والاتفاقية العربية لمكافحة جرائم تقنية المعلومات .

أما المشرع الجزائري وإن كان لم يجرم التزوير الإلكتروني من خلال نصوص قانون العقوبات ،إلا أنه قام بتجريمه من خلال استحداث القانون 04/09 المتضمن قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،حيث جرم كل جريمة ترتكب بواسطة منظومة معلوماتية ومنها التزوير.

كما جرم التزوير الوقع على الوثائق والشهادات الالكترونية كتجريم تزوير جواز السفر الإلكتروني وبطاقات الشفاء الإلكترونية وأصدر قوانين خاصة بهذه الوثائق والسندات ووضع العقوبات المترتبة على تزويرها.

إضافة إلى هذا جرم المشرع الجزائري التزوير الواقع على التوقيع الكتروني وكذا شهادة التصديق الالكتروني من خلال إصدار القانون 04/15 المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

الباب الثاني

الآليات الإجرائية لمكافحة جريمة التزوير الالكتروني

الباب الثاني: الآليات الإجرائية لمكافحة جريمة التزوير الإلكتروني

إذا كانت ظاهرة الإجرام الالكتروني تثير العديد من المشكلات التي تتعلق بالقانون الجنائي الموضوعي بحثا عن إمكانية تطبيق نصوص التقليدية على هذا النوع المستحدث من الإجرام، فهي أيضا تثير في الوقت ذاته العديد من المشكلات فيما يخص الجانب الإجرائي، حيث وضعت نصوص قانون الإجراءات الجزائية لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات كبيرة في إثباتها أو التحقق منه أو جمع الأدلة المتعلقة بها.

لذا فإن دراسة الجوانب الإجرائية لمكافحة الجرائم الالكترونية، ومنها جريمة التزوير الالكتروني يعد من المقدمات الضرورية التي تستظهر مدى كفاءة الدول في التعامل مع هذا النوع المستحدث من الجرائم، فلا يكفي مجرد التجريم الموضوعي لتجريم التزوير الالكتروني، فمثل هذا الأمر لو حصل سوف يؤدي بنظم الإجراءات الجنائية إلى حالة من الجمود.

كما أن الطابع التقني والدولي لجريمة التزوير الالكتروني يطرح العديد من الإشكالات خاصة في المجال الإجرائي، لاسيما الشروط المتعلقة بالاختصاص القضائي في مسائل الجريمة الالكترونية.

إضافة إلى هذا فإن الطبيعة الخاصة للجرائم الالكترونية تتطلب إجراءات وأساليب خاصة ونوعية للبحث والتحقيق لاكتشاف الدليل الرقمي وتحصيله وهنا تثار مشكلة مدى حجية هذا الدليل أمام القضاء الجنائي.

على هدي ما تقدم سوف نتناول في هذا الباب دراسة الأحكام الإجرائية لمكافحة جريمة التزوير الالكتروني ضمن فصلين، نتطرق في الفصل الأول إلى بيان الأحكام الإجرائية لمكافحة جريمة التزوير الالكتروني على المستوى الداخلي، في حين نخصص الفصل الثاني لدراسة الأحكام الإجرائية لمكافحة جريمة التزوير الالكتروني على المستوى الدولي.

الفصل الأول

القواعد الإجرائية لمكافحة جريمة التزوير الالكتروني على المستوى الداخلي

الفصل الأول: القواعد الإجرائية لمكافحة جريمة التزوير الإلكتروني على المستوى الداخلي

تعد متابعة الجريمة الالكترونية بصفة عامة وجريمة التزوير الالكتروني بصفة خاصة من أهم التحديات التي تواجه الأجهزة الأمنية كونها تتعلق بمحل غير مادي إضافة إلى صعوبة مراقبة ومنع حدوث مثل هذه الجرائم وكذا التحري عن مرتكبيها.

وبناءا على هذا سنتطرق في هذا الفصل لأهم القواعد الإجرائية الداخلية والتي جاء بها المشرع الجزائري لمواجهة هذه الأنماط المستجدة من الجرائم، حيث نخصص المبحث الأول لبيان قواعد الاختصاص القضائي المتعلقة بجريمة التزوير الالكتروني في حين نخصص المبحث الثاني لبيان أهم القواعد الإجرائية لجمع الأدلة في هذه الجريمة وهذا على النحو الآتي:

المبحث الأول: قواعد الاختصاص القضائي المتعلقة بجريمة التزوير الالكتروني:

الاختصاص القضائي هو السلطة التي يقررها القانون للقضاء في أن ينظر في دعاوى من نوع معين حددها المشرع[1]، وفق قواعد إجراءات معينة.

والأصل أن القضاء في كل دولة يبحث فيما إذا كان مختصا بنظر هذه القضية أو تلك، لذا فإن قواعد الاختصاص تشكل فن عمل القاضي أساسا، فالقاضي الوطني يلتزم في البداية بالفصل في الاختصاص الدولي، أي بيان عما إذا كان هو أصلا كقضاء وطني مختص بنظر الدعوى أم لا، ومن ثم البحث في الاختصاص الداخلي كون هذه الدعوى داخلة أصلا في اختصاص القضاء الإقليمي لهذه الدولة. [2]

و الاختصاص الجنائي نوعان: دولي ويقصد به سلطة محاكم كل دولة في نظر دعاوى معينة، داخلي يقصد به توزيع الدعاوى الجنائية التي تدخل في اختصاص القواعد الوطنية على المحاكم الوطنية المتنوعة، وفقا للضوابط والمعايير التي حددها المشرع.وسنحاول بيان هذه القواعد في مطلبين ،خصصنا الأول لدراسة **قواعد الاختصاص الجنائي الدولي** والمطلب الثاني **قواعد الاختصاص الجنائي الداخلي:**

[1]– محمود نجيب حسني، شرح قانون الإجراءات الجنائية، القسم الخاص، المرجع السابق، ص 723.

[2]– حسين بن سعيد بن سيف الغافري، المرجع السابق ،ص 452.

المطلب الأول: قواعد الاختصاص الجنائي الدولي:

إن شبكة الانترنت ليس لها مقر في دولة معينة، ولا تخص شخصا محددا، بل نجدها موزعة على المعمورة، فهي تجتمع لعدد كبير من الشبكات مختلفة النوع والمصدر والوظيفة، فبالتالي هي لا تخضع لرقابة أو سيطرة دولة معينة، ولا يوجد قانون جنائي موحد يحكمها[1]، بل على العكس تتعدد القوانين الجنائية التي تطبق عليها بعدد الدول المرتبطة بها.

وحيث أن الأصل هو الارتباط بين تطبيق التشريع العقابي الوطني من حيث المكان وبين الاختصاص الدولي للمحاكم الوطنية، بمعنى آخر كل جريمة يسري عليها قانون العقوبات الوطني تختص بنظرها المحاكم الوطنية، وهنا يثار التساؤل حول مدى انطباق القوانين الوطنية على الجرائم الالكترونية والتي تتميز بكونها عابرة للحدود ؟.

وبالرجوع إلى القواعد العامة التي تنظم مسألة تطبيق القواعد من حيث المكان نجدها محكومة بثلاثة مبادئ أساسية نوجزها في الفروع التالية:

الفرع الأول: تطبيق مبدأ الإقليمية على جريمة التزوير الالكتروني

إن قواعد القانون الجنائي بشقيه الموضوعي والإجرائي تعد مظهرا من مظاهر سيادة الدول لذلك فإن تطبيقها من حيث المكان يخضع لمبدأ مستقر أولا وهو مبدأ الإقليمية.

وسنحاول في هذا الفرع التطرق إلى تعريف مبدأ الإقليمية ثم نتطرق في الجزء الثاني إلى تطبيق مبدأ الإقليمية في مواجهة جريمة التزوير الالكتروني وهذا على النحو الآتي:

أولا: تعريف مبدأ إقليمية القاعدة الجنائية:

يقصد بمبدأ الإقليمية خضوع الجرائم التي تقع في إقليم دولة معينة لقانونها الجنائي النافذ، بحيث تصبح محاكمها هي صاحبة الولاية بنظر الدعوى الناشئة عنها ولا تخضع لسلطان أي قانون أجنبي، وفي المقابل فلا مجال لأن تمتد سريان قانون الدولة الجنائية خارج نطاقها الإقليمي وفقا لحدودها المعترف بها، حيث يصطدم بسيادة غيرها من الدول، إلا في أحوال استثنائية حماية للمصالح الجوهرية

[1]– جميل عبد الباقي الصغير، المرجع السابق، ص 43

للدولة ومتطلبات التعاون الدولي في مكافحة الإجرام. [1]وعليه فمبدأ إقليمية القاعدة الجنائية يقصد به أن التشريع العقابي ينطبق على جميع الجرائم التي تقع على إقليم الدولة مهما كانت جنسية مرتكبها أو جنسية المجني عليه. [2]

ويجد مبدأ الإقليمية منطقه في سببين أولهما نظري وهو أن القانون الجنائي باعتباره حام لحقوق المجتمع، فهو أداة كل دولة في فرض سيادتها داخل إقليمها، حيث أن تأمين الحقوق الجديرة بالحماية للمجتمع وأفراده يعد أحد أهم مظاهر سيادة الدول على إقليمها بغض النظر عن جنسية الجاني أو المجني عليه، وبغض النظر عن المصلحة المستهدفة سواء أكانت مصلحة تلك الدولة أو مصلحة دولة أجنبية، أما الوجه السلبي فيعني عدم تطبيق قانون الدولة على الجرائم التي ترتكب خارج إقليمها ولو كان مرتكبها أو المجني عليه من مواطنيها. [3]

والأصل أن عناصر الركن المادي للجريمة يكتمل في نطاق إقليم دولة واحدة، حيث يقع السلوك الإجرامي وتترتب أثاره في إقليم دولة واحدة، بيد أن بعض الجرائم يتجاوز مداها أحيانا حدود الدولة، حينما يتجزأ ركنها المادي أو يتوزع على أكثر من مكان بحيث يمكن وقوع السلوك في إقليم دولة بينما تتحقق النتيجة الجريمة في إقليم دولة أخرى، ويتجلى ذلك في عدد من الجرائم ذات الطبيعة العابرة للحدود الوطنية. وهذا ما يقودنا إلى التساؤل عن مكان وقوع الجريمة في هذه الحالة من أجل تحديد القانون الواجب التطبيق، فهل هو مكان السلوك الإجرامي أم المكان الذي تحققت فيه النتيجة ؟.

انقسم الرأي بخصوص هذه المسألة إلى ثلاث اتجاهات، فذهب الاتجاه الأول إلى أن العبرة في تحديد مكان وقوع الجريمة بالمكان الذي وقع فيه السلوك الإجرامي بغض النظر عن المكان الذي تحققت فيه النتيجة أو المفترض تحققها فيه. [4] وفي المقابل ذهب اتجاه آخر إلى أن مكان وقوع الجريمة يتحدد بالمكان الذي تحققت فيه النتيجة أو من المفترض تحققها فيه. [5]

---

[1]– عدنان الخطيب، موجز القانون الجزائي، الكتاب الأول، المبادئ العامة في قانون العقوبات دون طبعة، مطبعة جامعة دمشق، سوريا، 1963، ص 79

[2]– حسين بن سعيد بن سيف الغافري، المرجع السابق، ص 453

[3]– محمد زكي أبو عامر، قانون العقوبات، القسم الخاص، المرجع السابق، ص 87

[4]– حظي هذا الاتجاه بتأييد كبير من الفقه وهذا ما أخذ به المشرع الفرنسي وكذا المشرع المصري

[5]– أخذ بهذا الاتجاه كل من المشرع الألماني وكذا التركي

وبين هذا وذلك ذهب اتجاه ثالث إلى أن العبرة تكون بمكان حصول أي منهما. [1]

ويعد مبدأ إقليمية القاعدة الجنائية هو القاعدة الأساسية المطبقة في غالبية الدول، فمثلا تنص المادة 113 من قانون العقوبات الفرنسي على أنه يطبق القانون الفرنسي على الجرائم المرتكبة على إقليم الجمهورية، وتعتبر الجريمة قد ارتكبت على إقليم الجمهورية إذا كان أحد عناصر الجريمة قد وقع على هذا الإقليم ".

وفي الولايات المتحدة الأمريكية قرر القضاء الأمريكي عام 1999 في جرائم المراهنات والقمار عبر شبكة الانترنت الاعتماد على مكان مرتكب الجريمة وليس على المكان الذي يتواجد فيه الخادم أو المضيف أو المزود.كما أخذ بمبدأ إقليمية القوانين القانون المصري وذلك في المادة 25 فقرة 1 من قانون العقوبات المصري. [2]

ثانيا مدى تطبيق مبدأ الإقليمية على جريمة التزوير الالكتروني:

يمتد أثر الجريمة الالكترونية إلى خارج إقليم الدولة التي وقع، بل قد تمتد في وقت واحد إلى عديد من دول العالم كما هو الحال في الاعتداءات الفيروسية، فهل سلطات مكان حصول النشاط أي حيث الفيروس في القاعدة الوطنية هي المختصة أو مكان إصابة القواعد في الدول الأخرى، أي حيث حصل الضرر الجنائي أو سلطات كل هذه الأماكن ينعقد لها الاختصاص ؟.[3]

---

[1]– أقر هذا الاتجاه العديد من التشريعات كالمشرع الايطالي وكذا الدانماركي، وكذلك المشرع الجزائري وذلك بنصه في المادة الثالثة من قانون العقوبات بقولها :" يطبق قانون العقوبات الجزائري على كافة الجرائم التي ترتكب في أراضي الجمهورية "، إضافة إلى هذا مصت المادة 586 من قانون الإجراءات الجزائية الجزائري على أنه " تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر ".

[2]– تنص المادة 2 فقرة 01 من قانون العقوبات المصري على أنه :" لا تسري أحكام هذا التشريع على كل من ارتكب في خارج القطر فعلا يجعله فاعلا، أو شريكا في جريمة وقعت كلها أو بعضها في القطر المصري ".

[3]– محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، المؤتمر السادس للجمعية المصرية للقانون الجنائي حول مشكلات السياسة الجنائية في مجال الجرائم الواقعة على البيئة والجرائم الواقعة في مجال تكنولوجيا المعلومات، المنعقد في الفترة ما بين 25–28 أكتوبر 1998، مصر، دار النهضة العربية، مصر، 1993، ص 364 .

وعموما لتحديد مكان وقوع الجريمة أهمية بالغة في تحديد السلطات والمحاكم المختصة لمحاكمة مرتكبيها أي وقع الفعل فيها أو في جزء من دائرة اختصاصها، وعليه فالعبرة في تحديد الاختصاص القضائي هو بأركان الجريمة وليس بآثارها أو بالمكان الذي يظهر فيه دليل من أدلتها. [1]

ويرى مؤيدو هذا الاتجاه أن العبرة بمكان النشاط كون المكان الذي يسهل فيه التحريات عن الجريمة والفاعل بسهولة وبالتالي يكون أدنى إلى تحقيق العدالة[2]، فإذا كانت الجريمة المعلوماتية لها طابع الجريمة المستمرة فهي تعد مرتكبة في جميع الأماكن التي امتدت إليها.[3]

وبناءا على ما سبق نستطيع القول أن قانون دولة ما يمكن أن ينطبق على الكثير من الجرائم الالكترونية طالما أن الاختصاص ينعقد بمجرد وقوع أحد العناصر المكونة للجريمة أو حتى وقوع النتيجة على هذا الإقليم. [4]

ونستنتج مما سبق أنه ولقيام جريمة التزوير الالكتروني يكفي تحقق أحد عناصرها المشكلة لركنها المادي في إقليم دولة ما لتختص تلك الدولة بمكافحتها.إلا أنه يثار هنا تساؤل حول علاقة الفرع بالأصل في موضوع مزور الانترنت وأثر ذلك على الاختصاص القضائي ؟ بمعنى آخر ما مدى إمكانية انطباق قانون دولة يكون فيها مزود الانترنت مجرد فرع أو تابع لمزور آخر مركزه في دولة أخرى خاصة إذا كان هذا الفعل غير مجرم في دولة المركز خاصة وأنه في هذه الحالة الدولة لا تقبل تطبيق القانون الأجنبي على أراضيها ؟.

---

[1]– غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر والقانون، مصر 2013، ص 226 .

[2]– محمد محي الدين عوض، المرجع السابق، ص 364 .

[3]– جميل عبد الباقي الصغير، المرجع السابق، ص 63 .

[4]– وهذا ما أكدته كل من المادة 30 من الاتفاقية العربية لمكافحة تقنية المعلومات والمادة 22 من اتفاقية بودابست، المتعلقة بإجرام الفضاء الالكتروني، وكذا المادة 22 من الاتفاقية الأوروبية حول الجرائم المعلوماتية، والتي تقضي على أنه يجب على كل دولة طرف في هذه الاتفاقيات بمعاقبة الجرائم المنصوص عليها إذا ارتكبت الجريمة ضمن النطاق الإقليمي للدولة .

الفرع الثاني: تطبيق مبدأ الشخصية على جريمة التزوير الالكتروني:

إضافة إلى مبدأ الإقليمية فإن القانون الواجب التطبيق يمكن أن يتحدد أيضا وفقا لمعايير أخرى كمبدأ الشخصية أو مبدأ العينية أو مبدأ العالمية، وغالبا ما تأخذ بها التشريعات الجنائية كمبادئ احتياطية أو مكملة لمبدأ الإقليمية. وقد وجد مبدأ شخصية القاعدة القانونية كتكملة للمبدأ الأصلي، وسنحاول توضيحه فيما يلي:

أولا: تعريف مبدأ الشخصية القاعدة القانونية:

يقصد بمبدأ شخصية القاعدة القانونية –ويطلق عليه أيضا مبدأ الجنسية – أن التشريع العقابي ينطبق على كافة من يحملون جنسية الدولة أيا كان الإقليم الذي ارتكبت فيه الجريمة، بمعنى آخر أن التشريع العقابي يرتبط بجنسية مرتكب الجريمة أو جنسية المجني عليه.[1] فيخضع حسب هذا المبدأ المواطن لقانون بلاده أينما وجد.

ويعد مبدأ الشخصية مكملا لمبدأ الإقليمية فقد يكون هذا الأخير غير كاف لملاحقة المجرمين الذين يرتكبون جرائمهم خارج إقليم الدولة، فالمواطن الذي يرتكب جريمته في الخارج ثم يعود لوطنه قد يفلت من العقاب لأنه لا يخضع لقانون وطنه طبقا لمبدأ الإقليمية بسبب ارتكابه جريمته خارج إقليمها، وفي نفس الوقت لا يمكن للدولة التي يحمل جنسيتها أن تسلمه تطبيقا لمبدأ عدم جواز تسليم الرعايا، فضلا عن ذلك فإنه إذا صدر حكم بالإدانة وتطبيق العقوبة عليه فلن ينفذ الحكم لأنه لن يعود لتلك الدولة مكان جريمته مرة ثانية، وعليه فحتى لا يفلت من العقاب كان لزاما الأخذ بمبدأ الشخصية. [2]

وقد أخذ بمبدأ شخصية القاعدة القانونية المشرع الفرنسي من شقه الايجابي بحيث ينطبق القانوني الفرنسي متى كان الجاني فرنسي الجنسية (المادة 6/113) من قانون العقوبات الفرنسي، وكذلك في شقه السلبي بحيث ينطبق القانون متى كان المجني عليه لحظة ارتكاب الجريمة يتمتع

[1]– جميل عبد الباقي الصغير، المرجع السابق، ص 85 .

[2]– جميل عبد الباقي الصغير، المرجع السابق، ص 57

بالجنسية الفرنسية (المادة 7/113) من قانون العقوبات الفرنسي وكان هذا لحماية للمجني عليه ضد الجرائم التي تقع عليه في الخارج. [1]

أما بالنسبة للمشرع الجزائري فقد نص على مبدأ الشخصية وذلك من خلال المواد 582 و 583 من قانون الإجراءات الجزائية، شريطة أن تكون الجريمة تأخذ وصف جناية في القانون الجزائري، أما إذا كانت جنحة فيجب أن تكون بهذا الوصف في القانونين معا الجزائري والأجنبي، وأن يعود الجاني إلى الجزائر وألا يكون حكم عليه في الخارج، وفي حالة الحكم بالإدانة لابد أن يثبت أنه قضى العقوبة أو سقطت عنه بالتقادم أو حصل على العفو عنها. [2]

كما نصت المادة 584 من قانون الإجراءات الجزائية الجزائري على معاقبة الجاني الجزائري الذي ارتكب الجريمة في الخارج وفقا للقانون الجزائري حتى ولو اكتسب الجنسية الجزائرية بعد ارتكاب الجرم.

وتجدر الإشارة إلى أن المشرع الجزائري وخلافا للمشرع الفرنسي قد أخذ بمبدأ الشخصية أو الجنسية بشقه الإيجابي، أما الشق السلبي والذي يقضي بتطبيق العقوبات على مرتكبي الجرائم في الخارج مهما كان جنسيتهم ضد رعايا الدولة، فلا وجود لهذا المبدأ في التشريع الجزائري. [3]

ثانيا: مدى تطبيق مبدأ شخصية القاعدة الجنائية على جريمة التزوير الالكتروني:

إذا كان الأخذ بمبدأ شخصية القاعدة القانونية يخدم مكافحة الجرائم المرتكبة من طرف مواطن في دولة أجنبية، وأيضا الأجنبي الذي يرتكب جريمة في بلد عن بلده الأم، إلا أنه قد يصطدم بمجموعة من العقبات، فمن ناحية نجد أن محاكمة المجرم الذي يقيم في دولة أجنبية تحتاج إلى إجراءات طويلة وشقة ومكلفة، وذات الشيء نجده عند تنفيذ الأحكام الصادرة في الخارج، كما أن العقاب على ما وقع في الخارج قد يكون فعال ويصطدم بعقبات جمة حتى مع وجود اتفاقيات تسليم

---

[1]– Yves Mayaud, code pénal, 108e edition, Dalloz, Paris, 2001, p115.

[2]– تنص المادة 582 من قانون الإجراءات الجزائية على أن :" كل واقعة موصوفة بأنها جناية معاقب عليها في القانون الجزائري ارتكبها جزائري خارج إقليم الجمهورية يجوز أن تتابع ويحكم فيها في الجزائر .

– غير أنه لا يجوز أن تجري المتابعة أو المحاكمة إلا إذا عاد الجاني إلى الجزائر ولم يثبت أنه حكم عليه نهائيا في الخارج وأن يثبت في حالة الحكم بالإدانة أنه قضى العقوبة أو سقطت عنه بالتقادم أو حصل العفو عنها".

[3]– الهام بن خليفة، المرجع السابق، ص 208.

المجرمين، كون أن الدول التي وقعت أو انضمت إلى هذه الاتفاقيات قليل جدا مقارنة بعدد الدول المرتبطة بالانترنت، أضف إلى ذلك مخاطر تطبيق القانون الوطني على الجرائم التي تقع في الخارج والتي يختص بها القانون الأجنبي في ذات الوقت من شأنها الإطاحة بمبدأ من أهم المبادئ الدستورية وهو عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة، لأن امتداد الاختصاص لقانون دولة ما التي فيها تلقي الرسالة غير المشروعة –والتي تمر عبر شبكة الانترنت – ولقانون الدولة حيث تم البت سوق يؤدي بالطبع إلى محاكمة الجاني لأكثر من مرة عن فعل واحد. [1]

ومن الناحية العكسية قد يكون القانون الوطني غير مختص بنظر الواقعة مما يعني مشقة المضرور من خلال الانتقال إلى الدولة التي ارتكبت الجريمة في حقه لرفع دعواه المدنية. والأخطر من ذلك أن يكون الفعل غير معاقب عليه في هذه الدولة، مما يعني وقوع المجني عليه والمتضرر من الجرم في ظلم شديد.

الفرع الثالث: تطبيق مبدأ العينية على جريمة التزوير الالكتروني:

إذا كان تطبيق قواعد القانوني الجنائي يخضع لمبدأ مستقر وهو مبدأ الإقليمية، إلا أن هذا الأخير قد لا يوف بغرضه كونه مظهرا من مظاهر السيادة، أما بعض الجرائم التي تمس بالمصالح الأساسية للدولة والمرتكبة خارج إقليمها من هنا جاء مبدأ العينية كمبدأ احتياطي لمبدأ الإقليمية، والذي سنحاول بيانه فيما يلي:

أولا: تعريف مبدأ العينية:

يطلق عليه أيضا مبدأ الآثار، ويقصد به أن التشريع العقابي الوطني ينطبق على جرائم معينة تتميز بكونها تمس مصالح الدولة الأساسية والجوهرية حتى وإن وقعت خارج إقليم الدولة وبغض النظر عن جنسية مرتكبها، فالمعول عليه هنا هو طبيعة هذه الجرائم.[2]

ويجد لهذا المبدأ تطبيق في التشريع المقارن كالتشريع الفرنسي بالنسبة للجنايات والجنح والتي تشكل اعتداء على المصالح الأساسية للجمهورية الفرنسية وهذا في المادة 113 من قانون العقوبات

[1]– جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دون طبعة، دار النهضة العربية،2002،مصر،، ص 60.

[2]– حسين بن سعيد بن سيف الغافري، المرجع السابق، ص 458.

الفرنسي والتشريع الأمريكي، الذي قرر امتداد التشريع الأمريكي إلى الجرائم الواقعة في الخارج والتي من شأنها المساس بالمصالح الأمريكية في قانون العلاقات الخارجية، حيث أنه يجعل الاختصاص الأمريكي قائما طالما هناك سلوك ذو تأثير على الإقليم الأمريكي، وأيضا يمتد الاختصاص القضائي الأمريكي ينظر الجرائم الواقعة في الخارج التي يقرر النائب العام إحالتها متى كانت الواقعة تشكل عمل إرهابيا يمس المصالح الأمريكية. [1]

أما المشرع الجزائري فقد أخذ بمبدأ العينية وهذا في المادة 588 من قانون الإجراءات الجزائية الذي بمقتضاها تجوز متابعة وكذا محاكمة كل أجنبي، سواء أكان فاعلا أصليا أو شريكا وارتكب جناية أو جنحة ضد أمن الدولة أو مصالحها الأساسية أو المحلات الدبلوماسية والقنصلية الجزائرية أو أعوانها، وكذا تزييفها لنقود أو أوراق مصرفية وطنية متداولة في الجزائر، وأيضا كل جناية أو جنحة ترتكب إضرارا بالمواطن الجزائري.[2]

والجرائم المعنية بمبدأ العينية وفقا للمادة 588 من قانون الإجراءات الجزائية هي الجنايات والجنح ضد الشيء العمومي والمنصوص عليها في الباب الأول من قانون العقوبات الجزائري والتي تشمل الجنايات الجنح ضد أمن الدولة والمتمثلة في جرائم الخيانة والتجسس وكذا جرائم التعدي على الدفاع الوطني أو الاقتصاد الوطني إضافة إلى الاعتداءات والمؤامرات والجرائم المرتكبة ضد سلطة الدولة وسلامة الوطن، وأيضا جنايات التقتيل والتخريب المخلة بالدولة والجرائم الموصوفة بأفعال إرهابية أو تخريبية وجنايات المساهمة في حركات التمرد.

وقد أضاف المشرع الجزائري أيضا الجنايات والجنح متى سبب مرتكبها أضرارا بالمواطن الجزائري.

[1]– حسين سيد الغافري المرجع االسابق ، ص 459.

[2]– تقضي المادة 588 من قانون الإجراءات الجزائية الجزائري بأنه :" تجوز متابعة ومحاكمة كل أجنبي، وفقا لأحكام القانون الجزائري، ارتكب خارج الإقليم الجزائري بصفة فاعل أصلي أو شريك في جناية أو جنحة ضد أمن الدولة الجزائرية أو مصالحها الأساسية أو المحلات الدبلوماسية والقنصلية الجزائرية أو أعوانها، أو تزييفها لنقود أو أوراق مصرفية وطنية متداولة قانونا في الجزائر أو أي جناية أو جنحة ترتكب إضرارا بمواطن جزائري

ثانيا: مدى تطبيق مبدأ عينية القاعدة الجنائية على جريمة التزوير الالكتروني:

تطبيقا لنص المادة 588 من قانون الإجراءات الجزائية الجزائري فإن تزوير المحررات المصرفية –كصورة من صور التزوير– يشكل جنحة من شأنها إلحاق الضرر بالمصالح الأساسية للدولة الجزائرية، وعليها فإذا وقع هذا التزوير على محررات مصرفية في الجزائر من طرف أجنبي خارج حدود الدولة الجزائرية فهنا يطبق على الجاني القانون الجزائري.

وتشمل المادة أعلاه أيضا جرائم التزوير المنصوص عليها في المواد من 197 إلى المادة 204 من قانون العقوبات الجزائري إضافة إلى التزوير في الأوراق المصرفية المنصوص عليها في المادة 219 من قانون العقوبات.

وحرصا من المشرع الجزائري على مكافحة الجرائم المعلوماتية، فقد تبنى الأخذ بمبدأ العينية من خلال القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهذا ضمن الفصل السادس من القانون تحت عنوان الاختصاص القضائي وتحديدا المادة 15 والتي تقتضي بأنه زيادة على قواعد الاختصاص الجزائية، يعطى للمحاكم الجزائرية الاختصاص بنظر الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج التراب الجزائري، إذا كان مرتكبها جزائريا واستهدف بجرمه هذا مؤسسات الدولة الجزائرية أو دفاعها أو اقتصادها الوطني.[1]

وإذا كان مبدأ العينية يحل مشكلة عدم كفاية مبدأ الإقليمية، إلا أن الأخذ بهذا المبدأ قد يصطدم بمجموعة من العقبات، فمحاكمة المجرم الذي يقيم في دولة أجنبية يحتاج إلى إجراءات طويلة وشاقة، كما أن العقاب على فعل ما وقع في الخارج قد يصطدم بعقبات جمة أهمها مبدأ عدم جواز تسليم الرعايا، حتى مع وجود اتفاقيات تسليم المجرمين، خاصة وأن الدول المنظمة أو الموقعة على اتفاقيات تسليم المجرمين قليل جدا بالمقارنة بعدد الدول المرتبطة بالانترنت.

[1]– المادة 15 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية للجمهورية الجزائرية، العدد 47.

من خلال ما سبق نجد أن المشرع قد أخذ بجميع المبادئ السابقة أما مبدأ العالمية[1] فلم يأخذ به المشرع الجزائري مقتصرا على المبادئ السالفة الذكر متبعا في ذلك خطة معظم التشريعات العقابية. [2]

وهنا يطرح التساؤل عن سبب عدم الأخذ به كمبدأ احتياطي في حالة عدم كفاية المبادئ السابق ذكرها، خاصة وأنه في حالة الأخذ به فهذا يغنينا عن الأخذ بنظام تسليم المجرمين، وهذا تحقيقا للردع العام والخاص وضمانة لعدم إفلات المجرم من العدالة.

فمن المسلم به أن القانون الجنائي وكغيره من فروع القانون العام يعتبر بصورة عامة من أهم مظاهر السيادة، ويطبق على كل الجرائم الواقعة داخل الحدود الإقليمية للدولة وفقا لمبدأ إقليمية القوانين.غير أن الأخذ بهذا المفهوم التقليدي لم يعد على إطلاقه خاصة بعد التطورات الحاصلة على الساحة الدولية نظرا للتقدم التكنولوجي لاسيما في مجال المعلوماتية.

وعليه فبالرغم من أن مبدأ إقليمية القانون ما زال يشكل أساس القانون الجنائي، فإن ضرورة تحسين أداء القانون الجنائي في مواجهة الجريمة أدت إلى إيجاد قيود على مبدأ الإقليمية تهدف إلى الحد من الارتباط المطلق للنصوص الجنائية بإقليم الدولة.

وبالإضافة إلى هذا التطور المتعلق بسريان النصوص الجنائية من حيث المكان، وفقا لمبدأ عالمية النص الجنائي وتطبيق القانون الجزائي الأجنبي الذي تبنته بعض التشريعات، كآلية للتعاون فيما بينها لمكافحة هذا النوع المستحدث من الجرائم التي أصبح مكافحتها من أهم التحديات التي تواجهها الدول بكافة مكونات مؤسساتها البشرية والفنية.

---

[1]– يقصد بمبدأ العالمية مد الاختصاص الوطني في ملاحقة ومحاكمة ومعاقبة مرتكب أنواع معينة من الجرائم يحدها القانون الوطني بغض النظر عن مكان حدوث الواقعة الإجرامية ويصرف النظر أيضا عن جنسية مرتكبيها أو ضحاياها شريطة أن يتم القبض على الجاني ضبطه في إقليم تلك الدولة، بمعنى أن واقعة الضبط هي التي تخول الاختصاص لمحاكم الدولة .للمزيد انظر، عبد الرحمان خلفي، محاضرات في القانون الجنائي العام، دار الهدى ، الجزائر، ص 68 وما بعدها، انظر أيضا : الهام بن خليفة، المرجع السابق، ص 213 وما بعدها

[2]– من بين الدول التي لا تنص في قوانينها الوطنية على مبدأ العالمية الجزائر ومصر، في حين أخذت به بعض الدول لكن يتحفظ، وتعد بلجيكا من أول الدول التي أخذت بهذا المبدأ، إضافة إلى المشرع الفرنسي الذي أخذ به هو أيضا ونص عليه في قانون العقوبات، وذلك تحديدا في المادة 213 من قانون العقوبات، كما أخذت بهذا المبدأ دولة لبنان ونصت عليه في المادة 23 من قانون العقوبات، وأيضا سوريا في المادة 23 من قانون العقوبات والتي أخذت به كمبدأ احتياطي أو ثانوي في حالة ما إذا تعذر الأخذ بمبدأ الإقليمية أو الشخصية أو العينية .

ومن هنا نتساءل ثانية إلى أي حد يمكن أن يساهم تفعيل تطبيق الاختصاص الجنائي العالمي من طرف المحاكم الوطنية لتحقيق هذا الهدف ؟ والذي تواجهه صعوبات قانونية أهمها صعوبة الإثبات واحتمال تنازع الاختصاص والإخلال بمبدأ المحاكمة العادلة، وصعوبات واقعية تتمثل أساس في غياب الإرادة السياسية والتمسك بمبدأ السيادة المطلقة.

الفرع الرابع: أثر خصوصية جريمة التزوير الالكتروني على مسألة الاختصاص القضائي

إن أهم ما تتميز به جريمة التزوير الالكتروني بصفة خاصة والجريمة الالكترونية بصفة عامة هو طابعها المتخطي لحدود الدولة الواحدة ما يعطيها بعدا دوليا، الأمر الذي يطرح في كثير من الأحيان صعوبة عند تحديد الاختصاص.

وكما سبقت الإشارة قد ترتكب الجريمة في إقليم دولة معينة من طرف أجنبي فتكون الجريمة هنا خاضعة للاختصاص الجنائي للدولة التي ارتكبت الجريمة في إقليمها طبقا لمبدأ الإقليمية، وكذا لاختصاص الدولة التي ينتمي إليها الجاني طبقا لمبدأ شخصية القوانين، كما قد تلحق هذه الجريمة تهديدا لأمن وسلامة دولة أخرى، فتدخل هي أيضا في اختصاصها استنادا إلى مبدأ العينية، وهو الأمر الذي يترتب عليه تنازع في الاختصاص بين كل هذه الدول. [1]

لقد ذهب الفقه الجنائي لإيجاد حل لمثل هذا التنازع الإيجابي ذلك بإعطاء الأولوية لأي من الدول المتنازعة وفقا لأحد معايير الاختصاص الذي يكون الأكثر جدوى وفعالية لضمان سرعة ملاحقة الجريمة، وهنا قد يكون مبدأ الإقليمية هو الأكثر قبولا، وذلك أن الدولة التي وقعت في إقليمها الجريمة هي أرجح الدول اختصاصا بملاحقة الجريمة ومعاقبة فاعلها، كون أن أدلة الإثبات متوافرة ومن اليسير إجراء التحقيقات الكفيلة لإظهار الحقيقة.

وقد شهد مفهوم الإقليمية تطورا ملحوظا فيما يتعلق بتحديد مكان وقوع الجريمة الالكترونية، فلم يعد يلازم وقوع فعل مادي أو حتى أحد العناصر المكونة لهذا الفعل، بل بلغ الأمر حد نزع الصفة المادية كلية عن هذا الفعل، تطبيقا لذلك ذهب القضاء الفرنسي إلى القول بتطبيق القانون الفرنسي وعليه اختصاص المحاكم الفرنسية إذا كان مركز البث أو الجهاز الخادم موجدا خارج الإقليم الفرنسي

[1]– جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، المرجع السابق، ص 73.

بينما تظهر الرسائل يبثها هذا الجهاز في فرنسا، واعتبر أن الجريمة مرتكبة في كل مكان تظهر فيه هذه الرسائل محل البحث.

ووفقا لهذا الاتجاه الموسع لمبدأ الإقليمية فإن هناك من اعتبر أن الاختصاص القضائي في الجريمة الالكتروني –عموما– يؤول للدولة التي يوجد بين إقليمها والجريمة علاقة فعلية وجوهرية. [1]

ومن التشريعات المقارنة التي تتجه إلى التوسع في مفهوم الإقليمية التشريع الأمريكي الذي يعطي الاختصاص لمحاكمه الجنائية بمجرد حدوث آثار الجريمة على إقليمها فقد قضي في أمريكا بأنه إذا تم إدخال بيانات من مكان معين وكانت تتضمن ما يشكل جريمة الكترونية، وكانت هذه البيانات مقروءة في دولة أخرى، فإن الاختصاص ينعقد لمحاكم الدولة التي يمكن الاطلاع على تلك البيانات في إقليمها. [2]

وعلى الرغم من اختلاف القوانين المقارنة في تحديد المحكمة المختصة عندما تمر الرسالة الالكترونية المعاقب عليها في إقليم أكثر من دولة، وكان القانون يعاقب في جميع تلك الدول، فإن الحل الأنسب عند بعض الفقه الجنائي، هو أن يؤول الاختصاص لجميع هذه الدول، ما دامت النتيجة تتحقق في بلد آخر غير بلد تحميل الرسالة وإدخالها على الشبكة المعلوماتية، من ذلك أن يرسل المتهم برنامجا من برامج الفيروسات من جهاز يقع في دولة معينة إلى جهاز آخر يقع في دولة ثانية مرورا بجهاز ثالث ورابع في دول أخرى وبالتالي تختص محاكم الدولة التي حدث منها البث والدولة التي انتهى إليه الفيروس والدولة التي مر بها هذا الفيروس بجهاز فيها ،وحتى لا يترك أمر مسألة الاختصاص لمحض اجتهادات الفقه والقضاء كان من اللازم تحديد الموقف القانون الدولي منها من خلال الاتفاقيات الدولية والإقليمية، ففي هذه الإطار يمكن استخدام اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية لتكون أساسا لاتخاذ التدبير اللازمة للحصول على الولاية القضائية على الجرائم المعلوماتية، فقد حددت المادة 15 من هذه الاتفاقية المعايير التي بموجبها يمكن للأطراف والمتعاقدة الحصول على الولاية القضائية على الجرائم التي تشملها أحكام هذه الاتفاقية، ومن ذلك

[1]– شيماء عبد الغني محمد عطا الله، المرجع السابق، ص 367.

[2]– نفس المرجع، ص 368.

نصت هذه المادة على أنه يتعين على كل دولة طرف أن تعتمد ما قد يلزم من تدابير لتأكيد سريان ولايتها القضائية على الجرائم المقررة في الحالات الآتية:

– عندما يرتكب الجرم في إقليم تلك الدولة و عندما يرتكب الجرم ضد أحد مواطني تلك الدولة وعندما يرتكب الجرم أحد مواطني تلك الدولة أو شخص عديم الجنسية مكان إقامته المعتاد في إقليمها.

وعلى المستوى الأوروبي فثمة اتفاقية مجلس أوروبا لمكافحة الجريمة المعلوماتية في المادة 22 من الباب الثالث من هذه الاتفاقية مسألة الاختصاص بنصها على أنه يعتمد كل طرف ما قد يلزم من تدابير تشريعية، وذلك لإقرار الاختصاص بشأن أي جريمة معلوماتية وذلك عندما ترتكب الجريمة: – في إقليمه أو من جانب أحد مواطنيه إذا كانت الجريمة معاقبا عليها بموجب القانون الجنائي بمكان ارتكابها أو في حالة ارتكاب الجريمة خارج الاختصاص القضائي الإقليمي لأي دولة.

بالإضافة إلى أن هذه الاتفاقية لا تستبعد أي اختصاص جنائي يمارسه أحد الأطراف وفقا لقانونه الوطني، وفي حالة مطالبة أكثر من طرف من الأطراف بالاختصاص القضائي بشأن أي جريمة معلوماتية تقررها هذه الاتفاقية، يقوم الأطراف متى كان ذلك ملائما بالتشاور لغرض تحديد الاختصاص القضائي الأكثر ملائمة للمحاكمة، وهذا ما أخذ به المشرع الجزائري بموجب القانون 04/09 في المادة 15 منه، حيث اعتبر أنه وبالإضافة إلى قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكب خارج الإقليم الجزائري عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

والملاحظ على هذا النص أنه ما هو إلا تكرار لقاعدة الاختصاص العيني المنصوص عليها في المادة 588 من قانون الإجراءات الجزائية ولا يشكل إضافة جديدة إلى قواعد الاختصاص مثلما استهل به نص المادة 15 من القانون 04/09.

وبناءا على ما سبق نصل إلى نتيجة مفادها أن الجرائم الالكترونية تستعصي في غالب الأحيان الخضوع للقوالب القانونية التي تحكم مسألة الاختصاص المكاني، وعليه فإن خصوصية هذا الصنف المستحدث من الجرائم تتطلب تجاوز القوالب والمعايير التي طرحها الفقه التقليدي بخصوص مسألة

تنازع الاختصاص والعمل على تبني حلول أكثر مرونة تأخذ في الحسبان النطاق الجغرافي لهذه الجرائم وسهولة ارتكابها والتخلص من آثارها إضافة إلى طالعها التقني والمتطور.

المطلب الثاني: قواعد الاختصاص الجنائي الداخلي:

إن قواعد الاختصاص الداخلي بخصوص جريمة التزوير الالكتروني بصفة خاصة والجرائم الالكترونية بصفة عامة تخضع للقواعد المنصوص عليها في قانون الإجراءات الجزائية والتي يمكن ردها إلى ثلاث أنواع هي الاختصاص الشخصي والمكاني والنوعي مع النص على حالات التوسع أو امتداد الاختصاص في حالات الاستعجال وعليه سنحاول بيان كل هذه القواعد في الفروع التالية:

الفرع الأول: الاختصاص الشخصي:

يحكم الاختصاص الشخصي مبدأ أو أصل عام يتمثل في عدم الاعتداء بشخص الجاني في تحديد الاختصاص، ويسود هذا المبدأ استثناء أو حالات للخروج من هذا المبدأ نوجزها فيما يلي:

أولا: الأصل العام:

الأصل أن اختصاص القضاء الجزائي العادي يشمل الفصل في الدعاوى الجزائية المقامة في جميع الجرائم مهما تكن صفة أو حالة مرتكبها ما دام معاقب عليها بمقتضى قانون العقوبات سواء وقعت داخل الإقليم أو خارجه. [1]

وعليه يقتضي المبدأ العام للاختصاص الشخصي خضوع جميع الأشخاص الذين ارتكبوا جرما معينا لذات القضاء وهذا كنتيجة حتمية لمبدأ المساواة بين الأفراد وفقا لهذا المبدأ فالقضاء الجنائي يختص بالنظر في كل الجرائم المعلوماتية مهما كانت صفة مرتكبها كما فيها جريمة التزوير الالكتروني.

ثانيا: الاستثناءات الواردة في هذا المبدأ:

إن الأخذ بالمبدأ الشخصي في تحديد الاختصاص الجزائي القضائي قد ترد عليه بعض الاستثناءات التي تقتضي الخروج عن هذا المبدأ أو الأصل العام، فقد يحدث أن يجعل المشرع لبعض

[1]– جلال ثروت، تطور الإجراءات الجنائية، دون طبعة، دار الجامعة الجديدة، الإسكندرية مصر، 2003، ص 317.

العناصر الشخصية كالسن والصفة محل نظر واعتبار في مجال الاختصاص، فتكون المحكمة في هذه الحالة مختصة شخصيا إذا كان القانون يقرر اختصاصها بالنسبة لفئة معينة من المتهمين رأي المشرع عدم وضعهم على قدم المساواة مع غيرهم من الأشخاص، وذلك بالنظر إلى حداثة سنهم مثلا أو تمتعهم بصفة خاصة كان يكون عسكريين. [1]

وقد أنشأ لمثل هذه الحالات محاكم خاصة أو استثنائية من أمثلتها محكمة الأحداث المختصة بنظر الدعاوى الخاصة بجرائم الأحداث[2] والمحاكم العسكرية الخاصة بنظر لجرائم العسكريين. [3]

الفرع الثاني: الاختصاص النوعي:

يتحدد اختصاص المحاكم الجزائية نوعيا بالنظر إلى جسامة الجريمة المرتكبة إن كانت تشكل جناية أو جنحة أو مخالفة، وتقسم تشريعات والدول غالبا المحاكم إلى نوعين محاكم للجنايات ومحاكم للجنح والمخالفات، نفصلها فيما يلي:

[1]– حسين بن علي زاهر الهلالي، الاختصاص الجزائي وفقا لأحكام قانون الإجراءات الجزائية، دراسة منشورة في مجلة الأمانة الدورية، مجمع البحوث الدراسات بأكاديمية السلطان قابوس لعلوم الشرطة، العدد 16 – يناير، 2005، ص 48.

[2]– لقد أخذ المشرع الجزائري على الأخذ بهذه الحالات الاستثنائية، وذلك من خلال إنشائه لقسم الأحداث وذلك على مستوى كل محكمة، حماية لهذه الفئة ولمستقبلها خاصة بعد صدور القانون 15–12 المؤرخ في 15 يوليو 2015، المتعلق بحماية الطفل، انظر الجريدة الرسمية رقم 39 المؤرخة في 19 جويلية 2015، الذي ألغى المواد من 442 إلى 494 من قانون الإجراءات الجزائية والخاصة بالقواعد الخاصة بالمجرمين الأحداث ويهدف هذا القانون إلى تحديد قواعد وآليات حماية الطفل الحدث (وهو كل من لم يبلغ الثامنة عشر (18) سنة كاملة)
وقد نصت المادة 80 من القانون 12/15 من قانون حماية الطفل على أنه :" يتشكل قسم الأحداث من قاضي الأحداث رئيسا، ومن مساعدين محلفين اثنين (2)
يقوم وكيل الجمهورية أو أحد مساعدين بمهام النيابة ..... ويختارون من بين الأشخاص الذي يتجاوز عمرهم ثلاثين عاما والمتمتعين بالجنسية الجزائية والمعروفين باهتمامهم وتخصصهم في شؤون الأطفال....."

[3]– أنشأ المشرع الجزائري المحاكم العسكرية وهذا لإخضاع فئة العسكريين لمحاكم عسكرية استثنائية بوصفها جريمة تأديبية تهدد النظام الذي تخضع القوات المسلحة، وعليه يختص القضاء العسكري وتفصل المحاكم العسكرية في الجرائم الالكترونية بما فيها التزوير المرتكبة من قبل العسكريين .

أولا: محاكم الجنح والمخالفات:

تختص المحكمة بالنظر في الجنح والمخالفات – وتعتبر جنحة كل جريمة يعاقب عليها قانون العقوبات الجزائري بالحبس من مدة تزيد على شهرين إلى خمس سنوات أو بغرامة أكثر من 2000 ألفي دينار جزائري.

أما المخالفة فهي كل جريمة يعاقب عليها بالحبس من شهرين فأقل أو بغرامة ألفي (2000) دينار فأقل.[1]

وطالما جريمة التزوير الالكتروني لاسيما تزوير المحررات العرفية أو المصرفية وكذا التجارية، تكيف على أساس أنها جنح، فعليه ينعقد الاختصاص نوعيا لمحكمة الجنح بالنظر في هذه القضايا.

ثانيا: محكمة الجنايات:

يوجد على مستوى مقر كل مجلس قضائي محكمة جنايات ابتدائية ومحكمة جنايات استئنافية ،[2] تختصان بالفصل في الأفعال الموصوفة جنايات وكذا الجنح والمخالفات المرتبطة بها، وتنظر محكمة الجنايات الابتدائية كمحكمة شعبية ذات ولاية عامة في القضايا الموصوفة بأنها جنايات والمحالة إليها بقرار نهائي من غرفة الاتهام أحكام هذه المحكمة قابلة للاستئناف أما محكمة الجنايات الاستئنافية. [3]

ومن خلال استقراء المادة السابقة نستنتج أنه حتى ينعقد الاختصاص لمحكمة الجنايات بالفصل في الجرائم المعروضة عليها يجب أن تتوافر جملة من الشروط هي:

– أن تكون الجريمة المعروضة عليها ذات وصف جنائي أو على الأقل ذات وصف جنحي أو مخالفاتي مرتبطة الجناية موضوع المتابعة ارتباطا قويا ومتماسكا

[1]– المادة 328 من قانون الإجراءات الجزائية .

[2]– أخذ المشرع الجزائي في قضايا الجنائيات بمبدأ التقاضي على درجتين وهذا بتشكيل محكمة جنايات ابتدائية ومحكمة جنايات استئنافية، وهذا كضمانة للمتهم يحفظ بها حقوقه وذلك وفق للشرعية والمحاكمة العادلة وكذا احتراما لكرامة وحقوق الإنسان، وتبنى المشرع هذا المبدأ من خلال تعديله لقانون الإجراءات الجزائية بموجب لقانون 17-07 المؤرخ في 27 مارس 2017 المعدل والمتمم لقانون الإجراءات الجزائية .

[3]– المادة 248 من قانون الإجراءات الجزائية والمعدلة بالقانون 07/17.

– أن تكون هذه الجريمة قد أحيلت إليها بمقتضى قرار إحالة نهائي صادر عن غرفة الاتهام، ولا تختص محكمة الجنايات بالفصل في أي اتهام آخر غير وارد في قرار غرفة الاتهام.[1]

– أن يكون الشخص المحال إليها من الأشخاص البالغ جزائيا.

وعليه فمحكمة الجنايات تختص بالأفعال الموصوفة قانونا بأنها جنايات وهي الجرائم المعاقبة عليها بالإعدام، السجن المؤبد، السجن المؤقت، ولهذه المحكمة كامل الولاية في الحكم جزائيا عن الأشخاص البالغين المحالين إليها بحكم من غرفة الاتهام وإنزال العقوبات المقررة لها قانونا، وليس لها أن تقرر عدم اختصاصها وتختص بالفصل في الدعوى المدنية التبعية عند نظرا فتحكم بالتعويض الذي تراه مناسبا.[2]

ولما كانت جريمة الالكتروني يمكن أن تأخذ وصف الجناية خاصة في مجال التزوير في المحررات الالكترونية المصرفية أو التجارية إذا ارتكب من طرف رجال أحد المصارف، فهنا ينعقد الاختصاص لمحاكم الجنايات بنظر كل الجنح والمخالفات المرتبطة بهذا الجرائم كونها صاحبة الاختصاص ولا يمكنها فقرر عدم اختصاصها[3] وإنما عليها أن تفصل في الدعوى العمومية المحالة إليها، ولو كانت لا تختص بها طبقا لقواعد الاختصاص، فمثلا إذا تبين لمحكمة الجنايات أن جريمة التزوير الالكتروني ليست جناية –وفقا لقرار غرفة الاتهام– إنما تشكل جنحة فيجب عليها أن تفصل فيها بالرغم من عدم اختصاصها بها. [4]

الفرع الثالث: الاختصاص المكاني:

مع اتساع رقعة الدولة واستحالة جمع الاختصاص في محكمة واحدة ما دفع إلى تنظيم القضاء على أساس معيار آخر، معيار يحدد المحكمة المختصة من حيث المكان، بعد أن يتم تحديدها بالنوع والدرجة، وعليه يوجد معيار الاختصاص الإقليمي أو المكاني.

---

[1]– المادة 250 من قانون الإجراءات الجزائية الجزائري.

[2]– عبد العزيز سعد، أصول الإجراءات أمام محكمة الجنايات، دون الطبعة، دار هومة للطباعة والنشر والتوزيع، الجزائر 2010، ص 14 .

[3]– المادة 251 من قانون الإجراءات الجزائية الجزائري.

[4]– الهام بن خليفة، المرجع السابق، ص 228–229.

عليه سنحاول من خلال هذا الفرع التطرق إلى معايير تحديد الإقليمي ثم نتطرق إلى مدى ضرورة توسيع نطاق الاختصاص المكاني، وهذا على النحو الآتي:

أولا: معايير تحديد الاختصاص المكاني:

إن قواعد الاختصاص المكاني تتدخل بعد تطبيق جميع قواعد الاختصاص الأخرى لتحدد المحكمة المختصة محليا أو مكانيا بنظر الدعوى.

وتحدد تشريعات الدول مجموعة من الضوابط أو المعايير يلجأ إليها لتحديد الاختصاص المكاني، ويتحدد هذا الاختصاص بثلاثة معايير هي:

أ- مكان وقوع الجريمة:

مكان وقوع الجريمة هو البقعة من الأرض التي تقع عليها الجريمة والمحكمة التي وقعت فيها الجريمة مختصة مكانيا، ويتم ذلك وفقا لطبيعة الجريمة، كما في حالة إتلاف المعلومات أو البرامج باستخدام القنبلة المنطقية يتم تحديد مكان وقوعها بالمكان الذي وقع فيه الفعل التنفيذي، وفي حالة اختلاف المكان وقوع الفعل عن مكان حدوث النتيجة اعتبر كل من المكانين محلا لوقوع الجريمة، فمثلا لو قام شخص ما ببث فيروس معلوماتي عبر شبكة الانترنت من مكان ما وتحققت النتيجة (تدمير المعلومات) في مكان آخر فإن الاختصاص ينعقد لمكان البث ولمكان تدمير المعلومات. [1]

وفي الجرائم السلبية كما في جريمة التزوير الالكتروني، يتحدد مكان وقوع الجريمة بالمكان الذي كان يجب أن ينفذ فيه العمل أو السلوك الذي يفرضه القانون.أما الشروع في ارتكاب الجريمة، فالمكان يتحدد بالمكان الذي وقع فيه عمل من أعمال البدء في التنفيذ، وقد يحصل أن تتحقق أعمال التنفيذ في أكثر من موقع وبالتالي تختص به أكثر من محكمة.

وفي الجريمة المستمرة كجريمة الدخول أو البقاء غير المشرع في نظام المعالجة الآلية فإن المكان يتحدد بكل محل يقع فيه الاستمرار، وفي الجرائم المتتابعة يعتبر كل محل يقع فيه أحد أفعال الداخلة فيه مكانا لها.

[1]- حسين بن سعيد بن سيف الغافري، المرجع السابق، ص 462

ب- مكان إقامة المتهم:

مكان إقامة المتهم هو المكان الذي يوجد فيه محل إقامة المتهم فعليا ويقصد به المكان الذي يقيم فيه أو يسكنه، وقد يكون حكميا ويقصد به الموطن القانوني الذي يوجد فيه الشخص عادة أو تعرف فيه سيرته وشؤونه.

والعبرة في تحديد هذا المكان يكون بوقت ارتكاب الجريمة، فهذا الأخير هو من ينشئ للدولة حقها في العقاب، وبالتالي حقها في توجيه الاتهام إلى الشخص بسبب الجريمة المنسوبة إليه.[1]

وإذا تعددت أمكنة إقامة المتهم كانت جميع المحاكم التي تتبعها هذه الأمكنة مختصة مكانيا بالجريمة، وإذا غير المتهم محل إقامته في الفترة ما بين ارتكابه الجريمة وبين البدء في اتخاذ الإجراءات ضده، فالعبرة بمحل الإقامة الثاني.

ج- مكان القبض على المتهم:

يقصد بمكان القبض على المتهم وتصح محاكمته فيه بحيث تكون المحكمة التي يقع هذا المكان في دائرتها هي المختص مكانيا بنظر الدعوى، والحكمة المتوخاة هنا تكمن في أنه من الجائز أن يكون قد عثر مع المتهم على بعض الأدلة التي تساعد القاضي على كشف الحقيقة والتي يؤدي نقلها إلى إتلافها أو ضياعها. وهذا الشيء متصور جدا في الجرائم المعلوماتية حيث الأدلة الرقمية، أو لأن الجريمة قد تكون تافهة لا تستدعي نقل المتهم إلى مكان محكمة أخرى، كذلك قد يكون المتهم من معتادي الإجرام الخطرين وبالتالي يكون من الخطورة نقله من مكان القبض عليه أو قد يتعذر معرفة مكان ارتكاب الجريمة [2]. وفي الاختصاص المكاني ثمة تساؤل يثور في الحالة التي تتوافر فيها المعايير الثلاثة السالفة الذكر جميعا فأي منها يقدم على سواه في حالة تنازعها ؟

إن قواعد الاختصاص السالفة الذر تعتبر من النظام وبالتالي لا يجوز للخصوم الاتفاق على مخالفتها صراحة أو ضمنا سواء بالتعديل أو بالإلغاء هذا من ناحية.

[1]- جلال ثروت، المرجع السابق، ص 316.

[2]- حسين بن سعيد بن سيف الغافري، المرجع السابق، ص 463.

ومن ناحية أخرى يعتبر الدفع بعدم الاختصاص من الدفوع الجوهرية التي يجب على المحكمة الرد عليه، ويحق لكل طرف في الدعوى الدفع به وفي أي حالة كانت عليها الدعوى.ومن ناحية ثالثة يحق للمحكمة ودون طلب من الخصوم إثارة موضوع الاختصاص إذا تبين لها أنها غير مختصة بنظر الدعوى والقضاء بعدم الاختصاص.

ويرى الفقه في الجزائر أنه يتعين تفضيل الجهة التي حرت الدعوى العمومية فيها أولا، إلا إذا اقتضى حسن سير العدالة أن تختص بها جهة معينة دون سواها، في حين يرى الفقه الفرنسي أن الادعاء هو الذي يحدد المحكمة والمختصة، إذ هو الذي يختار المحكمة التي يرفع فيها الدعوى.[1]

وما تجدر الإشارة إليه إن قواعد الاختصاص السالف ذكرها، هي ذاتها التي تطبق في الجرائم الالكترونية بما فيها جريمة التزوير الالكتروني.

ثانيا: مدى ضرورة توسيع نطاق الاختصاص المكاني:

إن تمديد الاختصاص المكاني لسلطة البحث والتحدي في الجرائم الالكترونية إلى كامل التراب الوطني ضرورة فرضتها تحديات هذه الجرائم التي تمتاز بسرعة ارتكابها، وهو إجراء يأخذ بعين الاعتبار خصوصية الأدلة الرقمية أو الالكترونية نظرا لما تتسم به من سرعة زوالها وسهولة المساس بها، وعليه فهي تعد حالة من حالات الاستعجال التي تبرر هذا التوسع في الاختصاص هذا من جهة.

ومن جهة أخرى ونظرا للتحولات التي عرفتها الظاهرة الإجرامية – لاسيما في مجال المعلوماتية– ولغياب جهات قضائية متخصصة في مكافحة الأشكال الجديدة للإجرام ودعم فاعلية الجهات القضائية التقليدية أنشأ المشرع الجزائري جهات قضائية داخل نطاق النظام القضائي العادي ومدى لها صلاحية النظر في الجرائم الواردة على سبيل الحصر بموجب القانون 14/04 المؤرخ في 10 نوفمبر 2004، الذي نص على تمديد الاختصاص المحلي لهذه المحاكم وهذا في المواد 37 و

[1]– محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحداث التعديلات التشريعية الجزء الثاني، المرجع السابق، ص 805 .

40 منه دون تحديدها وفعلا فقد صدر المرسوم التنفيذي رقم 348/06[1] المؤرخ في 2006/10/05 المتضمن تمديد الاختصاص المحلي لبعض المحاكم وكلاء الجمهورية وقضاة التحقيق. [2]

ولهذه المحاكم اختصاص إقليمي واختصاص نعي نحاول توضيحهما فيما يلي:

1- الاختصاص الإقليمي:

في إطار الحديث عن الاختصاص الإقليمي أو المحلي للمحاكم الجزائية، تجدر بنا الإشارة إلا أنه قد تم بتاريخ 26 فبراير 2008 تحديد الجهات القضائية المختصة بهذه الجرائم وذلك عن طريق تدشين القطب الجنائي ذو الاختصاص الموسع الكائن مقره بمحكمة سيدي أمحمد بالجزائر العاصمة ضمن تشكيلة تضم 12 قاضيا وذلك ضمن الأقطاب الجزائية الآتية:

أ- الاختصاص الإقليمي لمحكمة سيدي أمحمد (الجزائر العاصمة):

يمتد اختصاصها إلى محاكم ومجالس قضاء كل من: الجزائر، الشلف، الأغواط، البليدة، تيزي وزو، الجلفة، المدية، مسيلة، بومرداس، تيبازة، عين الدفلى. [3]

ب- الاختصاص الإقليمي لمحكمة قسنطينة:

يمتد اختصاصها المحلي ووكيل الجمهورية وقاضي التحقيق لها إلى محاكم المجالس القضائية لـ: قسنطينة، أم البواقي، باتنة، بجاية، بسكرة، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج، الطارف، الوادي، خنشلة، سوق أهراس، ميلة.[4]

ج- الاختصاص الاقليمي لمحكمة ورقلة:

تمثل اختصاصها المحلي واختصاص وكيل الجمهورية، وقاضي التحقيق بها إلى محاكم المجالس القضائية لورقلة، أدرار، تمنراست، إليزي، تندوف، غرداية.[1]

---

[1]- المرسوم التنفيذي 348/06 المؤرخ في 12 رمضان 1427 الموافق لـ 05 أكتوبر 2006 المتضمن تحديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية للجمهورية الجزائرية، العدد 71 الصادرة بتاريخ 27 رمضان 1427 الموافق لـ 05 أكتوبر 2006، ص 29.

[2]- عبد المجيد جباري، عملية تعديل قانون الإجراءات الجزائية بين الإثراء التشريعي والتطبيق القانوني، مجلة المفكر البرلماني، العدد 21، 2008، ص 179.

[3]- المادة 02 من المرسوم التنفيذي رقم 348/06 المتضمن تحديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

[4]- المادة 03 من المرسوم التنفيذي رقم 348/06، المصدر السابق.

د- الاختصاص الإقليمية لمحكمة وهران:

يمتد اختصاصها المحلي واختصاص وكيل الجمهورية وقاضي التحقيق لها إلى محاكم المجالس القضائية لـ: وهران، بشار، تلمسان، تيبازة، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت، النهامة، عين تيموشنت، غليزان. [2]

2- الاختصاص النوعي:

للأقطاب الجزائية صلاحية النظر في بعض أنواع الجرائم الخطيرة والمحددة على سبيل والتي تتمثل في الجرائم المتعلقة بالمتاجرة بالمخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف.

وكان في بادئ الأمر المشرع الجزائري قد أعطى لهذه الأقطاب الجزائية المختصة بنظر الجرائم أعلاه وعلى سبيل الحصر، إلا أنه وبعد صدور الأمر 05/10 بتاريخ 26 أوت 2010 المتمم للقانون 01/06 المتعلق بالوقاية من الفساد ومكافحته أقر بوضع الجرائم المنصوص عليها في هذا القانون باختصاص الجهات القضائية ذات الاختصاص الموسع وفقا لقانون الإجراءات الجزائية وهذا بموجب المادة 24 مكرر 1 فقرة 01 من القانون 01/06.

وطبقا لهذا فقد أعطى قانون الإجراءات الجزائية على مستوى التحقيق لوكلاء الجمهورية وأيضا ضباط الشرطة القضائية اختصاصات أوسع في سبيل تسهيل إجراءات البحث والتحري عن تلك الجرائم وكشف مرتكبيها وجمع الاستدلالات عنها بما يمكن من مجابهة الصعاب التي قد تعترضهم اعتبارا لخطورة تلك الأفعال ولطبيعتها الخاصة. [3]

وقد نصت المادة 40 مكرر من قانون الإجراءات الجزائية على أن الجهات القضائية التي تم توسيع اختصاصها المحلي تخضع لقانون الإجراءات الجزائية المتعلقة بالدعوى العمومية والتحقيق والمحاكمة، غير أن هذه المحاكم تنفرد ببعض الإجراءات الخاصة، حيث يتعين على ضابط الشرطة القضائية أن يخبر وكيل الجمهورية فورا لدى المحكمة الكائن بها مكان أحد الجرائم السابق ذكرها،

---

[1]- المادة 03 من المرسوم التنفيذي رقم 348/06، المصدر السابق.

[2]- المادة 04 من المرسوم التنفيذي رقم 348/06،المصدر السابق.

[3]- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة السادسة، دار هومة للطباعة والنشر والتوزيع، الجزائر 2011، ص 68 .

ويبلغونه بأصل نسختين من إجراءات التحقيق بحيث يرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابع له القطب الجزائي.

فإذا رأى النائب العام المخطر أن الجريمة تدخل ضمن اختصاص القطب الجزائي، فإنه يطلب بالإجراءات فورا، وفي هذه الحالة يتلقى ضباط الشرطة القضائية العاملون بدائرة اختصاص هذه المحكمة التعليمات مباشرة من وكيل الجمهورية لدى القطب الجزائي.ويجوز للنائب العام لدى المجلس القضائي التابع له القطب الجزائي المختص أن يطالب بالإجراءات في جميع مراحل الدعوى.

وفي حالة فتح تحقيق قضائي يصدر قاضي التحقيق أمرا بالتخلي عن الإجراءات لفائدة قاضي التحقيق لدى القطب الجزائي، وهنا يتلقى ضباط الشرطة القضائية التعليمات من قاضي التحقيق للقطب الجزائي المتخصص.

أما بخصوص جريمة التزوير الالكتروني فباعتبارها من الجرائم المعلوماتية المنظمة العابرة للحدود الوطنية، فيختص بها محليا ونوعيا أحد الأقطاب الجزائية المتخصصة والتي يقع في دائرتها ارتكاب هذه الجريمة.

ولقد نص المشرع الفرنسي هو الآخر على تمديد الاختصاص للأقطاب الجزائية الموسعة، والتي تختص بالنظر في مجموعة من الجرائم، وذلك في المواد 43 الفقرة الثانية والمادة 52 فقرة 1 والمادة 382 والمادة 522 من قانون الإجراءات العقابية.

غير أن المتمعن في هذا المواد يجد أن هذا التمديد لا يخص جريمة التزوير طبقا للمادة 441 فقرة 1 وما يليها من قانون العقوبات الفرنسي، فالمشرع الفرنسي لم يذكرها في قائمة الجرائم التي تختص بها هذه الأقطاب، ويفهم من ذلك أن هذه الجريمة لا تمتد فيها الاختصاص بل تخضع للقواعد العامة، وهو ما يؤخذ على المشرع إذ نعتبره إغفال منه على هذه الجريمة نظرا لأنها في البداية كانت من قبيل جرائم الاعتداء على نظم المعالجة الآليات للمعطيات ثم بموجب قود فران الذي عدل قانون العقوبات سنة 1992 أصحبت من قبيل جرائم التزوير في المحررات.[1]

[1]– الهام بن خليفة، المرجع السابق، ص 236.

والجدير بالذكر بصدد امتداد الاختصاص، وعلى عكس تنازع الاختصاص على الصعيد الدولي فإن هذه المشكلة وعلى فرض حصولها على المستوى الإقليمي، في حالة ما إذا باشرت جهات متعددة من أجهزة الضبط القضائي البحث والتحري عن جريمة الكترونية ما في آن واحد، فإن ذلك لا يؤثر على فعالية البحث ولا يمكن اعتباره تنازعا في الاختصاص، يقدر ما يمكن اعتباره تضافرا في الجهود، وهي في جميع الأحوال تتسم بالشرعية طالما أن الاختصاص المحلي في هذه الجرائم تمتد ليشمل كامل إقليم الجمهورية.

المبحث الثاني: القواعد الإجرائية للتحقيق وجمع الأدلة في جريمة التزوير الالكتروني

تعد جريمة التزوير الالكتروني من الأنماط الإجرامية التي فجرتها حديثا ثورة تقنية المعلومات والاتصالات، حيث تعتبر من الجرائم المستحدثة التي لم تكن معروفة في القانون الجزائي الإجرائي، وعليه فأي محاولة للتعامل إجرائيا مع هذا النمط الإجرامي، خاصة في إطار عملية البحث والتحقيق، ما قد يخلق إشكالات في نطاق قانون الإجراءات الذي وضعت نصوصه لتحكيم إجراءات متعلقة بجرائم تقليدية لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع المتعلقة بها.

كل هذه التحديات دفعت بالمشرع الجزائي إلى إعادة النظر في كثير من المسائل الإجرائية، خاصة فيما يتعلق بمسألة الإثبات باعتبارها من أهم موضوعات هذا القانون، ذلك أن الدليل الذي يعتمد عليه إثبات هذا النوع من الجرائم والذي لابد من أن يكون من ذات طبيعتها التقنية، وهو الأمر الذي لا تكون فيه القواعد الإجرائية التقليدية لاستخلاص الدليل قادرة على القيام به، مما يستوجب تدخل المشرع لتكريس قواعد إجرائية يمكن من خلالها للجهات المكلفة بالبحث والتحري من جريمة التزوير الالكتروني والاعتماد عليها وصولا إلى الدليل أو الأدلة التي يمكن الاعتماد عليها في إثبات هذه الجريمة.

وبناءا على ما سبق، سنحاول من خلال هذا المبحث التطرق إلى إجراءات التحقيق وهذا من خلال المطلب الأول، في حين نخصص المطلب الثاني ببيان القواعد الإجرائية لجمع الدليل الالكتروني، وهذا على النحو الآتي:

المطلب الأول: الأجهزة المختصة بالتحقيق في جريمة التزوير الالكتروني:

يعد التحقيق إجراء من أهم الإجراءات التي تتخذ بعد وقوع الجريمة، لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على مختلف أنواعها.وإذا كانت الجهات المكلفة بالتحري والتحقيق عن الجريمة والمجرمين معتادة التعامل مع الجريمة بصورتها التقليدية، والتي يمكن إدراكها بالحواس لما يمكن أن يخلفه مرتكبوها من آثار مادية في مسرح الجريمة من بصمات وآثار أقدام أو بقع دم. ..، فإن مشكلة ستواجه هذه الجهات عند تعاملها مع الجرائم الالكترونية نظرا للبيئة الافتراضية التي ترتكب فيها هذه الجرائم. [1]

ونظرا لخطورة الجرائم الالكترونية بصفة عامة، وجريمة التزوير الالكتروني بصفة خاصة، اتجهت معظم تشريعات الدول إلى استحداث أجهزة متخصصة بمكافحة هذا النوع من الإجرام المستحدث لتتولى مهمة البحث عن هذه الجرائم.

وسنحاول في هذا المطلب بيان الأجهزة المختصة بالتحقيق عن جريمة التزوير الالكتروني في التشريع الجزائري في الفرع الأول،في حين نخصص الفرع الثاني لبيان الأجهزة المختصة بالتحقيق عن جريمة التزوير الالكتروني في التشريع الفرنسي.

الفرع الأول: الأجهزة المختصة بالتحقيق عن جريمة التزوير الالكتروني في التشريع الجزائري

إن الاختصاص العملي والفني في أعمال البحث والتحقيق في الجرائم الالكترونية بصفة عامة وجريمة التزوير الالكتروني بصفة خاصة يعود أساس إلى دائرة مكافحة الجرائم المعلوماتية التابعة للمديرية العامة للأمن الوطني، وكذلك الفرق التابعة لمركز الوقاية من جرائم الإعلام الآلي التابعة للدرك الوطني، إضافة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكل هذه الوحدات الخاصة تتكون أساسا من جملة من المختصين ممن تتوفر لهم صفة ضباط الشرطة القضائية لمباشرة إجراءات البحث والتحقيق في الجرائم الالكترونية. وبناء على هذا سنحاول بيان هذه الجهات والأجهزة كالآتي:

[1]– سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الطبعة الأولى، دار النهضة العربية، مصر، 1999، ص 95.

أولا:اختصاص ضباط الشرطة القضائية بالبحث والتحري في مجال جريمة التزوير الالكتروني:

إذا كان التحري في البيئة الرقمية يتطلب إحاطة السلطة المختصة بالبحث والتحري بتقنية عالية، فهل رصد المشرع الجزائري ضبطية قضائية مختصة ؟ وما مدى ارتباط تأهيل الضبطية القضائية بعنصري الفعالية والشرعية ؟.

ويتولى عادة ضباط الشرطة القضائية مسائل البحث والتحري في كافة الجرائم، بما في ذلك الجرائم المعلوماتية، فلا يوجد مانع قانوني يحد من ممارسة هؤلاء لأعمالهم المتعلقة بالبحث التحري في هذا المجال بعد تبليغهم بوقوعها.[1] سوى توفر شرط الاختصاص النوعي والذي يمكن تحديده في التمتع بصفة ضابط الشرطة القضائية، وذلك تقيدا بنص المادة 05 من الفصل الثالث المتعلق بالقواعد الإجرائية الخاصة بتفتيش النظم المعلوماتية الوارد في القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. [2]

وقد حددت المادة 14 من قانون الإجراءات الجزائية فئات الضبط القضائي والتي تشمل ضباط الشرطة القضائية، وأعوان الضبط القضائي، وكذا الموظفين والأعوان المنوط بهم قانونا بعض مهام الضبط القضائي.[3]

[1]– نصت على ذلك المادة 17 من قانون الإجراءات الجزائية الجزائري وهذا بقولها :" يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12–13 ويتلقون الشكاوى والبلاغات ويقومون بجمع الاستدلالات وإجراءات التحقيقات الابتدائية ..."

[2]– تقتضي المادة 05 من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال فإنه :" يجوز للسلطات القضائية المختصة وكذا ضابط الشرطة القضائية في إطار قانون الإجراءات الجزائية .. الدخول بغرض التفتيش ولو عن بعض إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها ..."

[3]– تنص المادة 14 من قانون الإجراءات الجزائية على أنه :" يشمل الضبط القضائي :

– ضباط الشرطة القضائية،

– أعوان الضبط القضائي،

– الموظفين والأعوان المنوط بهم قانونا بعض مهام الضبط القضائي ".

واعتنت المواد 15-19-20-21-27-28 من قانون الإجراءات الجزائية الجزائري بتعداد الموظفين والأعوان الذين تثبت لهم صفة الضبطية القضائية، المحددة بالمادة 14 السابقة الذكر، فجاءت المادة 15 من ذات القانون محددة لمن تثبت لهم صفة ضابط شرطة قضائية. [1]

وجاءت المادتان 19 و 20 لتحديد طائفة الأعوان[2]، في حين حددت المادتان 21 و 28 طوائف الموظفين الموكول إليهم بعض مهام الضبط القضائي[3]، أما المادة 27 فقد أحالت على القوانين الخاصة التي تخول الموظفين والأعمال مباشرة بعض سلطات الضبط القضائي. [4]

والملاحظ أن المشرع الجزائري وعبر مختلف التعديلات الواردة على قانون الإجراءات الجزائري، وكذا القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصالات ومكافحتها، قد أبقى على أجهزة الضبطية القضائية التقليدية في مواجهة هذا الإجرام، خلافا لغالبية الدول التي عملت على إيجاد أجهزة ضبط قضائي مختصة على مستوى المصالح الأمنية، حيث اكتفى بالنص على التدابير الإجرائية لمواجهة الإجرام المعلوماتي دون أو تؤهل أجهزتها على الوجه اللازم، خاصة وأن الإجراءات الجنائية المعلوماتية لا تعتمد فقط على التدريبات البدنية أو الفيزيولوجية لمأموري الضبط القضائي، وإنما تعتمد على قوة تكوين البناء العلمي والتكنولوجي لضباط الشرطة القضائية حتى تتولى

---

[1]- تنص المادة 15 من قانون الإجراءات الجزائية الجزائري على أنه :" يتمتع بصفة ضابط الشرطة القضائية :
1- رؤساء المجالس الشعبية البلدية،
2- ضباط الدرك الوطني،
3- الموظفون التابعون للأسلاك الخاصة للمراقبين، ومحافظي وضباط الشرطة للأمن الوطني،
4- ذوو الرتب في الدرك، ورجال الدرك الذين أمضوا في سلك الدرك الوطني ثلاث (3) سنوات على الأقل، والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع الوطني، بعد موافقة لجنة خاصة،
5- الموظفون التابعون للأسلاك الخاصة للمفتشين وحفاظ وأعوان الشرطة للأمن الوطني الذين أمضوا ثلاث (3) سنوات على الأقل بهذه الصفة والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية والجماعات المحلية، بعد موافقة لجنة خاصة،
6- ضباط وضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصيصا بموجب قرار مشترك صادر عن وزير الدفاع الوطني ووزير العدل،
يحدد تكوين اللجنة المنصوص عليها في هذه المادة وتسييرها بموجب مرسوم."

[2]- انظر المادتان 19 ،20من قانون الإجراءات الجزائية الجزائري.

[3]- انظر المادة 21 من قانون الإجراءات الجزائية الجزائري.

[4]- المادة 27 من قانون الإجراءات الجزائية الجزائري

مهمة جمع الاستدلالات في العالم الافتراضي من أجل كشف النقاب عن هذا النوع المتميز من الإجرام. [1]

فالتحري في الجرائم الالكترونية بشكل عام وجرائم التزوير الالكتروني بشكل خاص يتسم بالعديد من المعوقات التقنية التي من شأنها أن تعرقل عملية التحري وتؤدي إلى نتائج سلبية. فالمستوى المتدني لرجال الأمن والمحققين العالمين في مجال مكافحة الجرائم الالكترونية هو حيز معين لمرتكبي هذه الجرائم، ولقد أثبت الواقع أن بعضا من أعضاء الضبط القضائي قد أعانوا مجرمي المعلوماتية على ارتكاب جرائمهم عن جهل ودون قصد بدلا من ضبطهم، وذلك نظرا لعدم امتلاكهم المعرفة اللازمة للتعرف على مثل هذه الجرائم ووسائل ارتكابها.[2] كما أن هذا الأمر قد أدى بهم في كثير من الأحيان إلى التسبب في إتلاف آثار الجريمة وتدميرها من غير عمد نتيجة الإهمال أو الخطأ أو لعدم التعامل مع هذه الآثار بصورة مهنية. [3]

ونؤكد في هذا السياق أن فعالية مرحلة البحث والتحري مرهونة بمدى تمتع أعضاء الضبط القضائي بالمهارات الفنية للاستدلال عن الجرائم الالكترونية ولحين استكمال متطلبات تأهيل الضبطية القضية، نرى أنه من المفيد إعطاء صفة الضبط القضائي للعاملين في المجالات ذات الصلة بنظم المعلومات والاتصالات ولو كان ذلك بصفة مؤقتة، ويكون من المفيد أيضا تجنيد مهندسين وخبراء في مجال المعلوماتية مستقبلا ضمن مختلف جهات الضبط القضائي. [4]

---

[1]– نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، الطبعة الأولى،دار الفكر الجامعي،مصر، ص 100.

[2]– محمد الأمين البشري، التحقيق في الجرائم المستحدثة،الطبعة الأولى، مركز البحوث والدراسات، السعودية، 2004، ص 107.

[3]– هشام محمد فريد رستم، المرجع السابق، ص 439.

[4]– محمود عبد الحميد عبد المطلب، بحث بعنوان جرائم استخدام شبكة المعلومات العالمي (الجريمة عبر الانترنت)، بحث مقدم إلى مؤتمر القانون والكمبيوتر، المنعقد في الفترة بين 1 و3 ماي 2000، الطبعة الثالثة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004، ص 231.

وقد أشارت بعض الدراسات إلى أن الضبطية القضائية تصطدم في متابعة المجرم المعلوماتية نتيجة عدم الإلمام بكافة التشريعات الداخلية والدولية،[1] لاسيما في ظل القصور التشريعي وعدم إسقاط النصوص التجريم التقليدية على نصوص هذا النوع من الإجرام المستحدث.

في الأخير نرى أن الاعتماد على الضبطية التقليدية في البث والتحري عن جريمة التزوير الالكتروني وجرائم المعلوماتية عموما يؤدي إلى إهدار الفعالية والشرعية، والضمانة الأساسية لإعادة التوازن بين عنصري الفعالية والشرعية من خلال سلطة البحث والتحري هو إعادة تأهيل هذه الأخيرة من الناحية الفنية والتقنية، إضافة إلى إكسابها ثقافة قانونية واسعة للقوانين الوطنية والدولية على حد السواء.

ثانيا- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

انسياقا وراء فكرة أن الجريمة الالكترونية هي جريمة دولية تستدعي تعاونا دوليا لنجاح التصدي لها، فقد نصت الاتفاقية الأوروبية للجريمة المعلوماتية على وجوب إنشاء شبكة طوارئ دائمة لتفعيل المساعدة المتبادلة وهذا بموجب نص المادة 35 منها، وتطبيقا لهذا استحدث المشرع الجزائري الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[2] ومكافحتها بموجب القانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها، في المواد 13 و 14 من هذا القانون.

وتمارس الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته مجموعة من الصلاحيات والمهام منها ما هو وقائي يرمي إلى منع وقوع الجريمة المعلوماتية باتخاذ تدابير وقائية، ومنها يرمي إلى الكشف عن مرتكبيها، وهي تشكل على المستوى الدولي مركز اتصال في التبادلات والتعاون الدولي في مجال جمع المعطيات عن مرتكبي الجرائم المعلوماتية.

---

[1]- عبد الرحمان محمد بحر، معوقات التحقيق في جرائم الانترنت -دراسة مسحية على ضباط الشرطة بمنطقة البحرين، رسالة ماجستير في العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض 1992، ص .103

[2]- يقصد بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال حسب نص المادة 02 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنها :" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية ".

وتتولى الهيئة وفقا للمادة 14 تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي يجريها بشأن هذه الجرائم بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، وأيضا تبادل المعلومات مع نظيراتها في الخارج وعند جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم.

أ- التعريف بالهيئة واختصاصاتها:

استلزم الأمر لصدور التنظيم الذي طرحته نص المادة 13 السالفة الذكر الانتظار لمدة 06 سنوات كاملة، أين صدر المرسوم الرئاسي 15-261 بتاريخ 08 أكتوبر 2015 والذي اعتبر الهيئة حسب المواد من 01 إلى 04 منه بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال، توضع لدى وزير العدل المكلف، يقع مقرها بالجزائر العاصمة، تتولى المهام المنصوص عليها في المادة 14 من القانون 09-04 وذلك تحت رقابة السلطة القضائية وطبقا لأحكام قانون الإجراءات الجزائية.

وقد بينت الفقرة 02 من المادة 04 من المرسوم الرئاسي 15-261 المهام الأساسية التي تكلف بها الهيئة والمتمثلة في الوقاية من الجرائم المعلوماتية ومكافحتها وذلك من خلال الإسهام في أعمال البحث والتحقيق ومد يد العون لمصالح الشرطة القضائية و اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من خلال تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته إضافة إلى مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات والخبرات القضائية و ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية، والماسة بأمن الدولة وذلك تحت سلطة قاضي مختص وذلك كاختصاص حصري،كما تعمل الهيئة على تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مسارها من أجل استعمالها في الإجراءات القضائية و المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا المعلومات.

وتعمل في الجانب الدولي على تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المعلوماتية.

- ب- تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

تشكل الهيئة إداريا [1] من لجنة مديرة، ومديرية عامة، اللجنة المديرة تشكل من الوزير المكلف بالعدل رئيسا إضافة إلى الوزير المكلف بالداخلية والوزير المكلف بتكنولوجيات الإعلام والاتصال وقائد الدرك الوطني، والمدير العام للأمن الوطني، وممثلين أحدهما عن رئاسة الجمهورية والآخر عن وزارة الدفاع الوطني يكملهما قاضيان من المحكمة العليا. [2]أما المديرية العامة فيرأسها مدير عام يعين بموجب مرسوم رئاسي[3]، وتتمثل مهام هذه المديريات في ضبط برامج عمل الهيئة ودراسة مشروع الميزانية وتقديم تقارير خاصة بنشاط الهيئة[4]، وبالتالي فهي لا تسهم في الإجراءات الخاصة بالوقاية أو بمكافحة الجرائم المعلوماتية.

وعليه نلاحظ مما سبق أن هذه الهيئة تتوفر على تشكيلة متنوعة من مختصين في مجال التقنية لذلك فهي تساهم في تكوين المحققين المختصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال، ما يساهم في التحقيق من ميزانية الدولة، فعوض أن تبعث الدولة إطارات من الدرك الوطني إلى بلدان أجنبية كفرنسا والولايات المتحدة الأمريكية تكتفي بتكوينهم وتأهيلهم في هذه الهيئة، وبالتالي تطوير كفاءات سلك الدرك الوطني، حتى تكون أكثر عملية في مكافحة الجرائم المعلوماتية. [5]وإضافة إلى اللجان الإدارية تضم الهيئة مديريات تتسم مهامها وتشكيلها بالطابع التقني،

---

[1]- المادة 06 من المرسوم الرئاسي 15-261 ، المحدد لتشكيلة وتنظيم وسير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. .

[2]- المادة07 من المرسوم الرئاسي 15-261 المحدد لتشكيلة وتنظيم وسير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. .

[3]- المادة 09 من المرسوم الرئاسي 15-261 المرسوم الرئاسي 15-261 المحدد لتشكيلة وتنظيم وسير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

[4]المادة 08 من المرسوم 15-261 المرسوم الرئاسي 15-261 المحدد لتشكيلة وتنظيم وسير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

[5]- حسين ربيعي، المرجع السابق، ص 196.

باعتبارها المختصة بإنجاز المهام التقنية المتعلقة بالوقاية ومكافحة الجرائم المعلوماتية وتتمثل هذه المديريات في:

1-مديرية المراقبة الوقائية واليقظة الالكترونية:

نصت على هذه المديرية المادة 11 من المرسوم الرئاسي 15-261 وتعد هذه المديرية المركز العملياتي للهيئة كونها تتولى الجانب التقني الخاص وهذا بإنجاز الأعمال المتعلقة بالبحث والتحقيق في الجرائم الالكترونية، ولعل أن ما يزيد من دورها الفعال هو تنصيبها على رأس مركز العمليات التقنية وكذلك الملحقات مما يبرز دورها الفعال في تسيير وتأطير الأعمال المتعلقة بالوقاية أو بمكافحة الجرائم المعلوماتية.

2- مديرية التنسيق التقني:

نصت عليها المادة 12 من المرسوم الرئاسي 15-268 وتتمثل مهامها في الدور الوقائي والإعلامي كونها تتولى بإنجاز الخبرات القضائية وتكوين قاعدة معطيات تحليلية للإجرام المعلوماتي مع إعدادها لإحصائيات وطنية حول الإجرام المعلوماتي، إضافة إلى تسيير المنظومة المعلوماتية وإدارتها. إلا أن المرسوم الرئاسي 15-261 لم ينص على تشكيلة هذه المديرية، مما يترك المجال للقول بأن تشكيلتها تكون بناء على قرارات مشتركة بين وزراء العدل والدفاع والداخلية كما هو الحال بالنسبة لمديرية المراقبة الوقائية واليقظة الالكترونية.

وفعلا فإن هذا الدور الذي أناطه المشرع بهذه الهيئة على درجة بالغة من الأهمية ومن شأنه أن يحقق الفاعلية المتوخاة من مرحلة البحث والتحري، خاصة بعد صدور المرسوم الرئاسي 15-261 المحدد لكيفيات تنظيم وسير الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها، والذي سبق صدروه العديد من الإشكالات لاسيما فيما يتعلق بتشكيلة الهيئة وطبيعتها القانونية، ومدى مساهمتها في عمليات البحث والتحري في الجريمة الالكترونية دون اكتسابها لصفة الضبطية القضائية خاصة بعد التأخر الكبير لصدور هذا المرسوم.

ثالثا: الأجهزة المختصة على مستوى الأمن الوطني:

تضع مديرية الأمن الوطني في إطار تجسيد سياسة أمنية فعالة، كافة الإمكانات البشرية والتقنية المتاحة لديها لأجل التصدي لكل أنواع الجرائم، خاصة الجرائم المستحدثة ومن بينها، الجرائم الالكترونية، وهذا حماية للمصلحة العامة والخاصة على حد سواء نظرا لما تشكله هذه الجرائم من آثار وخيمة.تجسيدا لذلك أنشأت المديرية العامة للأمن الوطني وحدات متخصصة لمكافحة هذا النوع من الإجرام، إضافة إلى وحدات متخصصة على المستوى الجهوي نوضحها فيما يلي:

أ- على مستوى المديرية العامة:

بادرت المديرية العامة للأمن الوطني إلى تحديث بنيتها الهيكلية بغية خلق وحدات متخصصة تعمل كل منها على مكافحة نوع معين من الجرائم دون سواها، ولذلك قامت المديرية العامة للشرطة القضائية باستحداث أربع (04) مصالح مختصة في شكل مديرية الشرطة العلمية و نيابة مديرية الاقتصادية والمالية وكذا نيابة القضايا الجنائية إضافة إلى مصلحة البحث والتحليل

وبخصوص مكافحة الجرائم الالكترونية فقد أسندت المهمة لنيابة مديرية الشرطة العلمية والتقنية، تتولى أعمال البحث والتحري والتحقيق بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والمتمثلة في المخبر المركزي للشرطة العلمية الكائن مقره بالجزائر العاصمة ،[1] إضافة إلى المخبر الجهوي للشرطة العلمية الكائن مقره قسنطينة، وكذلك المخبر الجهوي للشرطة العلمية والكائن مقره بوهران، إضافة إلى ثلاث (03) مخابر أخرى وهذا على مستوى ورقلة، بشار، تمنراست، تتولى مهام البحث والتحقيق وتحليل الأدلة بمختلف أنواعها. [2]

ب- على المستوى الجهوي:

إضافة إلى المخبر المركزي للشرطة العلمية والتقنية بالجزائر العاصمة، يوجد أيضا مخابر جهوية على مستوى ولايات قسنطينة ووهران تتولى أعمال البحث والتحري بشأن الجرائم المعلوماتية،

[1]- المخبر المركزي للشرطة العلمية والتقنية أو المعهد الوطني للشرطة الجنائية، هو أحد مراكز تكوين الشرطة الجزائري تم انشاؤه سنة 1999، تلبية للحاجات التكوينية التخصصية للشرطة الجزائرية مقره الجزائر العاصمة، يضم 15 مصلحة يحتل المرتبة الثانية إفريقيا والأولى عربيا بين مخابر الشرطة .

[2]- للمزيد أنظر الموقع الرسمي للشرطة العلمية : www.dgsn.dz

وذلك تحت تسمية دائرة الأدلة الرقمية والآثار التكنولوجية والذي يضم ثلاث (03) أقسام فرعية هي قسم استغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات وقسم استغلال الأدلة الناتجة عن الهواتف النقالة، وأخيرا قسم لتحليل الأصوات، ويهتم بضمان الدعم التقني لمختلف مصالح الشرطة والأجهزة القضائية في مجال التحريات الالكترونية والكشف عن أسرار الجريمة الالكترونية من خلال الإجراءات التي تباشرها إما أثناء مرحلة البحث والاستدلال أو أثناء مرحلة التحقيق القضائي.[1]

رابعا: الأجهزة المختصة على مستوى الدرك الوطني:

يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة على مستوى القيادة العامة، أو على مستوى القياديات والمحلية، والمتمثلة في: قيادة الدرك الوطني، الوحدات الإقليمية، الوحدات المشكلة، الوحدات المتخصصة ووحدات الإسناد، هياكل التكوين المعهد الوطني للأدلة الجنائية وعلم الإجرام، إضافة إلى المصالح والمراكز العلمية والتقنية، والمصلحة المركزية للتحريات الجنائية.[2]

وتعمل مؤسسة الدرك الوطني إلى التطلع بمختلف الجرائم المرتكبة على شبكة الانترنت، وهذا لتسهيل مهمة البحث والمعاينة والتفتيش في أنظمة الحواسيب والعمل على مراقبة مختلف الشبكات، وبناء على ذلك تم وضع مصالح الشرطة القضائية التابعة للدرك الوطني في خدمة هذه الأهداف، حسب الاختصاص والصلاحيات وطبيعة الجريمة إلى ثلاث مستويات: مركزية، جهوية ومحلية.[3]

وسنحاول بيان هذه المصالح والمديريات في النقاط الآتية:

أ- أجهزة الدرك الوطني على المستوى المركزي:

يمكن إبراز هذه الأجهزة في المعهد الوطني للأدلة الجنائية، إضافة إلى مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها، وكذلك مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الاستعلام والأمن.وسنحاول تفصيل هذه الأجهزة والمصالح فيما يلي:

---

[1]- للمزيد أنظر : حسين ربيعي، المرجع السابق، ص 179 وما بعدها.

[2]- للمزيد انظر الموقع الالكتروني الرسمي لقيادة الدرك الوطني :
www.mdn.dz/sitecgn/index.php2l=ar8p=undefined

[3]- حسي ربيعي، المرجع السابق، ص 183

1- المعهد الوطني للأدلة الجنائية وعلم الإجرام:

يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام الكائن مقره بوشاوي مؤسسة عمومية ذات طابع إداري، تم استحداثه بموجب المرسوم الرئاسي 183/04 المؤرخ في 26 جوان 2004[1]، في إطار عصرنة قطاع الدرك الوطني، وهي يشكل أداة مستلهمة من الخبرات التطبيقية والتحاليل الحديثة والمدعومة بالتكنولوجيات المناسبة.[2] ويعد المعهد بمثابة هيئة مختصة في إجراء الخبرات والمعاينة وذلك بمختلف دوائره ومنها دائرة الإعلام الآلي والإلكترونيك، التي تختص بتحليل الأدلة الخاصة بالجرائم المعلوماتية، وذلك من خلال تحليل الدعامات الالكترونية، وإصلاح الدعامات التالفة، وإنجاز المقاربات الهاتفية.[3]

2- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها:

يعد مركز الوقاية من جرائم الإعلام والجرائم المعلوماتية ومكافحتها هيكلا متخصصا تابعا لقيادة الدرك الوطني، يقع مقره بالجزائر العاصمة بالدائرة الإدارية لبئر مراد رايس.ويوفر هذا المركز المساعدة التقنية للمحققين ويساهم في توجيه التحقيقات المرتبطة بتكنولوجيا الإعلام والاتصال، كونه هيئة تقنية تعمل تحت وصاية مديرية الأمن العمومي والاستعمال لقيادة الدرك الوطني.ولممارسة صلاحياته تم تقسيمه إلى عدة أقسام، قسم اليقظة المعلوماتية، قسم التحقيقات المعلوماتية، قسم الأمن الرقمي، مصلحة التقنية والاستغلال وأخيرا مصلحة الإدارة والوسائل.

ومن صلاحيات مراكز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ضمان يقظة عامة ومستمرة على شبكة الانترنت والوقاية من كل أنواع الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها وكذا تقديم المساعدة للتنظيمات العمومية الوطنية بخصوص هذه الجرائم.[4]

---

[1]- المرسوم الرئاسي رقم 183/04 المؤرخ في 8 جمادى الأولى عام 1425 هـ الموافق لـ 26 جوان 2004 م، المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام وتحديد قانونه الأساسي، الجريدة الرسمية للجمهورية الجزائرية، العدد 41 الصادرة في 27 جوان 2004.

[2]- حسين ربيعي، المرجع السابق، ص 184 .

[3]- المادة 06 من المرسوم الرئاسي 183/04 مهام المعهد الوطني للأدلة الجنائية وعلم الإجرام .

[4]- حلاب منير، دور الدرك الوطني في ميدان محاربة الجرائم المعلوماتية، الملتقى الوطني حول الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها يومي 16-17 نوفمبر 2015 كلية الحقوق، جامعة بسكرة، الجزائر، ص 3.

3- مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الاستعلام والأمن.

تم إنشاء مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الاستعلام والأمن وهذا على مستوى مديرية الأمن الداخلي بدائرة الاستعلام والأمن بوزارة الدفاع الوطني، وهذا بموجب المرسوم الرئاسي 14-183 المؤرخ في 11 يونيو 2014.[1]

يسير هذه المصلحة ضابط سام يعين طبقا للأحكام التنظيمية المعمول بها في وزارة الدفاع الوطني.[2] وقد حددت مهامها بصفة دقيقة وعلى سبيل الحصر. [3] وتقوم بضبط الإجراءات القضائية اللازمة لجمع الأدلة المادية والمعنوية المرتبطة بالجرائم ولجنح التابعة لاختصاصها.[4] كما تقوم هذه المصلحة بمعالجة الآثار القضائية للقضايا المتصلة بأمن الإقليم، الإرهاب، التخريب والجريمة المنظمة، هذا بالإضافة إلى المساهمة في الوقاية من أي شكل من أي أشكال التداخل الأجنبي، وفي قمعه، كما تساهم في الوقاية من الإجرام المتصل بالتكنولوجيات الجديدة للإعلام والاتصال، وفي قمعه.

ب- أجهزة الدرك الوطني على المستوى الجهوي:

تختص المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني بالتنسيق بين مختلف الوحدات، للشرطة القضائية، إضافة إلى دعمها بالوسائل الخاصة للتحريات والأبحاث المعقدة الخاصة بالجريمة الالكترونية، وبالتالي تساهم هذه الوحدات في تدعيم نشاط الأبحاث والتحريات التي تقوم بها الفرق الإقليمية للدرك الوطني.وهذه الأخيرة أعيد تنظيمها بتاريخ 21 جويلية 2007 بموجب التعليمة رقم 4-223 لسنة 2007 الصادرة عن ديوان قيادة الدرك الوطني، وذلك لتتماشى مع طبيعة الجرائم محل المعاينة، وهو ما يسمح بإنشاء خلية متخصصة لمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام

[1]- المرسوم رقم 14-183 المؤرخ في 13 شعبان 1435 الموافق لـ 11 يونيو سنة 2014، المتضمن إنشاء التحقيق مصلحة القضائي لمديرية الأمن الداخلي بدائرة الاستعلام والأمن ومهامها وتنظيمها، الجريدة الرسمية للجمهورية الجزائرية، العدد 32، الصادر في 12 يونيو 2014، ص 4.

[2]- المادة 02 من المرسوم 14-183،المصدر السابق.

[3]- المادتان 5-6 من المرسوم 183/14، المصدر السابق.

[4]- المادة من 7المرسوم 183/14،المصدر السابق .

والاتصال، وهو ما يسمح بتطبيق سياسة فعالة في مكافحة هذه الجرائم لاسيما في مجال أعمال البحث والتحقيق فيها. [1]

الفرع الثاني: الأجهزة المختصة بالبحث والتحري عن جريمة التزوير الالكتروني في التشريع الفرنسي

يعتبر النظام القانوني الفرنسي هو مصدر الهام بالنسبة للتشريع الجزائري، وهو الأقرب للنظام الجزائري من حيث وجهات النظر التشريعية والقانونية، وهذا ما دفعنا إلى التطرق إلى أجهزة الضبط القضائي المختصة بالبحث والتحري وجمع الأدلة في مجال الإجرام المتصل بتكنولوجيات المعلومات والاتصالات، نظرا للقيمة التي أولاها المشرع الفرنسي لدور الضبطية القضائية في محاربة هذه الظاهرة، وهذا من خلال رصده لأجهزة متعددة لمسايرة التطور المتسارع الذي تشهده مثل هذه الجرائم.

وعليه فيعتبر النظام الفرنسي من الأنظمة الفاعلة، والأكثر تطورا وتماشيا مع الجرائم الالكترونية، وذلك من خلال تبني سياسة وإستراتيجية في مواجهة هذه الجرائم.وهذه الأجهزة تتواجد على مستوى مصالح الشرطة وعلى مستوى مصالح الدرك الوطني وتوجد أيضا على مستوى الجمارك. وسنحاول بيان هذه الأجهزة كالآتي:

أولا: على مستوى الشرطة:

توجد على مستوى الشرطة الفرنسية العديد من الأجهزة المختصة بالبحث والتحري في الجرائم الالكترونية، منها ما يتمتع باختصاص وطني، ومنها ذات اختصاص إقليمي، سنحاول بيانها فيما يلي:

أ- المكتب الوطني لمكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصال:

يعد المكتب أو المرصد الوطني لمكافحة الجرائم المرتبطة بتكنولوجيات المعلومات والاتصال هيئة وزارية مشتركة، أنشأت بموجب المرسوم البيوزاري المشترك رقم 2000- 405 المؤرخ في 15 ماي 2000، وذلك على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية[2]، وهو

[1]- للمزيد : انظر : حسين ربيعي، المرجع السابق ،ص ص 186،187 .

[2]- تنص المادة من المرسوم الوزاري 2000-405 على أنه :

عبارة عن هيئة مختصة عبر كامل الإقليم الفرنسي تنشط في مجال الجريمة المعلوماتية، وقد جاء خلفا للفرقة المركزية لقمع الجريمة المعلوماتية المنشأة عام 1994، ويتولى هذا المرصد تسيير عمليات البحث والتحقيق الخاصة بجرائم المعلوماتية. ويعتبر هذا المرصد نقطة وصل مركزية تسمح بتبادل المعلومات مع مختلف الهيئات الدولية المختصة في هذا المجال كالأنتربول. [1]

ويتكون المكتب من رجال الشرطة والدرك الذين يعملون معا لمكافحة الجريمة المعلوماتية ويتدخلون في القضايا على المستويين الوطني والدولي، سواء بمد يد المساعدة أو بتبليغ مشترك في إطار التحقيقات المرتبطة بتكنولوجيات المعلومات والاتصال كتلك المتعلقة بتعطيل الأنظمة الحاسوبية، تزوير بطاقات الدفع والاعتداء على الأشخاص والمعلومات ويستعين هذا المكتب أو المرصد في أداء مهامه بوحدتين:

1- وحدة العمليات:

تتكون هذه الوحدة من فرق بحث وتحري مختصين، عددها خمسة وتتمثل في: فرقة مختصة في الجرائم المتعلقة ببطاقات الدفع الالكترونية، وفرقة مختصة بجرائم الاحتيال ضد موردي خدمات الاتصال، فرقة مختصة بالبحث في الجرائم الماسة بنظم الدفع الالكتروني، وفرقة مختصة بالبحث والتحري في جرائم القرصنة الالكترونية، وفرقة البحث والتحري خاصة بجرائم النصب والاحتيال الالكتروني.[2]

«L'office pour domaine de compétence, les informations spécifique a la criminalité liée aux technologie d'information et de la communication, dans les conditions fixés a l'article 3 sa compétence s'étend également taux infractions dont la commission est facilitée ou liée a l'utilisation de ces technologies ».

[1] – Quemener-Myriam, la coopération entre les organes de lute contre la cybercriminalité pour une stratégie globale de cyber sécurité française, Revue LAMY droit des affaires, numéro 87 , novembre 2013 , wolter kluwer, France, p102.

[2] – Thiery legalboudec, LOLCTIC et la lutte contre la cybercriminalité, actes du séminaire internationales, sur la lutte contre la cybercriminalité, organisé par le centre de recherche juridique et judiciaire à Alger le 5,6 mai 2010, 1ère 2dition, 2011, p150

2- الوحدة التقنية:

هي وحدة مجهزة خصيصا بوسائل وبرامج ذات مستوى تكنولوجي عال وهذا لتأمين المساعدة لمصالح البحث والتحري وتتكون من ثلاث خلايا كل خلية تضمن أداء وظيفة معينة على وجه الخصوص وهي: خلية المساعدة التقنية، خلية الرقابة التكنولوجية والتكوين، وخلية التحليل والتوثيق العلمي[1].كما يستقبل المكتب المركزي لمكافحة الجريمة المرتبطة بتكنولوجيات والمعلومات والاتصال التبليغات الصادرة عن كافة المضامين غير القانونية على الانترنت، وهذا من خلال برنامج يعتمد على صفحة ويب مجهزة باستمارة تبليغ عامة لجميع ميادين النشاطات غير القانونية كالإرهاب والتزوير.

ب- فرقة البحث والتحري عن جرائم الغش المعلوماتي:

تضم هذه الفرقة العملية حوالي 30 شرطيا، يعملون تحت سلطة محافظ شرطة باريس يختص أفرادها بمهمة البحث والتحقيق في المسائل الالكترونية، كما تضمن التكفل بمهمة التكوين التوعية لمصالح الشرطة الأخرى، وتختص إقليميا بحد مدينة باريس ويمكن تمديد اختصاصها إلى كامل الإقليم الفرنسي. [2]

وتنقسم هذه الفرقة إلى ثلاث خلايا: خلية البحث والتحقيق، خلية المبادرة وخلية الدعم، وتتبنى كهدف أساسي مكافحة جرائم المعلوماتية الماسة بالتقليد والتزوير في البرمجيات، والاعتداء على حقوق المؤلف والغير، إضافة إلى باقي الجرائم الأخرى المرتكبة عبر شبكة الانترنت.[3]

ج- فرقة مكافحة الغش المتعلقة بوسائل الدفع الالكتروني:

هي أيضا فرقة تابعة وخاضعة لمحافظة شرطة باريس، تضم في صفوفها خمسون (50) شرطيا مختصا بالبحث والتحقيق في الجرائم الحديثة المتعلقة بوسائل الدفع الالكترونية وما ينشأ عنها من تقليد أو تزوير كجرائم تزوير بطاقات الائتمان والاحتيال المالي.[4]

---

[1] -Ibid, p153

[2] - Quéméner Myriam, op.cit, p189

[3] - Frédérique Chopin, la cybercriminalité, Exposé publié sur L'en encyclopédie électronique : le répertoire de droit pénale, 2013, France, P02

[4] -Quéméner Myriam, op.cit, p190.

ثانيا- على مستوى مصالح الدرك الوطني:

يخضع الاختصاص للدرك الفرنسي، عدة فرق ووحدات مختصة في مجال مكافحة الجرائم المعلوماتية وذلك من خلال اختصاصها بالبحث والتحقيق بشأنها، كما تقدم دعما تقنيا حول تطور هذه الجرائم.وتعد كافة هذه الفرق والوحدات معنية بالتحقيقات المرتبطة بالتكنولوجيا الرقمية، ويمكن لموظفيها الاستنجاد بمحققين مختصين في التكنولوجيا الرقمية المتواجدين في كامل التراب الوطني والذين تم تكوينهم منذ 1998 وعينوا في فرق البحث، ولهم دور تقني بالإضافة إلى مساعدة المحققين الآخرين، فهم يشكلون في أقسام الأبحاث مجموعة تحقيق مختصة في القضايا على المستويين الوطني والدولي، ومجهزين بعتاد خاص، يسمح لهم بإجراء التحاليل التقنية الأولية للعناصر المادية التي تم تجميعها أثناء التحريات.[1]ومن بين أهم هذه الوحدات والفرق ما يلي:

أ- معهد البحث الجنائي للدرك الوطني:

يخضع هذا المعهد للإدارة العامة للدرك الفرنسي، ويتكون هذا المعهد من فرع التحقيق الجنائي الهندسي الرقمي، والذي يضم قسم الإعلام الآلي الالكتروني الذي تم إنشاؤه سنة 1992 المختص بتحليل بيانات الحاسوب في إطار التحقيقات القضائية المتعلقة بالإعمال الاقتصادية والمالية، وبالتالي يقوم بتقديم المساعدة التقنية للدرك الوطني.[2]

ويتابع هذا القسم الأبحاث اللازمة لتطوير أجهزة وتقنيات التحريات الجنائية، وهو مختص في مجالات استغلال الأطفال في الأعمال الإباحية، للتزوير المعلوماتي، جرائم الاتصالات اللاسلكية، التزييف والتحايل بوسائل الدفع الالكتروني، ولذلك يضع خلال التحقيقات المرتبطة بالتكنولوجيات الرقمية التي يقوم بها الدرك الوطني الفرنسي وسائل كبيرة وتقنيات خاصة للتحري، وتختص هذه الوسائل الموضوعة تحت تصرف المحققين والقضاة المعنيين خاصة في إصلاح وتحليل الأقراص

[1] -Quéméne Myriam, Ferry Joel, op.cit, p216.

[2]بن قارة مصطفى عائشة، الحماية الجنائية للحكومة الالكترونية، دراسة مقارنة، أطروحة دكتوراه، تخصص قانون عام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2017-2018، ص 188.

الصلبة، التدابير الكهربائية اللاسلكية، التفتيش الدقيق في الأوساط المعقدة كالشركات واستغلال الأغراض الالكترونية والبطاقات حتى وإن كانت متلفة. [1]

ب- الفرقة التقنية للأبحاث القضائية والتوثيق:

تختص هذه الفرقة وعلى مستوى كامل الإقليم الفرنسي، وتتمثل مهمتها على المستوى الوطني في تجميع ومقارنة وتحليل جميع معلومات الشرطة القضائية في الميدان العملياتي والاستراتيجي الناتجة عن الدعاوى التي يقيمها الدرك الوطني حول الجرائم المصنفة كجنايات أو جنح [2]، كما تعمل كذلك على إدارة المعلومات القضائية من خلال ضمان تسيير قاعدة البيانات الخاصة بذلك، وإنجاز التحقيقات القضائية من خلال عمل الفرقة الإقليمية للاستعلامات[3].وتختص هذه الفرقة بصفة عامة بجمع الأدلة الرقمية، وهو ما يجعل المعلومات الممكن استخلاصها من تلك الأخيرة سهلة البلوغ للمحققين والقضاء وذلك عن طريق نشاطات الخبرة أو التقنية ومعالجة المعلومات، الشبكات والاتصالات، الالكترونيات و مساندة الوحدات على أرض الميدان: خاصة في حالات التفتيش المعقدة.

[4]- وحدة الدعم الإسناد

وأنشأت هذه الوحدات من أجل استباقية لمجموعة بروتوكولات التبادل للانترنت، تم إنشاء مراقبة الانترنت، والمكلف بالكشف عن الجرائم المرتكبة على مستوى هذه الشبكات الرقمية، ونظرا لمنح المصلحة التقنية للأبحاث القضائية والتوثيق، شرطة شبكة الانترنت ومكافحة جميع أشكال الجريمة المعلوماتية (تبادل الصور أو الفيديوهات، التزوير. ..) وذلك بالتكفل بالشروع في التحريات قبل إعادة تحويل ملف تام للنيابة العامة المؤلهة إقليميا. [5]وتتمتع هذه الوحدات باختصاص إقليمي وطني، في مجال أعمال البحث والتحقيق بشأن الجرائم المعلوماتية، وتتكون من محققين من الدرك متخصصين

---

[1] – Quéméner Myriam, Ferry Joel, op.cit, p221

[2] – Céliae Renard, castétes , cours de droit de l'internet, Paris, France 2010, P538.

[3] – Myriam Quéméner, Jean Paul, cuber sécurité , op.cit, p190.

[4]– نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 137.

[5] – Joël Blondeau et Yves crosser, la cyber délinquance sans haute surveillance revue de gendarmerie N°244, 2012 , P23

في هذا الإجرام مكونتين تكوينا يتماشى مع التقدم والتطور التكنولوجي الذي تشهره التقنية (الانترنت)، تحت اسم (N.T.E.C.H) ويصل عددهم إلى 70 محققا.[1]

ثالثا- على مستوى الجمارك:

تعد الجمارك إدارة جبائية، تطور دورها في السنوات الأخيرة، وهي تلعب دورا اقتصاديا، وهذا كونها بناءا على القواعد المحددة للتجارة الدولية بمراقبة النفقات التجارية.

ومع ظهور الجريمة المعلوماتية تطور دور الجمارك، وبدأت تتدخل مصالحها في مكافحة هذه الجرائم وهذا من خلال استعمال حقها في حجز البضائع المقلدة على مستوى مخازن البريد ومخازن التوصيل على السريع، والتي تعتبر أفضل مكان يلجأ إليه المقلدون لإرسال سلعهم المباعة عبر شبكة الانترنت، وهذا ما يشكل أخطار على صحة الاقتصاد الفرنسي.[2]

وعليه فمع ظهور الجريمة المعلوماتية وتطورها المتسارع، تطور دور الجمارك وذلك، بإنشاء خلية مختصة بمكافحة هذا الإجرام، وفي ظل هذه الأوضاع فقد تقرر بتاريخ 26 جوان 1999 إسناد مهام قضائية لإدارة الجمارك بهدف تدعيم فعالية الإجراءات الجنائية، فأصبح بمقدور بعض أعوان الجمارك المختصين والمؤهلين مباشرة متابعات قضائية بموجب طلب من وكيل الجمهورية أو قاضي التحقيق، وقد تدعم ذلك بصدور القرار المؤرخ في 05 ديسمبر 2002 المتضمن إنشاء الإدارة المركزية للجمارك الجزائرية، نظم أعوان جمارك مؤهلين يصطلح عليهم "ضباط الجمارك القضائية " وهو مرفق يعمل وفق مبدأ الاختصاص الوطني تابع المديرية العامة للجمارك الفرنسية، يسير من قبل قاضي التحقيق. [3] وتقتضي الإشارة إلى أن 40 بالمائة من نشاط هذا الجهاز يتركز حول التقليد والتزوير عبر الانترنت.

كما أنه وبتاريخ فيفري 2009، صدر قرار بإنشاء "خلية الجمارك المعلوماتية " والذي شكل نقطة تحول في عمل واختصاص هذه الخلية من خلال نصوص قانونية ووسائل مادية تسمح لها

---

[1]- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 135

[2]- Quéméner Myriam, le coopération entre les organes de lutte contre la cybercriminalité, op.cit, p03

[3]- حسين ربيعي، المرجع السابق، ص 169.

بمزاولة عملها، ، وهو ما مكنها بالإطاحة بشبكة دولية مختصة بتقليد المنتجات القادمة من الصين بيعها بأوروبا وثم تبييضها بسويسرا. [1]

وبناء على ما سبق نجد أن النظام الفرنسي وفي مجال مكافحة الجرائم الالكترونية وكذا مسائل البحث والتحقيق بشأنها من الأنشطة الفعالة والرائدة في هذا المجال، بحكم تعدد وتنوع الوحدات والهيئات المختصة بهذه المهام، وهو النظام الذي يحاول المشرع الجزائري الاقتداء به، وهذا ما ظهر لنا جليا في العديد من الوحدات، فكانت المهام المسندة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الاتصال تكاد تنطبق على المهام التي يتكفل بها المكتب المركزي لمواجهة الإجرام المرتبط بتكنولوجيات المعلومات والاتصالات.وكل هذا جاء استجابة لمطالب دولية ضمانا لنجاح مكافحة مثل هذا النوع من الإجرام، وتسهيلا للتعاون الدولي في ذلك.

المطلب الثاني: القواعد الإجرائية لجمع الأدلة في جريمة التزوير الالكتروني:

نظرا للطابع الخاص الذي تتميز به الجريمة الالكترونية خاصة جريمة التزوير الالكتروني، لاسيما أن إثباتها يحيط به الكثير من الصعاب، ومما لاشك فيه أن كشف ستر هذا النوع من الجرائم يحتاج إلى أدلة خاصة ومختلفة عما ألفناه من الجرائم التقليدية.فقد أفرزت الظاهرة الرقمية عن ارتباط الحاسوب بالانترنت، ظهور الدليل الرقمي أو الدليل الالكتروني.[2]

ويعد الدليل الالكتروني هدف إجراءات التحقيق الابتدائي، أو بمعنى آخر فإن عملية الإثبات الجنائي للجرائم الالكترونية عموما وجريمة التزوير الالكتروني على وجه الخصوص ترتكز على الدليل الالكتروني، ذلك ما يثير بشأنه تساؤلات عدة أهمها ما المقصود بالدليل الالكتروني ؟ وما هي الشروط

---

[1]–نفس المرجع والصفحة.

[2]– أطلق عليه المشرع الأوروبي مصطلح الدليل الالكتروني وهذا في التوصية رقم 13/95 في 1995/09/11 بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات .

U.C, le commendation N, f(95) 13 of the committee of ministers to member states concerning problems of criminals law connected with information technology (Adopted by the committee of ministers on 11 September 1995 at the 543 meeting of the minister's deputies) Voir le site https://www.usdoj.gov/criminal/cybercrime/cyber.Htm vu le 21/11/2017

الواجب توافرها فيه ؟ ما مدى حجيته في الإثبات الجنائي ؟ وهل يعد الدليل دليلا كافيا أما جهات التحقيق لتحال بعد ذلك الدعوى العمومية بناء عليه إلى المحكمة.هذه التساؤلات نحاول الإجابة عليها في الفروع الآتية:

الفرع الأول: مفهوم الدليل الالكتروني:

ونتيجة للتطور العلمي وانتشار التقنية الرقمية في التعاملات اليومية، ، اختلف الوسط الذي ترتكب فيه الجريمة من وسط مادي إلى وسط معنوي أو ما يعرف بالوسط الافتراضي، وهو ما استتبع ظهور طائفة من جديدة من الأدلة تتفق وطبيعة الوسط الذي ارتكبت فيه وهي الأدلة الرقمية أو الالكترونية[1]، والتي سنحاول توضيح ومصادرها وأشكالها في العناصر الآتية:

أولا: تعريف الدليل الالكتروني:

الدليل –بصفة عامة– هو أساس كشف الحقيقة الواقعية[2]، ويعرف بأنه: " الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها، وأنه الواقعة التي يستمد منها القاضي البرهان على إثبات قناعته بالحكم الذي ينتهي إليه، ومؤدى ذلك أن الدليل بالمعنى السابق ليس سوى وسيلة للتوصل إلى الحقيقة القضائية ومن ثم لا يوجد ما يمنع أن يكون هذا الدليل ناشئا أو مستمدا من أنظمة الحاسبات[3]، الممزوجة بالمعالجة الآلية للمعلومات، طالما يمكن الوصول من خلاله إلى ذات الهدف وهو الوصول إلى الحقيقة.[4] ووضع الخطط المناسبة وبدونها لا يعدو أن يكون مجرد آلة صماء كباقي الآلات بل أنه توجد برامج خاصة تساهم في استخلاص الدليل الالكتروني مثل برامج معالجة الملفات وبرامج النسخ.[5]

---

[1]– ياسر محمد الكومي محمود أبو حطب، الحماية الجنائية والأمنية للتوقيع الالكتروني في التشريع المصري والتشريعات المقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص قانون جنائي، كلية الحقوق، جامعة حلوان، مصر، 2016 ،ص 243.

[2]– محمد كمال عبد السيمع شاهين، الجوانب الإجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي –دراسة مقارنة، أطروحة دكتوراه، تخصص قانون جنائي، كلية الحقوق، جامعة حلوان، مصر، 2015، ص 241 .

[3]– هشا محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص 147.

[4]– محمد كمال عبد السميع شاهين، المرجع السابق، ص 342.

[5]– ايهاب عبد السميع روبي، المرجع السابق، ص 191.

وقد تعددت التعاريف التي قيلت بشأن الدليل الالكتروني وتباينت بين التوسع والتضييق، فقد عرفة البعض بأنه " الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة "[1]، أو أنه " معلومات يقبلها العقل والمنطق ويعتمدها العلم ويتم الحصول عليها لإجراءات قانونية وعلمية لترجمة البيانات الحاسوبية والمخزنة في أجهزة الحاسب الآلي وملحقاته ويمكن استخدامه في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات الحقيقة.[2]

أما الأستاذ كيسي (Eoghan casey) فيعرف الأدلة الجنائية الرقمية بأنها الأدلة التي تشمل جميع البيانات الرقمية التي يمكن لها أن تثبت أن هناك جريمة قد ارتكبت أو توجد علاقة بين الجريمة والجاني أو بين الجريمة والمتضرر منها "، والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة والرسومات والخرائط والصوت والصورة.[3]

أما التعريف المقترح للدليل الالكتروني من قبل المنظمة الدولية لأدلة الحاسوب[4] (IOCE) (International organisation of computer évidence) أن الدليل الإلكتروني هو:"المعلومات المخزونة أو المتنقلة في شكل ثنائي ويمكن أن يعتمد عليها في المحكمة.[5]وهو نفس المعنى تقريبا المتبنى من قبل الفريق العلمي العامل على مستوى الأدلة الرقمية (SWGDE) standard working group on digital évidence باعتبار هذا الأخير أنشئ من أجل توحيد الجهود التي تقوم بها

[1]– عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص 969.

[2]– محمد أمين البشري، التحقيق في الجرائم المستحدثة، المجلة العربية للدراسات الأمنية والتدريب، العدد ثلاثون، السعودية، 2000، ص 234.

[3]– Eoghan Casey, Digital evidence and computer crime forensic science, computer and the internet, second edition, academic press an imprint of Elsevier, London, 2004, p260

[4]– المنظمة الدولية لأدلة الحاسوب (IOCE) هي تنظيم دولي تم اعتماده في أبريل نيسان عام 1995 مقره الولايات المتحدة الأمريكية، وتسعى هذه المنظمة إلى توفير منتدى دولي لوكالات أنفاذ القانون لتبادل المعلومات بشأن التحقيق في جرائم الحاسوب وغيرها من قضايا الطب الشرعي، ويتألف من أجهزة إنفاذ القانون والوكالات الحكومية المعنية بالتحقيق الرقمي وتحقيقات الطب الشرعي، وذلك بناءا على دعوة من المجلس التنفيذي بالمنظمة / للمزيد عن المنظمة يرجب الرجوع للموقع الخاص بها : http://www.IOCE.org/index.phpid=15

[5]– عبد الناصر محمد محمود فرغلي، عبيد سيف سعيد، ورقة بحث مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الإثبات الجنائي بالأدلة الرقمية من الناحية القانونية والفنية، دراسة تطبيقية مقارنة، الرياض، الفترة من 12 إلى 14 /2007/11، ص 13 .

المنظمة الدولية لأدلة الحاسوب (IOCE)، وتطوير مختلف التخصصات والمبادئ التوجيهية، والمحافظة ودراسة الأدلة الرقمية بما فيها الصوتية والمصورة.[1]

وبعد استعراض التي قيلت بشأن الدليل الالكتروني نلاحظ أنها متقاربة من بعضها البعض، وأنها حاولت استيعاب هذا النوع المستحدث من الدليل بالرغم من حداثته، وارتباطه بالتقنية الرقمية إلا أن هناك بعض الملاحظات ينبغي الإشارة إليها تتمثل في:

– هناك خلط في تعريف الدليل الالكتروني بمفهوم برامج الحاسب الآلي عند بعض الفقهاء حيث تم اعتبار هذا الدليل كبيانات يتم إدخالها إلى جهاز الحاسوب وذلك لإنجاز مهمة ما وهذا التعريف ينطبق تماما على مفهوم الحاسب الآلي.[2] صحيح قد يتفق المصطلحان في أن كليهما يعد آثار معلوماتية أو رقمية حيث يتركهما كل مستخدم للنظام المعلوماتي ويتخذ شكلا واحدا هو الشكل الرقمي لأن البيانات داخل الحاسب سواء كانت في شكل نصوص أو حروف أو أرقام أو رموز أو صور أو أصوات تتحول إلى طبيعة رقمية لأن تكنولوجيا المعلومات الحديثة تتركز على تقنية الترقيم التي تعني ترجمة أو تحويل أي مستند معلوماتي مؤلف من نصوص أو صور إلى نظام ثنائي فيه تمثيل الأعداد يفهم الحاسب قوامه الرقمان (1,0) بل أكثر من ذلك قد تعد بعض البرامج دليلا الكترونيا مثل برامج الاختراق، إلا أن الفرق بين الدليل الالكتروني وبرامج الحاسوب وتوجيهه إلى وعلى ضوء ما سبق يمكننا أن نعرف الدليل الالكتروني على أنه كل دليل تم التحصل عليه بأي وسيلة من وسائل التكنولوجيا الحديثة يتضمن بيانات رقمية مخزنة في أجهزة الحاسوب الآلي والتي يمكن بواسطتها استخدامها في إثبات الجريمة الالكترونية أو نفيها.

ثانيا: خصائص الدليل الالكتروني:

تتميز البيئة الرقمية التي يعيش فيها الدليل الالكتروني بأنها متطورة بطبيعتها، فهي تشمل أنواعا متعددة من البيانات الرقمية تصلح متفردة أو مجتمعة، لكي تكون دليل للبراءة أو الإدانة.وقد انعكس

[1]– Eoghan casey, op.cit, p261 .

[2]– ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2006، ص 22.

هذا العالم الرقمي على طبيعة هذا الدليل مما جعله يتصف بعدة خصائص ميزته عن الدليل الجنائي التقليدي، نحاول بيانها فيما يلي:

أ- الدليل الالكتروني دليل علمي:

من الممكن أن يتشابه الدليل الالكتروني مع الدليل التقليدي في هذه الخاصية، إلا أنه الدليل الالكتروني يتميز بأنه دليل علمي[1] مستمد من الوسائل التكنولوجية الحديثة ويجد أساسه في العالم التقني، ولذلك فإن ما يطبق على الدليل العلمي يطبق على الدليل الالكتروني فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة[2]. ووفقا للقاعدة الراسخة في القضاء المقارن بأن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة.[3]

وبتطبيق ذلك على الدليل الالكتروني يتبين أن له ذات المجال وذات الطبيعة سواء من الناحية العلمية أو القانونية التي يجب ألا يخرج عنها وإلا فقد معناه[4]، وليس معنى ذلك أن هناك قواعد جامدة يرتبط بها الدليل الالكتروني من حيث طبيعته العلمية، وإنما يجب الأخذ في الاعتبار أن العلم الرقمي أو التقني هو علم متطور جدا، ويجد ذاته في قدرته الكبيرة على التطور المستمر ويتطور بالتالي معه الدليل الالكتروني.

ب- الدليل الالكتروني دليل تقني:

إن الدليل الالكتروني مستوحى من البيئة الرقمية أو التقنية، وتتمثل هذه الأخيرة في إطار الجرائم الالكترونية في العالم الافتراضي، الكامن في أجهزة الحاسب الآلي والخوادم والشبكات بمختلف أنواعها. فالأدلة الرقمية ليست مثل الدليل العادي، فلا تنتج التقنية سكينا يتم به اكتشاف القائل أو اعترافا مكتوبا أو بصمة أصبع. .. إنما تنتج التقنية نبضات رقمية تصل إلى درجة التخيلية في شكلها

---

[1]- يعرف الدليل العلمي بأنه :" الدليل المتحصل من الأجهزة والوسائل العلمية التي أقرها العلم الحديث والخبرات الإنسانية المتمثلة في الطب الشرعي وعلم النفس التجريبي، فهو ثمرة توظيف معطيات العلوم الحديثة في مجال الإثبات الجنائي مقربا بين نظرية العلم والقانون ". أنظر السيد محمد سعيد عتيق، المرجع السابق، ص 98.

[2]- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص 977.

[3]- السيد محمد سعيد عتيق، المرجع السابق، ص 109.

[4]- راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، مجلة "كلية الحقوق للبحوث القانونية والاقتصادية، العدد الأول، يناير، 2008، دار الجامعة الجديدة، مصر، ص 18 .

وحجمها ومكان تواجدها غير المعلن، فهي ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان.[1]ومؤدى ذلك يجب أن يكون هناك توافق بين الدليل الالكتروني المرصود وبين البيئة التقنية التي يعيش فيها، لمعنى صحة نسب الدليل الالكتروني إلى المجتمع المعلوماتي المولود فيه.

ج- الدليل الالكتروني يصعب التخلص منه:

تعد ميزة صعوبة التخلص من الدليل الالكترونية أهم الخصائص التي يتميز بها هذا الأخير وتميزه عن غيره من الأدلة المادية التقليدية والتي يمكن التخلص منها بسهولة، حيث يمكن التخلص من الأوراق الأشرطة المسجلة إذا حملت في ذاتها إقرارا بارتكاب شخصا لجريمة ما وذلك بتمزيقها أو حرقها أو إتلافها، كما يمكن التخلص أيضا من بصمات الأصابع بمسحها من موضعها كما يمكن أيضا تهديد الشهود لعدم الإدلاء بالشهادة، أما بالنسبة للأدلة الالكترونية فإن الأمر مختلف حيث يمكن استرجاعها بعد محوها وإصلاحها، وإظهارها بعد إخفائها، مما يؤدي إلى صعوبة الخلاص منها، لأن هناك العديد عن البرامج الحاسوبية وظيفتها استعادة البيانات التي تم حذفها أو إلغائها، أو عن طريق إعادة تهيئة أو تشكيل للقرص باستخدام الأمر سواء كان هذه البيانات صورا أو رسومات أو كتابات أو غيرها.[2]

د- الدليل الالكتروني قابل للنسخ:

هذه الميزة لا تتوفر في أنواع الأدلة التقليدية الأخرى، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل من التلف والتغيير، حيث يمكن استخراج نسخ من الأدلة الجنائية الرقمية المطابقة للأصل ولها نفس القيمة العلمية، وذلك عن طريق نسخ طبق الأصل من الدليل.

ويترتب من هذه الخاصية مسائل هامة في القانون لعل أبرزها مسألة التخلص من الدليل ومدى تجريمها والعقاب عليها، كما في حالة إعداد برامج من قبل مرتكبي الجرائم الالكترونية مهمتها الأساسية هي التخلص من الأدلة وذلك بإزالة محتويات الحاسب الآلي، وهنا يمكن إدانة مرتكب

[1]- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، دون طبعة، دار الجامعة الجديدة، مصر، 2010، ص 62.

[2]- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 63.

الجريمة في حالة استخدامه لهذه البرمجيات للتخلص من الأدلة، وعليه فالمشرع الجنائي مطالب في هذه الحالة بوضع نصوص قانونية تجرم حتى التخلص من الأدلة لاسيما إذا كانت هناك علاقة بين التخلص من الأدلة والدليل الرقمي ذاته.

ثالثا: مصادر الدليل الالكتروني:

يمكن الوصول إلى الدليل الالكتروني المتعلق بجرائم التزوير الالكتروني من عدة مصادر وهي:

أ- أنظمة الحاسوب وملحقاتها:

تعد الحواسيب مصدرا غنيا بالأدلة الرقمية، وخاصة تلك الحواسيب الشخصية التي تعد بمثابة أرشفة سلوكية للأفراد، كونها تحتوي على الكثير من المعلومات المتعلقة بنشاطات الأفراد ورغباتهم.[1]وعملية حجز الحاسوب أو ضبطه قصد تفحصه، تعد نقطة البداية في الكشف عن الجرائم الالكترونية عموما، كون جهاز الحاسوب هو وسيلة النفاذ إلى شبكة الانترنت، أيا كان شكل هذا الحاسوب، ويجب أن تشمل عملية الفحص جميع البرمجيات المخزنة في المكونات الصلبة أو الذاكرة الملحقة بالحاسوب، وكذا جميع البرمجيات التي تم إلغاؤها من قبل، كما يجب التأكد من أن المكونات الصلبة والبرمجيات تعمل بشكل سليم ومنتظم وأن الحاسوب غير مصاب بفيروس قد يؤثر على نظامه أو على ملفات التشغيل أو التنفيذ، لأن ذلك يمكن أن ينال من صحة الدليل الرقمي عند عرضه على القضاء.[2]

2- فحص نظام الاتصال بالانترنت:

يقصد بنظام الاتصال بالانترنت بالمفهوم الإجرائي مدى إمكانية اقتناع محكمة الموضوع بالإجراءات المتبعة حال استخدام وسيلة الانترنت. [3] ومن أهم المسائل المثارة في صدد فحص نظام الاتصال بالانترنت سعيا وراء إقامة الدليل على الإدانة، مسألة مدة إمكانية تحديد مكان الجريمة أو جهاز الحساب الآلي الذي انطلق منه النشاط المادي للجريمة، وإن كان هذا الأمر لا يقود تحديدا إلى

[1]- محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2011، ص 346 .

[2]- عمر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص 1009.

[3]- عمر بن يونس، الإثبات الجنائي عبر الانترنت، المرجع السابق، ص 11 .

الشخص مرتكب الجريمة استنادا إلى الدليل الرقمي فقط، إلا أنه يمكن أن يساعد حتما في التوصل إليها عبر إقامة الدليل التقليدي فيما بعد.وتشمل عملية فحص أنظمة بالانترنت، فحص حركة التنزيل والتحميل ودرجة الاستيعاب والشبكات المحلية، النظام الأمني المحاط بالانترنت. ... الخ، فعملية الفحص هذه قد تؤدي إلى الحصول على دليل رقمي يفيد في كشف الحقيقة.[1]

ومن خلال فحص تتبع حركة مسار الانترنت[2] يمكن التعرف على مكان ارتكاب الجريمة أو الحاسوب أو الحاسوب الذي كان وسيلة السلوك الإجرامي، غير أن ما يتم التوصل إليه بفضل التتبع هو عنوان رقمي فقط، حيث يرى الفقه أن هذا الدليل غير كاف لنسبة الجريمة لمالك الحاسوب، فمن الممكن ألا يكون هو من ارتكب الجريمة كأن يكون الجهاز قد سرق منه أو أجره في إحدى مقاهي الانترنت. أو أن يكون هناك من يستخدم حاسوبه احتيالا، الأمر الذي تطلب من جهات التحقيق التأكد عن طريق استكمال نقص هذا الدليل التقني بالدليل المادي كالاعتراف أو الشهادة أو الخبرة، حتى يمكن نسبة الجريمة لمرتكبيها الحقيقي. [3]

كذلك من الطرق المستخدمة في فحص نظام الاتصال بالانترنت فحص الخادم أو الملقم، وهو عبارة عن جهاز حاسب آلي ضخم مهنته تحقيق حركة الاتصال بالمواقع والصفحات التي تتم استضافتها على هيئة رقمية فيه، وهناك من الخوادم ما تكون مهنتها مختصرة فقط على القيام بتحقيق التواصل مع حلقات النقاش المباشرة أو غير المباشرة.[4]

ويتم من خلال هذه الطريقة معرفة الرسائل الالكترونية التي قام الجاني أو المجني عليه بإرسالها أو استقبالها، والمواقع التي تم زيارتها، وعليه يسهل على المحقق الجنائي الاتصال بجميع من كانوا على اتصال بالجاني أو المجني عليه ما يساهم بقدر كبير في كشف حقيقة الجرم.

---

[1]– محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 347.

[2]– يقصد بمسار الانترنت : الحركة التراسلية للنشاط الممارس من خلال الانترنت، فالحاسوب بمجرد أن يتعرف على المسار، يقوم تلقائيا باختيار البروتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات، وهذه الحركة التي أشار إليها علماء الانترنت تتشابه مع شبكة العنكبوت / للمزيد انظر : عمر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص 998 .

[3]– محمد أحمد المنشاوي، المرجع السابق، ص 524.

[4]– حسين بن سعيد بن سيف الغافري، المرجع السابق، ص 472.

ج- مخرجات الحاسوب:

قد يتخذ الدليل الالكتروني المستمد من الحاسوب أو الانترنت شكل المخرجات الورقية التي يتم الحصول عليها عن طريق الطابعات أو الراسمات، كما يمكن أن يتخذ الشكل الالكتروني كالأشرطة والأقراص الليزرية وغيرها من الأشكال الالكترونية، وإلى جانب ذلك يوجد مخرج ثالث وهو عرض المعلومات والبيانات المتعلقة بالدليل الرقمي عن طريق شاشة الحاسوب كما يمكن كذلك الحصول على ما يفيد الحقيقة من خلال المحررات الالكترونية سواء أكانت تحمل معلومات في صورة حروف أو أرقام أو علامات أو صور أو فيديوهات أو مكالمات، ومهما كان نوع المحرر، وحتى يتمكن الخبير من فك رموزه لابد من كشف عن الرقم السري أو القيام بالتعاون مع هيئة التصديق الالكتروني.[1]

ويمكن أن تستعمل هذه المحررات للحفظ الاحتياطي ويضعها الجاني في مكان بعيد وآمن، أو يودعها مثلا في خزائن البنوك التجارية أو مراكز التوثيق الحكومة الآمنة.[2]

الفرع الثاني: حجية الدليل الالكتروني في نطاق الإثبات الجنائي

إن مجرد وجود دليل يثبت وقوع الجريمة ونسبتها إلى شخص معين لا يكف للتعويل عليه، إذ يلزم أن تكون لهذه الأدلة قيمة قانونية، فما مدى حجية الدليل الالكتروني في الإثبات الجنائي ؟.

فالمقصود بحجية الدليل الالكتروني هو قيمة ما يتمتع به هذا الدليل بأنواعه المختلفة من قوة استدلالية على صدق نسبة الفعل الإجرامي إلى شخص معين ولقبول الدليل الالكتروني كأساس تشيد عليه الحقيقة سواء كان الحكم الصادر يوحي بالإدانة أو البراءة.[3]وكمحاولة للإجابة على السؤال أعلاه نتطرق إلى شروط قبول الدليل الالكتروني وكذا بيان سلطة القاضي الجنائي في قبول الدليل الالكتروني، لنعرج في الأخير لبيان موقف المشرع الجزائري في مسألة قبول الالكتروني وهذا من خلال العناصر الآتية:

---

[1]- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة ن مقارنة،دون طبعة، دار النهضة العربية، ، مصر، 2002، ص 15-16.

[2]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتي، دون طبعة، المكتب الجامعي الحديث، مصر، ص 2012، ص 56 .

[3]- ضياء علي أحمد النعمان، الغش المعلوماتي، الظاهرة والتطبيقات، الطبعة الأولى، المطبعة العربية، المملكة العربية، 2011، ص 294 .

أولا: شروط قبول الدليل الالكتروني:

لقبول الدليل الالكتروني كأساس تشيد عليه الحقيقة سواء أكان الحكم الصادر يوحي بالإدانة أو البراءة يجب أن تتوافر في هذا الدليل عدة شروط تتمثل في:

أ- ضرورة أن يكون الدليل الالكتروني متحصلا عليه بطريقة مشروعة:

إن اقتناع القاضي بالأدلة الالكترونية يحكمه ضابطان، يتمثل الأول في ضرورة أن تتأسس هذا الاقتناع على دليل الكتروني مقبول، فالقاضي الجنائي ليس حرا في تقدير الدليل الالكتروني، بل هو حر في تقدير الدليل الالكتروني المقبول في الدعوى، ما تم الحصول عليه بطريق مشروع.فمشروعية الدليل الالكتروني تعد ضمانا كبيرا للحرية الفردية، بل للعدالة ذاتها ،ويعني مبدأ مشروعية الدليل الجنائي الالكتروني بما يتضمنه من مفاهيم الكترونية، ضرورة اتفاق الإجراء مع القواعد القانونية والأنظمة المتبعة في وحدات المجتمع المتحضر، أي أن قاعدة مشروعية الدليل الجنائي لا تقتصر فقط على مجرد المطابقة مع القاعدة القانونية، بل يجب أن تراعى المبادئ السامية لحقوق الإنسان، وقواعد النظام وحسن الآداب في المجتمع.[1]

وبناء على ذلك فلابد أن يستمد القاضي اقتناعه الذاتي في مجال إثبات جريمة التزوير الإلكتروني من دليل الكتروني مشروع، فلا يجوز الاستناد إلى دليل استند من إجراء باطل وإلا بطل معه الحكم، فما بني على باطل فهو باطل.

وقد وضعت الاتفاقيات الدولية والدساتير الوطنية[2] والدساتير الوطنية[3] والقوانين الإجرائية[1] نصوصا تتضمن ضوابط لشرعية الإجراءات الماسة بالحرية ومن ثم فإن مخالفة هذه النصوص في

---

[1]- حسين الربيعي، مرجع سابق، ص 265.

[2]- نصت على هذا المواد 5-11-12 من الإعلان العالمي لحقوق الإنسان لسنة 1948 وكذا المواد 3-8-38 من الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية لسنة 1950، وأيضا الاتفاقية الدولية ضد التعذيب وسائر المعاملات غير الإنسانية والحاطة من الكرامة البشرية لسنة 1984

[3]- نصت على هذا المواد 46-47-40-41-46-47 من المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى الموافق ل30 ديسمبر 2020المتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر 2020 المتضمن تعديل الدستور الجزائري لسنة 1996 المعدل والمتمم،الجريدة الرسمية للجمهورية الجزائرية،العدد82.

تحصيل الدليل يؤدي إلى عدم مشروعية الدليل ومن هنا فإن لا يجوز للقاضي أن يقبل في إثبات إدانة المتهم دليلا الكترونيا تم الحصول عليه من تفتيش لنظام معلوماتي باطل، كصدور إذن من جهة غير مختصة.

غير أن هذا لا يعني حصر حالات عدم المشروعية في نطاق مخالفة النصوص المقررة لضمانات الحرية الفردية، إذ بعيدا عن هذه النصوص، يرى الفقه والق0ضاء أن يتصف الدليل بعدم المشروعية متى كانت طريقة الحصول عليه تتعارض مع القواعد العامة للإجراءات الجنائية والمبادئ القانونية العامة[2] كالقواعد التي توجب احترام قيم العدالة وأخلاقياتها[3]، والنزاهة في الحصول على الأدلة واحترام حقوق الدفاع.[4]وفي هذا الصدد يثور التساؤل حول قيمة الدليل غير المشروع في الإثبات الجنائي، بمعنى هل يجوز قبول الدليل الالكتروني غير المشروع ؟.

فرق فقه الجنائي في هذا المجال بين أمرين: دليل الإدانة ودليل البراءة، فبالنسبة لدليل الإدانة، وانطلاقا من قاعدة أن الأصل في الإنسان البراءة وأن يعامل المتهم على أنه بريء في مختلف مراحل الدعوى، وهنا يقتضي الأمر أن تكون الأدلة التي يؤسس عليها حكم الإدانة مشروعة سواء كانت تقليدية أو الكترونية، وعليه فأي دليل يتم الحصول عليه بطريقة مشروعة يتم إبطاله بما في ذلك الدليل الالكتروني وعدم إنتاج الإجراء الباطل للآثار التي تترتب عليه مباشرة.[5]

أما بالنسبة لدليل البراءة، فهناك اختلاف مدى اشتراط المشروعية بوجه عام في دليل البراءة ظهرت بموجبه ثلاث اتجاهات، الأول: يتمسك باعتبار المشروعية شرطا لازما في كل دليل في حين

---

[1]– انظر المواد 45–47 من الأمر 66–155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية المعدل المتمم.

[2]– جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دراسة مقارنة، دون طبعة دار النهضة العربية، القاهرة، 2002، ص 110.

[3]– محمد زكي أبو عامر، المرجع السابق، ص 120.

[4]– وتجدر الإشارة هنا إلى أن هناك اختلاف بين قاعدة مشروعية الدليل الجنائي عن قاعدة شرعية الجرائم والعقوبات، حيث تعني هذه الأخيرة مجرد التوافق مع أحكام القاعدة القانونية المكتوبة، بخلاف القاعدة الأولى فهي أعم، حيث تشمل فضلا عن القواعد القانونية، المبادئ التي نصت عليها المواثيق والمعاهدات الدولية وقواعد النظام العام وحسب الآداب السائدة في المجتمع .

[5]– عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع سابق، ص 218.

يقتصر الاتجاه الثاني يقصر المشروعية على دليل الإدانة وحده، أما الاتجاه الثالث يذهب إلى التفرقة بين ما إذا كانت طريقة الحصول على الدليل غير المشروع ترقى إلى مرتبة الجريمة من عدمه.

وفي هذا المجال ترجح الرأي أو الاتجاه القاضي أن المشروعية لازمة في دليل الإدانة دون البراءة، فالقاعدة هي افتراض البراءة المتهم ومن ثم فأي دليل يساعد على تأكيد هذه القاعدة يجب قبوله، خاصة وأن قيد المشروعية ذاته هو احترام حقوق الدفاع مما يستتبع قصر هذا القيد على دليل الإدانة في حين لا يخضع قيد البراءة لهذا القيد.

2- ضرورة أن يكون الدليل الالكتروني ذو علاقة بموضوع الجريمة المعلوماتية:

لقبول الدليل الالكتروني في مجال الإثبات الجنائي أن تكون هناك علاقة ما بين الدليل وما بين الواقعة محل الدعوى، وعليه لابد من مطابقة الدليل الالكتروني المستخرج من الحاسوب للأصل المخزن بداخله.[1]

3- يجب أن يكون الدليل الالكتروني يقينيا:

يشترط في الأدلة الالكترونية أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، وهنا يستوجب أن تقترب نحو الحقيقة الواقعية قدر المستطاع وأن تبتعد عن الظنون والتخمينات.

ويترتب على ذلك أن كافة مخرجات الوسائل الالكترونية من مخرجات ورقية أو الكترونية أقراص مغناطيسية أو مصغرات فيلمية تخضع لتقدير القاضي الجنائي، ويجب أن يستنتج منها الحقيقة، بما يتفق مع اليقين ويبتعد عن الشك والاحتمال.[2]

واليقين في النظم الإجرائية هو عبارة عن حالة ذهنية أو عقلانية تؤكد وجود الحقيقة ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى، وما يتطلع في ذهنه من تصورات واحتمالات ذات درجة عالية من التأكيد ويمكن

[1]- ضياء علي أحمد النعمان، المرجع السابق، ص 315.

[2]- حسين بن سعيد بن سيف الغافري، المرجع السابق، ص 175.

الوصول إلى اليقين عن طريق نوعين من المعرفة إحداهما حسية تدرك بالحواس، والأخرى معرفية تدرك بالعقل عن طريق التحليل والاستنتاج.[1]

4- قابلية الدليل الالكتروني للمناقشة:

إذا كانت مخرجات الوسائل الالكترونية تعد أدلة إثبات قائمة في أوراق الدعوى التي ينظرها القاضي، فإنه يجب عليه مناقشتها أما الخصوم، ويترتب على ذلك أن هذه المخرجات سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسب، أم كانت بيانات مدرجة في حاملات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية، تكون محلا للمناقشة عند الاعتماد عليها أما المحكمة.[2]فإذا كان القاضي يحكم باقتناعه الشخصي لا باقتناع غيره، فإنه يجب عليه أن يعيد تحقيق كافة الأدلة القائمة في الأوراق لكي يمكن من تكوين اقتناع يقربه نحو الحقيقة الواقعية التي يصبوا إليها كل قاض عادل ومجتهد.[3]

ويترتب على هذا المبدأ أن القاضي لا يمكنه أن يحكم في الجرائم الالكترونية استنادا إلى علم شخصي له، أو استنادا إلى رأي الغير، إلا إذا كان الغير من الخبراء، وقد ارتاح ضمير القاضي التقرير المحرر منه، فقرر الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة عليه، بحيث أن الاقتناع الذي يكون قد أصدر حكمه بناء عليه يكون متدربا من عقيدته هو وليس من تقرير الخبير.[4]

وما تجدر الإشارة إليه هو أن القاضي، ولكي له السيادة والهيمنة على الدعوى الجنائية يجب أن يكون متدربا على كيفية التعامل مع التقنية المعلوماتية وتعقيداته بشكل واف، حتى يضمن له هذا التأهيل العلمي لنجاح مهمته. [5]

---

[1]- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، العربية،المرجع السابق، ص 91 .

[2]- هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 104.

[3]- حسين بن سعيد بن سيف الغافري، المرجع السابق، ص 476.

[4]- نبيل إسماعيل عمر، قاعدة عدم قضاء القاضي بعلمه الشخصي، المجلة العربية للدراسات الأمنية المجلد الأول، العدد الأول، 1989، الرياض، السعودية، ص 40.

[5]- ضياء علي أحمد النعمان، المرجع السابق، ص 312.

ثانيا: موقف المشرع الجزائري في مسألة قبول الدليل الالكتروني:

يعد التشريع الجزائري من التشريعات التي تبنت نظام الإثبات الحر في مجال الإثبات الجنائي، مسايرة في ذلك النظم اللاتينية كفرنسا وبلجيكا، وهو الأمر الذي كرسته المادة 212 من قانون الإجراءات الجزائية والتي تنص على أنه: " يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص ولا يسوغ للقاضي يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه".

والملاحظ من خلال المادة أعلاه أن المشرع الجزائري فتح باب الحرية في وجه تقديم الأدلة وتركها لمعيار القناعة الشخصية لقاضي الموضوع تعزيزا لمبدأ إثبات قرنية البراءة ولمجال ممارسة حقوق الدفاع الفردية.

كما نصت المادة 307 من قانون الإجراءات الجزائري أيضا على أنه: "... إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لهما على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر، وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها ولم يضع لها القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: **(هل لديكم اقتناع شخصي؟)**.

وقد منح التشريع الجزائري للقاضي حرية في تقدير أدلة الواقعة الإجرامية تبعا لاقتناعهم الشخصي، ويرجع ذلك إلى طبيعة الإثبات في المواد الجنائية الذي لا يتعلق بإثبات تصرفات قانون يحتاط أطرافها بأدلة مهيأة أو معدة مسبقا، وإنما يتعلق بوقائع إجرامية مادية ونفسية والركن المعنوي الذي يمثل ما تخفيه النفس البشرية وما تنطوي عليه، فالجريمة لا يراد إثبات مادياتها فقط، وإنما يتعلق كذلك بإثبات الركن المعنوي والتحقق من قيام القصد الجنائي وإثباته أمر صعب لأنه كامن في نفسه، وهذا أمر يستلزم التطلع إلى ذات المتهم وهو لا يتحقق إلا بالقيام بعمل تقديري من جانب القاضي.[1]

[1]– محمد محدة، المرجع السابق، ص 23.

وقد سبقت الإشارة إلى أنه وطبقا للمادة 02 فقرة أمن القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، تشمل الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وكذا كل جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الالكتروني، والقاضي في إطار تقديره للدليل الالكتروني ملزم باحترام ومراقبة القواعد العامة المنظمة لطرق استخلاص الدليل الالكتروني سواء كانت هذه الطرق تقليدية أو حديثة، فبالنسبة للتفتيش المعلوماتي مثلا فالقاضي يتحقق من مدى صحة محاضر التفتيش من حيث الشكل، وأنه قد تم إعداده من واضعه أثناء مباشرة وظيفته، ويكون مضمونه يدخل في اختصاصه.[1]

أما بالنسبة لتقارير الخبرة فقد ذهبت المحكمة العليا إلى القول أن الخبرة كشأنها شأن باقي أدلة الإثبات تخضع للسلطة التقديرية لقاضي الموضوع[2]، وهذا ما أكدته المادة 215 من قانون الإجراءات الجزائية الجزائري ، لكن الطبيعة العلمية والتقنية للجريمة الإلكترونية غالبا ما تفرض على القاضي الاستناد في تكوين قناعته على الخبرة والتقيد بالنتيجة المتوصل إليها من الخبير في تقرير خبرته ولا يمكن طرحها واستبعادها إلا إذا قدر أن ما تحمله من أدلة لا يتوافق مع ظروف وملابسات الواقعة أو تتناقض مع الحقيقة العلمية، كما سبقت الإشارة إليه.[3]

غير أن المشرع الجزائري في المادة 212 من قانون الإجراءات الجزائية وضع قيدا قانونيا وهذا بقوله: ". .. ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت فيها المناقشة حضوريا أمامه "، وهذا يعني أن القاضي لا يبني اقتناعه بالبراءة أو الإدانة إلا على الأدلة التي لها أصل في أوراق الدعوى والتي طرحت بالجلسة لمناقشتها، فالقاضي هنا له سلطة تقدير الدليل المقبول في الدعوى، إلا أنه مقيد بطرحه في معرض المرافعات لمناقشته حضوريا وشفويا وعلنيا، دون تفرقة في ذلك بين دليل الإدانة أو البراءة، وهذا لتمكين الخصوم من الإطلاع عليه وإبداء رأيهم فيه وعدم مفاجأتهم بأدلة أو وسائل إثبات استعملت كدليل ولا علم لهم بها.[4]

---

[1]– انظر المادة 214 من قانون الإجراءات الجزائية الجزائري.

[2]– قرار المحكمة العليا المؤرخ في 11 جويلية 1995 المنشور في نشرة القضاء رقم 58 لسنة 2006، ص 170 .

[3]– قرار المحكمة العليا المؤرخ في 04 جوان 2002 منشور في نشرة القضاء رقم 58 لسنة 2006 ص 255 .

[4]– محمد محدة، المرجع السابق، ص 37.

والملاحظ أن المشرع الجزائري من خلال قانون الإجراءات الجزائية لم بنص على أن الدليل الالكتروني هو دليل من نوع خاص، شأنه شأن الجرائم الالكترونية، وهنا تثار عدة إشكالات لاسيما بخصوص طبيعة الأدلة المقدمة أمام الجهات القضائية، بحيث يمكن لهذه الأخيرة وفي حال عدم إلمامها بتقنيات المعلوماتية عدم الاعتداد بهذا الدليل، حتى ولو كان حائزا على القوة الثبوتية، وتتوفر فيه كافة شروط الصحة وهذا ما يعد قصورا تشريعيا واضحا.ويستحسن أن يضع المشرع نصوصا خاصة تضبط أحكاما للدليل الالكتروني، كما هو الحال في نصوص القانون المدني الذي اعترف للتوقيع بحجية كاملة في إثبات صحة العقد[1]، لاسيما وأن الأمر أشد وقعا على المتهم كونه يتعلق بحريته وقرينه براءته والتي تبقى محل شك في مواجهة الدليل الالكتروني.

الفرع الثالث: القواعد الإجرائية لاستخلاص الدليل الالكتروني:

إن خصوصية الجريمة الالكترونية وذاتية الدليل الالكتروني سوف يقود دون شك إلى تغيير كبير إن لم يكن كليا في المفاهيم السائدة حول إجراءات الحصول على هذا الدليل، وذلك نتيجة لضآلة دور بعض الإجراءات التقليدية في بيئة تكنولوجيات المعلومات، ما يقودنا إلى إتباع نوع مستحدث من الإجراءات يتلاءم وطبيعة هذه البيئة.

وعلى ذلك سنتناول في هذا الفرع الإجرائية التقليدية لاستخلاص الدليل الالكتروني أولا، ثم نتعرض بعد ذلك للإجراءات الحديثة لاستخلاص هذا الدليل.

أولا: القواعد الإجرائية التقليدية في استخلاص الدليل الالكتروني:

لقد نظم المشرع كيفية استنباط الدليل عن طريق إجراءات تتبع وصولا إلى هذه الغاية، كالمعاينة والتفتيش، وضبط الأشياء وسماع الشهود وندب الخبراء، وهي تستخدم لجمع الدليل في جميع الجرائم التقليدية منها والمستحدثة.

[1]– انظر المادة 323 مكرر 01 من القانون 10/05 المتضمن تعديل القانون المدني الجزائري.

وبالرجوع إلى قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، نجد أن المشرع الجزائري، قد نص على قواعد إجرائية تقليدية خاصة بالتفتيش والحجز في مجال الجرائم الالكترونية.وانطلاقا من هنا سنتطرق إلى بيان التفتيش في البيئة الرقمية، لنعرج إلى إجراء الضبط في هذه البيئة، وفي الأخير سنتناول مسألة الخبرة في مجال البيئة الافتراضية.

أ- التفتيش:

يعد التفتيش إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة، ويعتبر من أهم إجراءات التحقيق في كشف الحقيقة لأنه غالبا ما يسفر عن أدلة مادية تؤيد نسبة الجريمة إلى المتهم. والتفتيش ليس غاية في حد ذاته وإنما هو وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله إلى أدلة مادية تسهم في بيان وظهور الحقيقة.[1]

وأكثر ما تخلفه الجريمة الالكترونية هو نبضات الكترونية وبيانات رقمية سريعة التلاشي، إذ لا يترك التغيير فيها أي أثر مادي يمكن من خلاله معرفة مقترفها، مما يستدعي الولوج إلى الأنظمة المعلوماتية محل الاشتباه للتوصل إلى الفاعل وهو ما يطلق عليه بالتفتيش المعلوماتي[2].

---

[1]- أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الطبعة الأولى، ديوان المطبوعات الجامعية، الجزائر، 1999، ص 40 .

[2]- يرى جانب من الفقه أن الاصطلاح الواجب إطلاقه على عملية البحث عن أدلة الجريمة في العالم الافتراضي هو الولوج أو النفاذ باعتباره المصطلح الدقيق بالنسبة للمصطلحات المعلوماتية، بينما مصطلح التفتيش فيعني البحث، القراءة والتدقيق في البيانات وهو مصطلح تقليدي أكثر، وهناك من يستخدم المصطلحين معا بغرض التنظيم والتنسيق بين المفاهيم التقليدية والحديثة، وهذا ما نستشفه من المادة 19 من الاتفاقية الأوروبية لجرائم الانترنت والتي تنص على أن :" 1- كل طرف ينبني الإجراءات التشريعية وغيرها من الإجراءات اللازمة تكون سلطاته المختصة مؤهلة قانونا لتفتيش أو للولوج بإحدى الطرق ..." .انظر: عائشة بن قارة مصطفى، حجية الدليل الالكترونية في مجال الإثبات الجنائي، المرجع السابق، ص 228 .

أما المشرع الفرنسي فيطلق على جمع الأدلة في الشكل الالكتروني المصطلح التقليدي وهو التفتيش ويستشف ذلك من خلال التعديل الذي أدخله على قانون الإجراءات العقابية، أما المشرع الجزائري فقد استخدم في المادة 05 من القانون 04/09 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مصطلح الدخول إلى منظومة معلوماتية أو بمنظومة تخزين معلوماتية بغرض التفتيش في إطار قانون الإجراءات الجزائية.

وهنا يثور التساؤل حول مدى انطباق مفهوم التفتيش على المنظومة المعلوماتية، ومدى قابلية مكونات وشبكات الحاسوب كمحل يرد عليه التفتيش والضوابط التي يجب مراعاتها في ذلك، وهذا ما سنتناوله فيما يلي:

1- مدى انطباق مفهوم التفتيش على المنظومة المعلوماتية:

يرد التفتيش التقليدي على الأدلة المادية التي تخلفها الجريمة وتفيد في كشف الحقيقة، فهل يكفي تعريف التفتيش التقليدي بهذا المعنى للإحاطة بكل عناصر التفتيش الواقع على نظم المعلومات والاتصالات، وإلى أي مدى ينطبق هذا المفهوم على المنظومة المعلوماتية ؟

1-1 مفهوم التفتيش في البيئة الالكترونية:

يعرف التفتيش المعلوماتي بأنه ذلك التفتيش الذي يرد على البيانات المعلوماتية الموجودة ضمن وسائط التخزين، وقد عرفه المجلس الأوروبي بأنه إجراء يسمح بجمع الأدلة المخزنة أو المخزنة في شكل الكتروني. [1]فمفهوم التفتيش الذي يرد على الماديات هو مفهوم عام يمكن أن يستوعب التفتيش في العالم الافتراضي نظرا لاتفاقه من حيث الهدف مع التفتيش التقليدي، إلا أن جانب من الفقه [2]يرى أن التفتيش في البيئة الرقمية من الأجدر إخضاعه لأحكام مستقلة تتلاءم والطبيعة الخاصة للجريمة الالكترونية والأدلة الناتجة عنها لأن التفتيش التقليدي ما هو إلا وسيلة للإثبات المادي وإنه يستهدف ضبط أشياء تتعلق بالجريمة أو تفيد في كشف الحقيقة وغايته دوما الحصول على الدليل المادي وهذا ما يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي وكذا شبكة الانترنت، فهي مجرد برامج وبيانات الكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي.

[1]- conseils de l'Europe, recommandation R°951 du comite des ministres aux états membre relatives aux problèmes de procédures pénale lies à technologie de 1 information adoptée par la comité des ministres le 11/09/1995, lors de la 543 réunion des délégués des ministres , p28

[2]- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 224

1-2: مدى قابلية المنظومة المعلوماتية للتفتيش:

يوجد للحاسب الآلي مكونات مادية وأخرى معنوية أو برمجية، كما أن له شبكات اتصال ولاسلكية محلية ودولية، ويقصد بالتفتيش هنا التفتيش عن معطيات الحاسب الآلي غير المادية والمخزنة في جهاز الحاسب الآلي، أو المخزنة في الأقراص، كما يقصد بالتفتيش في النظم المعلوماتية محل التحقيق. [1]ويثور الجدل الفقهي حول قابلية مكونات الحاسب الآلي المعنوية للتفتيش[2]، وهو ما عبر عنه المشرع الجزائري بمصطلح المنظومة المعلوماتية. [3]

ومن هنا أصبحت التشريعات الحديثة تجيز تفتيش الأجهزة الالكترونية لضبط المعلومات المتواجدة فيها والتي تفيد كشف الحقيقة، وهذا طبقا للمادة 09 فقرة 01 من اتفاقية بودابست إذ تلتزم بموجبها الدول الأطراف بتحويل السلطات المختصة صلاحية التفتيش والولوج إلى البيانات المعلوماتية التي تم احتواؤها، سواء في داخل النظام المعلوماتي أو على دعامة مستقلة، إضافة إلى تفتيش المكونات المتصلة بالنظام كما في حالة الحاسب الآلي المحمول أو الطابعة وأجهزة التخزين المتصلة، وإذا كانت البيانات مخزنة ماديا في نظام آخر أو في جهاز آخر فإنه يمكن الوصول إليها وضبطها من خلال النظام المعلوماتي مع النظم المعلوماتية الأخرى.[4]

---

[1]- هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، مصر، 1999، ص 79 .

[2]- حيث أن المكونات المادية للحاسوب لا تثير أي إشكال إذ يخضع تفتيش الحاسب الآلي إلى أحكام تفتيش المكان الذي يوجد به ذلك الجهاز، فإذا كان الحاسب الآلي مودعا في مكان خاص، كمسكن المشتبه به أو أحد ملحقاته، فتأخذ حكم المسكن، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكن المشتبه به مع مراعاة الضمانات المقررة في التشريعات المختلفة، فإذا كانت مكونات الحاسب الآلي المراد تفتيشه في المسكن غير متصلة بنهايات طرفية موجودة في مكان آخر، فلا يثور الخلاف بشأن تفتيشها، أما إذا كانت تلك النهايات مرتبطة في مكان آخر وتطلبت دواعي التفتيش الوصول إليها وتفتيشها، فيجب مراعاة الضمانات والاشتراطات التي يتطلبها المشرع لتفتيش تلك الأماكن، أما بالنسبة للأماكن العامة، فإذا وجد شخص وهو يحمل مكونات الحاسب المادية، أو كان حائزا لها أو مسيطرا عليها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها قانونا. / أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، مجلة البحوث الأمنية المجلد 29، جامعة نايف للعلوم الأمنية، السعودية، العدد 58، 2019، ص 87 .

[4] - Article 19 alinéa 1 du convention du conseils de l'Europe sur la cybercriminalité dispose que : « chaque partie adopte les mesures législatives et autres qui se révèlent

أما المشرع الجزائري فقد تجاوز هذا الخلاف الفقهي، مسايرا في ذلك أحكام الاتفاقية الأوروبية للجريمة المعلوماتية بالنص الصريح على جواز تفتيش المنظومة المعلوماتية بموجب المادة 05 القانون 09-04 المتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

وفي تقديرنا فقد أحسن المشرع الجزائري فعلا بنصه الصريح على جواز تفتيش المنظومة المعلوماتية وذلك كون البيانات والمعلومات المخزنة في الحاسب الآلي يصلح لأن يكون محلا للتفتيش، باعتبار أن التفتيش ليس غاية بل هو وسيلة للتوصل إلى ضبط أدلة الجريمة حيث أن ما يسفر عنه التفتيش من بيانات رقمية يمكن استنساخه على دعامات مادية أخرى أو طباعته على نحو يمكن الاستناد إليه في الإثبات الجنائي.

وقد يلجأ بعض مرتكبي الجرائم تهربا من إمكانية الخضوع للتفتيش إلى تخزين بياناتهم في أنظمة تقنية خارج إقليم الدولة عن طريق إدراجها في شبكة الاتصالات البعدية بهدف إعاقة التحريات[1]، فيتوافر التفتيش في إقليم دولة أجنبية إذا توافرت علاقة سببية بين أفعال سلطات التحقيق في بلد معين وبين عمل جهاز كمبيوتر يتواجد في الخارج[2]، وهو ما يثير صعوبات أمام الضبطية القضائية فيما يتعلق بإجراء التفتيش، وقد انقسمت النظم القانونية فيما يخص الحلول التي يمكن الأخذ بها لمواجهة هذه الصعوبات [3] ،فهناك من الأنظمة القانونية من قصر حق السلطات المختصة في

---

nécessaires pour habiliter ses autorités compétentes à perquisitionner où à accéder d'une façon similaire à un system informatique ou a une partie de celui-ci ainsi qu'aux données informatique qui y sont stockées, et a un support du stockage informatique permettant de stocker des données informatique sur son territoire …. »

[1] – Marie-Christine Piatti, les libertés individuelles à l'épreuve des nouvelles technologies de l'information, presses universitaire de Lyon, 10ème Edition, 2001, p167

[2] – conseil de l'Europe problèmes de procédure pénale liés à la technologie de l'information (Recommandation n°R(95)13 et exposé des motifs, op.cit, p188

[3] – بكري يوسف، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، مصر، 2011، ص 81

التفتيش عن المعلومات في أنظمة معلوماتية داخل إقليم الدولة دون أن يمتد هذا الحق إلى المعلومات التي يتم تخزينها خارج إقليم الدولة.[1]

في حين تعاملت بعض الأنظمة القانونية مع هذا الفرض بجواز القيام بتفتيش نظم الحاسب المرتبطة به حتى ولو كانت موجودة في دول أخرى، شريطة أن يكون هذا التدخل مؤقتا وأن تكون البيانات التي يتم التفتيش عنها ضرورية لإظهار الحقيقة.[2]

2- ضوابط التفتيش في المنظومة المعلوماتية:

تعرف الشرعية الإجرائية بأن الأصل في المشتكى عليه البراءة ولا يجوز اتخاذ أي إجراء على المشتكى عليه، إلا بناء على قانون وتحت إشراف القضاء وفي حدود الضمانات المقررة قانونا بناء على قرينة البراءة.[3]

ولما كان التفتيش يتضمن قيدا للحرية الفردية يمثل اعتداء على حرمة الحياة الخاصة فيجب أن تتوافر فيه الضمانات القانونية اللازمة لصحته هي ضابط موضوعية أخرى شكلية نوضحها في الآتي:

2-1: الضوابط الموضوعية لتفتيش المنظومة المعلوماتية:

يقصد بها الضوابط اللازمة لإجراء تفتيش صحيح، وهي في الغالب تكون سابقة له، ويمكن حصرها في ثلاث ضوابط أساسية هي: السبب والمحل والسلطة المختصة بالقيام به، نحاول تفصيلها فيما يلي:

- **سبب التفتيش في البيئة الالكترونية:** حتى يكون التفتيش صحيحا في البيئة الالكترونية فإنه يجب:

- **أن يكون بصدد جريمة تزوير الكتروني واقعة بالفعل:**

---

[1]- أخذ بهذا الفرض المشرع الجزائري بمقتضى المادة 5 من القانون 04/09 المتعلق بالجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، وكذا المشرع الفرنسي من خلال القانون 2003/239 المؤرخ في 18 مارس 2003 المتعلق بالأمن الداخلي

[2]- أسامة بن غانم العبيدي، المرجع السابق، ص 94 .

[3]- أحمد فتحي سرور، الشرعية الدستورية وحقوق الإنسان في الإجراءات الجنائية، دون طبعة، دار النهضة العربية، مصر، 1995، ص 127 .

إذا كان الهدف من إجراء التفتيش هو الحصول على أدلة تساهم في كشف حقيقة الواقعة الإجرامية ونسبتها إلى مرتكبها، فإن المنطق القانوني والعقلي يقتضي للقيام به ضرورة وقوع الجريمة بصورة قطعية سواء أكانت جناية أو جنحة[1]، أما المخالفات فلا يجوز بشأنها التفتيش نظرا لضآلة خطورتها.[2]

- اتهام شخص أو أشخاص معنيين بارتكابهم لجريمة التزوير الالكتروني أو اشتراكهم في ارتكابها:

يجب أن تتوافر في حق الشخص المطلوب تفتيش أو تفتيش مسكنه أو حاسبه الآلي دلائل كافية[3] تؤدي إلى الاعتقاد بأنه قد أسهم في ارتكاب جريمة الكترونية بصفته فاعلا أو شريكا في هذه الجريمة[4]، ويجب أن يكون الاتهام جديا وقامت من الدلائل ما يكفي لانتهاك حق الخصوصية لديه.[5]

- فلا بد من توافر أمارات قوية أو قرائن على وجود بيانات أو معدات معلوماتية تفيد في كشف الحقيقة بارتكاب جريمة التزوير الالكتروني فلا مجال لإجراء التفتيش إن لم تتوافر لدى المحقق أسباب كافية على أنه يوجد في مكان أو لدى الشخص المراد تفتيشه أدوات استخدمت في ارتكاب الجريمة أو أشياء متحصلة منها[6]. ويستوي أن تكون الأجهزة أو المعدات في حيازة الشخص أو

---

[1]- المادة 44 من قانون الإجراءات الجزائية الجزائري.

[2]- علاء عبد الباسط خلاف، الحماية الجنائية للحاسب الالكتروني والانترنت، الطبعة الثانية، معهد الكويت للدراسات القضائية والقانونية، الكويت، 2008، ص 375.

[3]- يقصد بالدلائل الكافية في الجرائم الالكترونية مجموعة المظاهر أو الأمارات المعنية القائمة على العقل والمنطق والخبرة الفنية والحرفية للقائم بالتفتيش والتي تؤيد نسبة الجريمة الالكترونية إلى شخص معين بوصفه فاعلا أصليا / هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 121، أنظر أيضا : شيماء عبد الغني، المرجع السابق، ص 282 .

[4]- أسامة بن غانم العبيدي، المرجع السابق، ص 98 .

[5]- علي حسن محمد الطوالبة، المرجع السابق، ص 70.

[6]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية المجلة القانونية التونسية، مركز النشر الجامعي، تونس، 2009، ص 50 .

منزلة وينبغي أن يكون هناك من الدلائل والأمارات الكافية أو الشبهات المقبولة ضد هذا الشخص بقدر يبرر تعرض التفتيش لحرمه مسكنه، أو ما يتصل بشخصه في سبيل كشف اتصاله بالجريمة.[1]

-محل التفتيش في البيئة الالكترونية:

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادي التي تتضمن سره، والسر الذي يحميه القانون هو ذلك الذي يستودع في محل له حرمة كالمسكن أو الشخص والرسائل ومحل التفتيش في الجريمة الالكترونية هو الحاسوب والشبكة التي تشمل في مكوناتها الخادم والمزود الآلي والمضيف والملحقات التقنية.[2]

-السلطة المختصة بالتفتيش:

يعتبر التفتيش إجراء من إجراءات التحقيق التي تمس بالحرية الشخصية وانتهاك حرمة الحياة الخاصة للأفراد، لذلك حرص المشرع الجنائي على إسنادها لجهة قضائية تكفل الحريات والحقوق وتضمنها، إلا أنه وبالنظر إلى ضرورات عملية مردها كثرة القضايا والحرص على سرعة إنجاز أعمال التحقيق فيها والاستفادة من قدرات رجال الضبطية القضائية أجيز لسلطة التحقيق تكليف هؤلاء بتنفيذ التفتيش.

ويجيز المشرع الجزائري لسلطة التحقيق التي تباشر إجراء التفتيش بنفسها أو عن طريق الإذن أو الإنابة أن تستعين في ذلك بخبير له دراية بعمل المنظومة محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.[3]

---

[1]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009، ص 209.

[2]- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 103.

[3]المادة 47 فقرة من قانون الإجراءات الجزائية الجزائري.

2-2- الضوابط الشكلية لتفتيش المنظومة المعلوماتية:

إضافة إلى الشروط والضوابط الموضوعية لتفتيش نظم الحاسب الآلي والتي سبق تناولها، توجد شروط أخرى ذات طابع شكلي يجب الالتزام بها عند القيام بالتفتيش، حماية للحريات الفردية من التعسف أو الانحراف أو استغلال السلطة، وتتمثل هذه الشروط في:

-صدور الإذن بالتفتيش:

لا يجوز تفتيش الحاسب الآلي إذا كان موجودا بالمساكن -حسب الأصل- إلا بإذن صادر عن السلطة القضائية المختصة، والذي يعتبر من الضمانات الجوهرية لحماية حق الخصوصية[1]، ويعد من الضمانات المقررة في قوانين الإجراءات الجنائية تسبيب أمر التفتيش، ويقصد بالتسبيب الأمر الصادر بالتفتيش يجب أن يكون مبنيا على عدد من القرائن والدلائل التي تدل على أن في المكان أو الشخص المراد تفتيشه ما يفيد في كشف.[2]

وقد أوجب القانون أن يتضمن الإذن المذكور بيان عنوان الأماكن التي ستتم زيارتها وتفتيشها وإجراء الحجز فيها وذلك تحت طائلة البطلان، والحقيقة أن التحديد في الإذن يطرح إشكاليات جمة لأنه لا يمكن تحديد المكان الذي يتواجد به البيانات المعلوماتية محل البحث والتحري في غالب الأحيان ومن ثم فإنه من الضروري التخلي عن هذا المبدأ حيال المعلوماتية[3]. ويتعين أن تأتي عبارات إذن التفتيش عامة ما أمكن حتى لا يكون نصها قيدا على نطاق التفتيش[4]، ولكن ليس إلى درجة

---

[1]- المادة 44 من قانون الإجراءات الجزائية الجزائري .

[2]- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، المرجع السابق، ص 258

[3] Francis Barbant, les perquisitions informatiques, Revue de barreau, tome 62 Automne, 2002, canada, p440

[4]- يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، الإمارات العربية المتحدة، فبراير 2002 منشور على الموقع الالكتروني:
http://www.arablaw.org/download/cybercrimesworkpaper.doc تاريخ الاطلاع على الموقع .2018/05/06

العمومية بحيث يجبر تفتيش كل المعطيات المعلوماتية بمؤسسة ما على سبيل المثال، لأن ذلك يقضي إلى عدم المشروعية.[1]

-الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش في البيئة الالكترونية

اشترطت التشريعات الإجرائية عند التفتيش التقليدي حضور أشخاص محددين قانونا كالمتهم والقائم بالتفتيش وشاهدين من أهل المتهم أو شاهدين تنيبهم النيابة العامة.[2]أما في مجال التفتيش المعلوماتي فإن هناك من القوانين من سكتت تماما عن التعرض لهذا الشرط ونجد تطبيق ذلك في الولايات المتحدة الأمريكية، حيث تصدر السلطة القضائية المختصة بالتحقيق أوامر بالتفتيش دون إخطار مسبق في الدعوى الجزائية المتعلقة بالحاسوب، وذلك خوفا من سهولة تدمير المعلومات الموجودة على ذاكرة الحاسوب بما قد يضر حسن سير العدالة على الرغم من المخاطر التي قد تترتب على استخدام مثل هذه الأوامر.[3]

أما بالنسبة للمشرع الجزائري ومن خلال المادة 45 من قانون الإجراءات الجزائية الجزائري، فقد استغنى عن ضمانة حضور الأشخاص المحددين في الفقرة الأولى من هذه المادة في جرائم معينة منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات والجرائم العابرة للحدود الوطنية، والحكمة من ذلك ترجع إلى ضرورة إضفاء نوع من السرية أثناء جمع الدليل الالكتروني، خاصة وأن هذا الدليل ذو طبيعة خاصة من حيث سرعة تعديله والتلاعب فيه عن بعد.

-تحرير محضر التفتيش:

باعتبار أن التفتيش عمل من أعمال التحقيق، فينبغي تحرير محضر يثبت فيه ما تم من إجراءات، وما أسفر عنه التفتيش من أدلة، وبالتالي فإنه لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما.[4]وعليه فيجب على من يقوم بإجراء التفتيش في التحقيقات أن يحرر محضر يبين فيه المكان أو الشخص الذي حصل في التفتيش واليوم والساعة التي حصل فيهما

---

[1] – Francis Barbant, op.cit, p440

[2]– المادة 45 من قانون الإجراءات الجزائية الجزائري .

[3]– علي حسن محمد الطوالبة، المرجع السابق، ص 50.

[4]– عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع سابق، ص 113.

التفتيش وهذا لحسن سير الأعمال وتنظيم الإجراءات، ولا يترتب على مخالفته البطلان ويكفي أن تقتنع المحكمة من الأدلة المقدمة إليها في الدعوى أن التفتيش قد أجرى وأنه قد أسفر عما قبل أنه قد تحصل منه.[1]

2-الميقات الزمني لإجراء التفتيش في جريمة التزوير الالكتروني:

يقصد بضمانة الميقات في التفتيش أن يجرى القائم به خلال فترة زمنية ما يحددها المشرع، وذلك حرصا على تضييق نطاق الاعتداء على الحرية الفردية وحرمة المسكن.

وقد حظرت بعض التشريعات الإجرائية تفتيش المساكن ليلا حيث اعتبرت هذا الحظر ضمانا للأفراد في مواجهة سلطة الدولة[2]، غير أنها أجازت التفتيش ليلا في بعض الأحوال استثناء كما هو في الجرائم المعلوماتية، حيث نص المشرع الجزائري على جواز تفتيش المساكن في أي ساعة من ساعات النهار أو الليل في سبيل كشف الجرائم المعلوماتية، وفقا للفقرة 47 من قانون الإجراءات الجزائية الجزائري. [3]

ومن خلال ما سبق توصلنا إلى أن جوهر تفتيش المنظومة المعلوماتية هو كشف نقاب السرية نظرا لما تحتويه نظم المعلوماتية من خفايا وأسرار، وعليه يعد من أخطر الإجراءات المستحدثة، ما يستوجب إحاطته بسياج من الضمانات التي تحفظ الخصوصية، لاسيما في ظل إهدار بعض التشريعات لأهم الضمانات حق المتهم في الخصوصية والسرية كالحضور الضروري لبعض

[1]- علاء عبد الباسط خلاف، المرجع السابق، ص 382.

[2]- المادة 47 فقرة 01 من قانون الإجراءات الجزائية الجزائري على أنه :" لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة (05) صباحا ولا بعد الساعة الثامنة (08) مساءا إلا إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا .... ".

[3]- تقضي الفقرة 03 من المادة 47 من قانون الإجراءات الجزائية الجزائري على أنه :" ... وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص ...".

الأشخاص أثناء إجراء التفتيش، والحدود الزمنية للتفتيش، وكذا حق السرية لدى بعض الأشخاص المكلفين بحفظ السر المهني.[1]

وما يمكن قوله في هذا الصدد أن متطلبات مواجهة الجريمة الالكترونية بصفة عامة وجريمة التزوير الالكتروني على وجه الخصوص وحفظ حق الفرد في الخصوصية هي متطلبات متناقصة قد تؤدي إلى تراجع خطير لمبدأ الشرعية أم عنصر الفعالية بالتضحية بحقوق الأفراد من أجل التنقيب عن هذا النمط المستحدث من الإجرام، وعليه فلا يتم الموازنة بين هذه المتطلبات إلا بالإحاطة بالضمانات الآنف بيانها.

ب- الضبط في البيئة الالكترونية:

يعتبر الضبط الأثر المباشر للتفتيش في مجال التنقيب عن الجريمة الالكترونية، ويقتضي البحث في مسألة الضبط في البيئة الالكترونية دراسة أمرين، أولهما الأشكال الذي يثار بشأن جواز ورود الضبط على كيانات منطقية غير محسوسة سريعة الزوال وبالتالي البحث عن مدى صلاحية المعطيات المعلوماتية للضبط، ثم أحكام ضبط المعطيات الرقمية.

[1]- يعتبر احترام السر المهني من أهم ضوابط التفتيش في المنظومة المعلوماتية، والملاحظ أن المشرع الجزائري لم يحدد إطارا واضحا لهذا القيد، إلا أننا نجده ضمن الأحكام الإجرائية الخاصة لتنظيم بعض المهن التي ألزم أصحابها بالمحافظة على السر المهني، فلا يجوز تفتيش مكتب المحامي إلا من قبل قاضي التحقيق المختص بحضور النقيب أو مندوبه أو بعد إخطارهما قانونا، وينسحب هذا القيد أيضا على مكتب المحضر القضائي وكذا الموثق / للتفضيل أكثر انظر :

- المادة 22 من القانون 07/13 المؤرخ في 29 أكتوبر 2013 المتضمن تنظيم مهنة المحاماة، الجريدة الرسمية الصادرة بتاريخ 30 أكتوبر 2013، العدد 55.

- المادة 4 من القانون 06/06 المؤرخ في 2006/02/20، المتضمن تنظيم مهنة الموثق، الصادرة بتاريخ 2006/03/08 العدد 14 .

- المادة 07 من القانون 03/06 المؤرخ في 2006/02/21، المتضمن تنظيم مهنة المحضر القضائي الجريدة الرسمية المؤرخة في 08 مارس 2006، العدد14.

1- مدى صلاحية المعطيات المعلوماتية للضبط:

يقصد بالضبط في قانون الإجراءات الجنائية وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها[1]، فالأصل في الضبط أن يرد على الأشياء المادية التي تصلح لوضع اليد عليها بمعنى أن تكون أشياء مادية يحوزها المتهم.

أما الضبط في مجال البيئة الالكترونية فيعني وضع اليد على الدعائم المادية المخزنة فيها البيانات الالكترونية أو المعلومات التي تتصل بالجريمة الإلكترونية التي وقعت وتفيد في كشف الحقيقة عنها وعن مرتكبيها.[2]

وعليه فهدف التفتيش سواء في ذلك تفتيش الأشخاص أو المساكن هو ضبط الأشياء التي تفيد في كشف الحقيقة، أي الأشياء التي تعد في ذاتها الدليل على الجريمة أو يمكن أن يستخرج منها هذا الدليل، وهذه الأشياء محل الضبط في التفتيش المعلوماتي قد تكون مادية أو معنوية.

- ضبط الماديات المعلوماتية:

سبقت الإشارة إلى أن الضبط يرد على الأشياء المادية التي تصلح لوضع اليد عليها، ولهذا لا يثير ضبط المكونات المادية للحاسب الآلي وملحقاته أية إشكالية باعتبارها أشياء مادية، بحيث تخضع لنفس الأحكام التقليدية، إذ أن وسائل التقنية الحديثة يصدق عليها وصف المنقول، ويمكن نقلها من مكان لآخر، فمكونات الحاسب الآلي المادية بجميع أنواعه لا يثير أي إشكال في ضبطه.[3]

-ضبط المعطيات المعلوماتية:

لقد أثارت الطبيعة المعنوية للمعلومات جدلا فقهيا حول ما إذا كان يجوز ضبط المكونات المعنوية للحاسب الآلي من معلومات وبرامج وما تحتويه صناديق البريد الالكترونية من رسائل وصور وبيانات ؟والجدل لا يزال محتدما إلى يومنا هذا بين المؤيد والرافض لإمكانية ضبط البيانات المعالجة

[1]- مأمون سلامة، المرجع السابق، ص 358.

[2]- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 266.

[3]- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، مصر، 2011، ص 132.

الكترونيا فيذهب جانب من الفقه إلى إمكانية خضوع الأشياء الالكترونية أو المكونات الالكترونية لكمبيوتر والأنظمة المعلوماتية المختلفة وبكافة أشكالها، سواء كانت قابلة للإحراز أم لا.

في حين ذهب آخر إلى أنه من غير الممكن ضبط البيانات الكترونيا لانتقاء الطابع المادي لها، ذلك أن بيانات الحاسب الآلي ليست كالأشياء المحسوسة، وبالتالي لا تصلح لأن يرد عليها الضبط، وقد أخذت بعض تشريعات الدول بهذا الاتجاه منه كألمانيا ورومانيا وجانب من الفقه الفرنسي. [1]

وهناك اتجاه ثالث وأخير يأخذ موقفا وسطا، يدعو إلى ضرورة تدخل التشريعات لتوسيع سائرة الأشياء التي يمكن أن يرد عليها الضبط ليشمل إلى جانب الأشياء المادية الأشكال المختلفة للبيانات الالكترونية.

ونرى من جانبنا إمكانية ورود الضبط على المعطيات المعلوماتية، لأن الاختلاف الفقهي هو اختلاف ظاهري، ففريق يشترط لضبط الكيانات المنطقية أن تكون مخزنة في وسيط الكتروني، وهذا ما لا يشترطه الفريق الثاني والواقع أن المعلومات لا يمكن أن تكون مجردة من وسيط التخزين، سواء أكان الوسيط ذاكرة الحاسوب، أم قرصا ممغنطا أم غير ذلك من الوسائط.

أما في الجزائر فقد تدخل المشرع الجزائري لاستكمال ما تبقى من فراغ تشريعي في المنظومة التشريعي، وذلك بموجب القانون المتضمن بقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث استحدث المادة 06، والتي استعمل في صلبها بدلا عن مصطلح الضبط مصطلحا الحجز والنسخ كمفاهيم تتماشى والبيئة الالكترونية، وذلك بقولها: (عندما تكتشف السلطة في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها أو أنه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون فاصلة للحجز والوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية. ...).

[1]– علي حسن الطوالبة، المرجع السابق، ص 145، انظر أيضا نبيلة هبة هروال، الجوانب الإجراءات لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 265 .

2- قواعد ضبط المعطيات المعلوماتية:

تبرز المشكلة في إحراز المضبوطات الالكترونية الموجودة على شبكة الانترنت أو داخل كمبيوتر يتم تفتيشه عن بعد، ففي هذه الحالة لا يكون بالإمكان إحراز هذه المضبوطات وفق القواعد التقليدية للضبط، بل يلزم لإحرازها اللجوء إلى طرق ووسائل تقنية وفنية تتفق مع الطبيعة الالكترونية لهذه البيانات، فهناك جوانب إجرائية لضبط المعلوماتية وجوانب أخرى فنية نحاول بيانها فيما يلي:

2-1- الجوانب الإجرائية لضبط المعطيات المعلوماتية:

تنص المادة 116 من الكتاب الثاني من اتفاقية بودابست، على أنه لكل دولة طرف في الاتفاقية أن تتخذ ما تراه مناسبا للحفاظ على المعلومات على وجه الاستعجال، إذا كان يخشى فقدان ذلك المعلومات أو العبث بها، كما لها أن تتخذ من الوسائل، ما يلزم الشخص الذي لديه تلك البيانات المخزنة والمطلوبة في حيازته أو تحت سيطرته أن يحافظ عليها، وأن يتخذ كل ما من شأنه المحافظة على صلاحياتها للفترة الضرورية من الوقت، بما لا يزيد عن 90 يوم لكي يمكن للسلطة المختصة من تقديمها، وللدولة أن تجدد الميعاد بإجراء جديد وهذا طبقا للفقرة 2 من المادة 16 وفي هذا الإطار نجد أن المشرع الجزائري قد التفت إلى صعوبة الوصول إلى البيانات المبحوث عنها والمشكوك فيها بسبب عائق المرور إليها، لعدم معرفة الرقم السري واحتمال التخلص منها من طرف المتهمين لذلك أجاز وضع اليد على كيان البرامج برمته وأنظمة تشغيله وكل ما يتعلق باستخدامه. [1]فضبط الأدلة عن طريق حجز المعطيات يجري وفقا لمقتضيات قانون الإجراءات الجزائية، إضافة إلى تدابير أخرى كمصادرة والبرامج والوسائل المستخدمة مع إغلاق المواقع محل الجريمة المنصوص عليها في المادة 394 مكرر 6 من قانون العقوبات الجزائري.

كما اهتم المشرع الجزائري بالقيود الواردة على الضبط المعلوماتي من خلال النص على إجراء وقائي مهم وهو الحجز عن طريق منع الوصول إلى المعطيات كإجراء خاص يتخذ لتأمين المعطيات المعلوماتية، وهذا من خلال نص المادة 07 من القانون 04/09 والتي جاء فيها: " إذا استحال إجراء

[1]- يستشف هذا من نص المادة 06 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها -السابق ذكرها- وهذا من خلال قولها: " ... يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية ..."

الحجز وفقا لما هو منصوص عليه في المادة 06 أعلاه، لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لها استعمال هذه المنظومة).

ومفاد هذا الإجراء هو منع الغير من المتهم أو غيره من الوصول إلى المعطيات التي تم الدخول إليها ولكن تعذر حجزها أو ضبطها لأسباب تقنية كترميزها أو تشفيرها عن طريق أي برنامج من برامج التشفير، والهدف من ذلك هو عدم امتداد العابثين إليها لتغيير مجرى التحقيق. [1]

ولم يكتف المشرع بالنص على الجوانب الإجرائية ذات العلاقة بفاعلية الضبط المعلوماتي، بل نص على اتخاذ الإجراءات الكفيلة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة، عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك كما استخدم برامج التشفير والتوقيف، وعلى المحقق الاستعانة بالخبير المؤهل لاستخدام هذه البرامج.[2]

وقد أصاب المشرع الجزائري فعلا في هذا المجال، لأن إتاحة الإطلاع على المحتوى المجرم يؤدي إلى استفحال الضرر وشيوع الإجرام المعلوماتي.كما أن المذكرة التفسيرية للاتفاقية الأوروبية لاتفاقية بودابست نصت على هذا الإجراء والذي يتم اللجوء إليه في حالة ما إذا كانت المعطيات تتضمن خطرا أو ضررا بالمجتمع، ومثال ذلك البرامج التي تحتوي على الفيروسات أو تقدم نموذجا لعمل الفيروسات.[3]

ويلاحظ أيضا أن المشرع حرص هنا على مبدأين هامين وهما: السرية حقوق الدفاع، فالمادة 85 من قانون الإجراءات الجزائية نفسه نص على معاقبة كل من أفشى أو أذاع مستندا متحصلا من

---

[1]– الهام بن خليفة، المرجع السابق، ص 294.

[2]– نصت على ذلك المادة 08 من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهذا بقولها :" يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك ".

[3]– هلالي عبد الله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الطبعة الأولى، دار النهضة العربية، مصر، 2003، ص 240.

تفتيش لأي شخص ليست له علاقة في الإطلاع عليها، وهذا ما أكدته المادة 09 من القانون 04/09.

2-2: الجوانب الفنية لضبط المعطيات المعلوماتية:

من الطبيعي أن يتبع عملية ضبط الأدلة عملية تخزينها، وهو ما ينطبق على المعطيات الرقمية كأدلة إثبات للجرائم المعلوماتية، غير أن الطبيعة الخاصة للأدلة الالكترونية تتطلب مسألة تحريزها وتأمينها إجراءات الضبط المنصوص عليها في التشريعات الإجرائية.

ويرى الفقه المقارن أنه على المحقق إتباع الإجراءات الفنية الآتية: [1]

- تأمين مسرح الجريمة الرقمية من العبث، إذ يجب عزل الحواسيب عن الشبكة لتجنب إجراء أي تغيير على الأدلة الرقمية من قبل الغير.

- ضبط الدعائم الأصلية للبيانات وعدم الاقتصار على ضبط نسخها، لأن الاكتفاء بضبط نسخ من دعائم البيانات المطلوبة وترك دعائمها الأصلية لدى من يجوزها من شأنه أن يشكل صعوبة إثبات صحة وسلامة النسخة المتحصل عليها مما يضر بسير مرحلة البحث والتحري.

كما ينصح الخبراء ضرورة مراعاة ظروف الحرارة والرطوبة المناسبة لتخزين الأحراز مع تأمين نقلها وحملها، كي لا تتعرض أثناء نقلها أو حملها لصدمات متفاوتة، قد تؤدي إلى إتلاف كلي أو جزئي لمحتوياتها. مع الإشارة إلى أن درجة الحرارة المسموح بها تتراوح ما بين 20% إلى 80% وبمراعاة هذه النسب يمكن أن تصل مدة التخزين لهذه الأقراص والأشرطة إلى ثلاث سنوات.[2]

ونرى في هذا الصدد أن عملية ضبط الأدلة في شكلها الرقمي يجب أن تراعى فيها طبيعة الأشياء المضبوطة نظرا للذاتية الخاصة لهذه الأدلة، وعليه يجب أن تحفظ في ظروف وأمكنة يراعى

[1]- انظر في ذلك رشيدة بوكر المرجع السابق، ص 242 وطارق محمد عبد الرؤوف الخن، المرجع السابق، ص 292 وهلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 210.

[2]- عبد الله بن عبد العزيز، التفتيش في الجرائم المعلوماتية في النظام السعودي، دراسة تطبيقية، دون طبعة، جامعة نايف العربية للعلوم الأمنية، السعودية، 2011، ص 115.

فيها هذا الجانب، وينصح الخبراء دائما أخذ نسخ على سبيل الاحتياط، لاسيما وأن مجرد الخطأ في الضبط يؤدي إلى ضياع الدليل الرقمي وبالتالي إفلات المجرم المعلوماتي.

والملاحظ أن المشرع الجزائري قد التفت إلى هذه المسائل الجد معقدة، وخرج عن القواعد العامة المقررة في الإجراءات الجزائية بشأن ندب الخبير، الذي كان قاصرا فقط في حالة التلبس، بينما أجازه في إطار التفتيش والضبط المعلوماتي، والتي تعد ضرورة لا غنى منها، نظرا للطابع الفني الخاص للجرائم الالكترونية.

ج-الخبرة الفنية:

سبقت الإشارة أن المشرع الجزائري من خلال القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها قد نص في نصوص التفتيش والضبط على أن تستعين سلطة التحقيق بأشخاص لهم دراية بعمل المنظومة المعلوماتية، من هذا المنطلق ارتأينا أن نتناول مسألة الخبرة الفنية أو التقنية وهذا من خلال البحث في مفهومها والقواعد القانونية التي تحكمها وعلى النحو الآتي:

1- تعريف الخبرة:

الخبرة القضائية عموما هي الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه.[1]

وإذا كان للخبرة تلك الأهمية في الجرائم التقليدية فإن أهميتها تزداد وتصبح ضرورية بل وحتمية في اشتقاق الأدلة الالكترونية لإثبات الجرائم الالكترونية، حيث تتعلق بمسائل فنية غاية في التعقيد ومحل الجريمة فيها غير مادي، والتطور في أساليب ارتكابها سريع ومتلاحق. [2]

ونظرا لأهمية الخبرة في مجال الجرائم الالكترونية نجد أن هناك بعض التشريعات نظمت أعمال الخبرة في مجال الجرائم الالكترونية مثل المشرع الفرنسي الذي يجيز الاستعانة بالخبرة في مجال تفكيك غموض الجريمة الالكترونية وأدلتها في المادة 60 فقرة 1 من قانون الإجراءات العقابية والتي جاء

[1]- عائشة بن قارة مصطفى، الحماية الجنائية للحكومة الالكترونية، المرجع السابق، ص 248.

[2]- عمر بن يونس، المرجع السابق، ص 1031.

فيها: " يمكن لوكيل الجمهورية وضباط الشرطة القضائية بكل الطرق تسخير كل شخص، كل مؤسسة، أو تنظيم خاص أو عام، أو كل إدارة عامة جديرة بتقديم معلومات مفيدة للتحقيق ولهم دراية أو معرفة بالنظام المعلوماتي أو بمعالجة معطيات معينة من أجل تقديم معلوماتهم الخاصة في الشكل الرقمي "، بمعنى أن الخبير المسخر يمكنه تسليم المعطيات المطلوبة عن طريق إرسالها بالحاسوب وشبكات الاتصال في أقرب الآجال.[1]

وفي ظل دراستنا للخبرة التقنية، ارتأينا التطرق إلى هذا النوع المستحدث من الخبرة الإشارة إلى القواعد القانونية والفنية التي تحكم الخبير التقني، وذلك فيما يلي:

2- القواعد القانونية التي تحكم الخبرة التقنية:

لما كانت الوسائل الالكترونية وشبكات الاتصال بينها متنوعة وتتمايز خصائصها فتتدرج تحت تخصصات فنية وعلمية ودقيقة، فإنه يستوجب على القضاء التدقيق عند اختيارها للخبير، فيجب التيقن بأنه تتوفر لديه الإمكانيات والقدرات العلمية والفنية في مجال التخصص الدقيق. [2] وسنتناول هذه القواعد من خلال التطرق إلى طرق اختيار الخبراء، وواجبات الخبير التقني فضلا عن تحديد مدى حجية تقرير الخبير وهذا على النحو الآتي:

-اختيار الخبير:

حدد المشرع الجزائري من خلال نص المادة 144 من قانون الإجراءات الجزائية طرق اختيار الخبير بقولها: " يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة. تحدد الأوضاع التي يجري بها قيد الخبراء أو شطب أسماءهم بقرار من وزير العدل. ويجوز للجهات القضائية بصفة استثنائية أن تختار بقرار مسبب خبراء ليسوا مقيدون في أي من هذه الجداول "، وذلك كحالة عدم وجود الخبرة المطلوبة ضمن هذه الجداول.

[1] – Christiane Féral-Schul, cyber droit, le droit à l'épreuve de l'internet, Quatrième édition, Dalloz, paris, France, 2006, p659.

[2] – هشام رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص 140.

ولقد ترك القانون للقاضي الحرية في ندب خبير واحد أو خبراء متعددين.[1] وهذا التعدد ضروري في مجال الخبرة التقنية، ذلك أنه من الصعوبة بمكان وجود متخصص منفرد له الدراية الكاملة بتقنيات الحاسوب، حتى وإن كان يملك القدرات المالية على الظهور بمظهر التفرد في مجال الخبرة القضائية، هذا من جهة، ومن جهة أخرى، لم يحدد المشرع طبيعة شخص الخبير سواء كان شخصيا طبيعيا أو شخصا معنويا كمؤسسة متخصصة تعمل في مجال المحاسبة مثلا، وإن كان الواقع العملي للخبرة الاستعانة بالشخص الطبيعي، إلا أنه في الجريمة الالكترونية يتعين الاستعانة بشركات ومنظمات أو مؤسسات متخصصة، حيث تملك موارد مادية من برامج وأجهزة حديثة، وموارد بشرية من مهندسين متخصصين في الحاسوب والانترنت. [2]

ويجب لصحة عمل الخبير أداء اليمين القانونية وذلك لحمله على الصدق والأمانة في عمله، وبث الطمأنينة في آرائه التي يقدمها سواء بالنسبة لتقدير القاضي أو لثقة بقية أطراف الدعوى، ولا يغني هذا الإجراء أي ضمانة أخرى من الضمانات، وقد أوجب المشرع الجزائري بنص المادة 145 من قانون الإجراءات الجزائية أن يحلف الخبير اليمين القانونية قبل أداء مهمته غير أنه إذا كان الخبير المعين مقيدا في الجدول فلا يلزم أن يجدد حلفه لليمين مرة أخرى. [3]

ويلتزم الخبير بتقديم التقرير الفني خلال المدة المحددة بأمر أو حكم الندب، وإذا لم يودع تقريره في المهلة المحددة فإنه يجوز للقاضي استبداله في الحين مع إلزامه برد جميع الأشياء والأوراق الوثائق التي تكون قد عهد به إليه في ظرف ثمان وأربعين ساعة، وقد يتعرض الخبير إلى عقوبات تأديبية وحتى جزائية.[4]

---

[1]– المادة 147 من قانون الإجراءات الجزائية الجزائري .

[2]– عائشة بن قارة مصطفى، الحماية الجنائية للحكومة الالكترونية، مرجع سابق، ص 251.

[3]– تنص المادة 145 من قانون الإجراءات الجزائية على أنه :" يحلف الخبير المقيد لأول مرة بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الآتي بينها :

أقسم بالله العظيم بأن أقوم بأداء مهمتي كخبير على خير وجه وبكل إخلاص وأن أبدي رأيي بكل نزاهة واستقلال..."

[4]– المادة 148 من قانون الإجراءات الجزائية الجزائري .

2-2: مدى حجية تقرير الخبير التقني:

بعد انتهاء الخبير من أبحاثه وفحوصاته، يتعين عليه أن يعد تقريرا يضمنه خلاصة ما توصل إليه من نتائج بعد تطبيق الأسس والقواعد العلمية الفنية على المسائل محل البحث.[1]ويخضع هذا التقرير شأنه شأن باقي وسائل الإثبات لتقرير القاضي، فالقانون لم يصف عليه أية قوة ثبوتية خاصة، فهو لا يلزم القاضي، الذي له مطلق الحرية في تقديره، فله أن يأخذ بنتائج الخبرة أو استبعادها، كما له أن يأمر بإجراء خبرة تكميلية[2] أو القيام بخبرة مضادة أو مقابلة، لاسيما إذا تعارضت النتائج التي توصل إليها الخبراء حول نفس المسألة أو تعارض تقرير الخبير مع شهادة الشهود.

وينبغي الإشارة في هذا الصدد أنه وإن كان من المقرر أن القاضي يملك السلطة التقديرية بالنسبة لتقدير الخبير، إلا أن ذلك لا يمتد إلى المسائل الفنية فلا يجوز تفنيدها إلا بأسانيد فنية.[3]

3- القواعد الفنية التي تحكم عمل الخبير في مجال الجرائم الالكترونية:

لما كانت عملية تجميع الدليل الرقمي تعد من أصعب الأمور التي تواجه الخبير التقني، لذلك كان لزاما عليه إتباع خطوات وأساليب علمية تتناسب مع البيئة التي يتواجد فيها هذا النوع من الدليل.

- متطلبات الخبرة في مجال الجريمة الالكترونية:

بالنظر إلى الطبيعة الفنية والعلمية للخبرة في مجال الجريمة المعلوماتية فإنه ينبغي للخبير الإلمام بتركيب الحاسب وصناعته ونظم تشغيله الرئيسية والفرعية والأجهزة الطرفية المحلقة به وكلمات المرور أو السر ورموز التشفير و القدرة على أداء المهام دون أن يترتب على ذلك إعطاب أو تدمير

---

[1]- المادة 153 فقرة01 من قانون الإجراءات الجزائرية الجزائية.

[2]- يقصد بالخبر التكميلية : الخبرة التي تأمر بها المحكمة عندما ترى نقصا واضحا في الخبرة المقدمة إليها وأن الخبير لم يجب عن جميع الأسئلة والفنية المعين من أجلها أو أنها لم تستوف حقها من البحث أو التحري، فتطلب المحكمة باستكمال النقص الملحوظ في تقرير الخبرة وتستند الخبرة التكميلية إلى الخبير الذي أنجزها أو خبير آخر، للمزيد أنظر: مولاي ملياني بعدادي، الخبرة القضائية في المواد المدنية، مطبعة حلب، الجزائر، 1992، ص 15.
كمل كرست المحكمة العليا الخبرة المضادة في قرارها الصادر بتاريخ 1998/11/18 تحت رقم 155373 بقولها :" إذا ثبت وجود تناقض بين خبرة وأخرى وتعذر فض النزاع بين الطرفين وجب الاستعانة بخبرة فاضلة وعدم الاقتصار على خبرة واحدة أو خبرتين تماشيا مع متطلبات العدل .

[3]- عائشة بن قارة مصطفى، الحماية الجنائية للحكومة الالكترونية، مرجع سابق، ص 253.

الأدلة المتحصلة من الوسائل الالكترونية[1]، وكذا التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة أو المحافظة على دعامتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو تطابق ما هو مسجل على دعامتها الممغنطة.بالإضافة إلى ضرورة إلمام الخبير أيضا، بنظم الحاسب الآلي بمكوناته المادية والبرامجية الفنية.و معرفته لوسائل وطرق فحص نظام الحاسب الآلي كبرامج كشف وإزالة الفيروسات وبرامج استرجاع البيانات والمعلومات وإصلاح التالف وإظهار المخفي منها، وكذا معرفته لوسائل نسخ البرامج والملفات وعمل نسخ من القرص الصلب طبق الأصل.

- الأساليب الفنية في عمل الخبير المعلوماتي في اكتشاف الدليل الإلكتروني:

يعتمد عمل الخبير المعلوماتي في سبيل تحري الحقيقة في مجال الجرائم المعلوماتي على جمع مجموعة من الأدلة الرقمية وتحصيلها من خوادم المواقع ومن جهاز المعتدي بعد التوصل إلى تحديده، ثم يقوم بعملية تحليل رقمي لها لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه وتحديد عناصر حركتها، ومن ثم التوصل في النهاية إلى معرفة بروتوكول الانترنت للحاسوب الذي صدرت منه الرسائل والنبضات الالكترونية.[2]

ويرى بعض المتخصصين أن عمل الخبير المعلوماتي في اشتقاق وتجميع الأدلة الرقمية يتم عبر المراحل الآتية:

المرحلة الأولى: تجميع المعلومات المخزنة لدى الطرف المقدم الخدمة من خلال تتبع الحاسبات الخادمات التي دخل منها الخادم المعلوماتي.

المرحلة الثانية: مرحلة المراقبة ويتم ذلك بطرق مختلفة أهمها استخدام برامج مراقبة يمكن تحميلها للبحث عن المعلومات المشتبه وحصر وتسجيل بيانات كل دخول وخروج بالموقع.

[1]- هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص ص، 142، 143.

[2]- رشيدة بوكر، المرجع السابق، ص 430.

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

ولما كانت عملية تجميع الأدلة في الشكل الالكتروني تعد من أهم وأصعب الأمور التي تواجه الخبير التقني، كان لزاما عليه أن يتبع عدة خطوات من أجل اشتقاق هذا الدليل، وتتمثل هذه الخطوات أو الخطوات في المراحل التالية:

خطوات ما قبل التشغيل:

– التأكد من مطابقة أحراز المضبوطات لما هو دون عليها و التأكد من صلاحية وحدات نظام التشغيل وكذا تسجيل معطيات وحدات المكونات المضبوطة.

خطوات تشغيل الفحص:

–استكمال تسجيل باقي معطيات الوحدات من خلال قراءات الجهاز وعمل نسخة من كل وسائط التخزين المضبوطة وعلى رأسها القرص الصلب لإجراء عملية الفحص المبدئي على هذه النسخة لحماية الأصل من أي فقد أو تلف أو تدمير سواء عن سوء الاستخدام أو لوجود فيروسات أو قنابل برمجية إضافة إلى تحديد أنواع وأسماء المجموعات البرامجية كبرامج النظام (برامج التشغيل)، برامج التطبيقات وبرامج الاتصالات، وما إذا كان هناك برامج أخرى ذات دلالة بموضوع الجريمة.

– إظهار الملفات المخبأة والنصوص المخفية داخل الصور و استرجاع الملفات التي محوها من الأصل وذلك باستخدام أحد برامج استعادة المعلومات وكذلك بالنسبة للملفات المعطلة أو التالفة و تخزين هذه الملفات أو المعطيات وعمل نسخ أخرى طبق الأصل من الأسطوانة أو القرص المحتوى لها ولفحصها عن طريق تطبيق الخطوات سالفة الذكر.

– إعداد قائمة يجرد فيها الخبير كل الأدلة الرقمية التي تم الحصول عليها، مع إجراء مراجعة لكل محتفظ بها في القرص الصلب لحاسوب آخر للتأكد من سلامة القائمة.

– تحويل الدليل الرقمي إلى هيئة مادية، وذلك عن طريق طباعة الملفات أو تصوير محتواها إذا كانت صور أو نصوص أو وضعها في أي وعاء آخر حسب نوع المعطيات المكونة للدليل.

ثانيا: القواعد الإجرائية الحديثة لاستخلاص الدليل الالكتروني

إزاء التعقيد التقني الذي تمتاز به الجريمة المعلوماتية، فقد عجزت الإجراءات التقليدية عن كشفها مما حمل التشريعات على استحداث تدابير إجرائية تلائم هذه الخصوصية، وتتمثل هذه التدابير في الإجراءات التي نصت عليها اتفاقية بودابست والاتفاقية العربية المتعلقة بتقنية المعلومات في التحفظ العاجل على البيانات المخزنة والكشف العاجل لبيانات المرور وأوامر تسليم المعلومات واعتراض معطيات المحتوى.

ومن بين المقومات التشريعية التي أرساها المشرع الجزائري ضمن خطته في مكافحة الجريمة الالكترونية ما جاء به في القانون 22/06 المؤرخ في 2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية من خلال إجرائي التسرب واعتراض المراسلات، تم من خلال القانون 04/09 استحدث إجراءين آخرين هما المراقبة الالكترونية وحفظا المعطيات المتعلقة بحركة السير.وسنتناول بالدراسة هذه الإجراءات على النحو الآتي بيانه:

أ- التسرب الإلكتروني واعتراض المراسلات:

استحدث المشرع الجزائري في مجال مكافحته جرائم المساس بأنظمة الحاسب الآلي عدة إجراءات للكشف عن الجريمة ومرتكبيها في ظل عجز أساليب البحث والتحري التقليدية في الكشف عن الجرائم المستحدثة من بينها الجرائم الالكترونية، وتتمثل هذه الإجراءات في عمليتين: الأولى هي عملية التسرب، أما الثانية فهي اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، والتي سنتناولها فيما يلي:

1- التسرب الإلكتروني:

لقد نظم المشرع الجزائري هذا الإجراء في قانون الإجراءات الجزائية وفق ثمانية مواد من المادة 65 مكرر 11 إلى المادة 65 مكرر 18 تناول من خلالها تحديد مفهوم هذا الإجراء وشروطه وسنحاول تفصيل ذلك كما يلي:

1-1: مفهوم التسرب الإلكتروني:

عرف الفقه التسرب الإلكتروني بأنه تقنية من تقنيات التحري والتحقيق الخاص تسمح لضابط أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم، وكشف أنظمتهم الإجرامية وذلك بإخفاء الهوية الحقيقية، وبتقديم المتسرب على أنه فاعل أو شريك .[1]

والتسرب في نطاق جريمة التزوير الالكتروني يمكن أن يتصور في دخول المتسرب للنظام المعلوماتي واشتراكه في محادثات الدردشة أو حلقات النقاش مستخدما في ذلك أسماء أو صفات مستعارة أو وهمية، ويظهر بمظهر عادي كأنه منهم، ولا يشترط الاتصال بالفضاء الافتراضي، بل يمكن أن يندس في مجموعة الإجرامية التي تزور المحررات الالكترونية، وهذا من أجل تمكنه من الحصول على الدعامات المزورة، أو ما يثبت التزوير في الشكل الالكتروني ويكون بحوزتهم.[2]

وقد عرف المشرع الجزائري التسرب من خلال المادة 65 مكرر 11على أنه :"قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بايهامهم أنه فاعل معهم أو شريك أو خاف".

2-1: شروط صحة التسرب الالكتروني:

إن إضفاء صفة المشروعية على إجراء معين مهما كان ماسا بحق الخصوصية لا يتأنى من خلال إباحة هذا الإجراء فقط، وإنما تقتضي المشروعية إحاطة الإجراء بالضمانات اللازمة لصيانة هذا الحق في الخصوصية.

وقد أحاط المشرع الجزائري عملية التسرب بجملة من الشروط التنظيمية والإجرائية، حيث تجلت معظم المواد التي جاءت في التسرب من المادة 65 مكرر 11 إلى المادة 65 مكرر 18 من قانون الإجراءات الجزائية من أجل إنجاح العملية وسيرها في ظروف سهلة تضمن أمن المتسرب، وصولا للأهداف المسطرة، وتتمثل هذه الشروط فيما يلي:

[1]- عبد الرحمان خلفي، محاصرات في قانون الإجراءات الجزائية، الطبعة الأولى، دار الهدى، الجزائر، 2010، ص ص 74،75.

[2]- الهام بن خليفة، المرجع السابق، ص ص 305، 306.

-صدور الإذن بالتسرب الالكتروني:

لا يمكن بأي حال من الأحوال لضابط الشرطة القضائية أن يباشر عملية التسرب بمفرده دون أن يكون متحصلا على إذن بذلك من الجهات المختصة.[1]

وينبغي أن يكون هذا الإذن مكتوبا ومسببا ومن ضمن المعلومات التي يجب أن يشتمل عليها طبيعة الجريمة، وهوية ضابط الشرطة القضائية الذي تحت مسؤوليته تسير هذه العملية. [2]

-المادة الزمنية لعملية التسرب:

يجب على وكيل الجمهورية أو قاضي التحقيق الذي يأذن بالقيام بعملية التسرب أن يذكر المدة الزمنية المحددة للعملية في الإذن، والتي لا يمكن أن تتجاوز 04 أشهر حسب المادة 65 مكرر 15، كما يذكر تاريخ مباشرة العملية وتاريخ نهايتها.[3]ويمكن أن تجدد مدة الإذن حسب مقتضيات التحري أو التحقيق، ضمن نفس الشروط الشكلية والزمنية ويجوز للقاضي الذي رخص بإجرائها أن يأمر، في أي وقت بوقف عملية التسرب قبل انقضاء المدة المحددة. [4]

-دوافع اللجوء لعملية التسرب:

نظرا لخطورة عملية التسرب وحساسيتها فإنه لا يتم التطرق إلى هذا الإجراء إلا إذا اقتضت ضرورات التحقيق والتحري ذلك، وهذا حسب نص المادة 65 مكرر 11 من قانون الإجراءات الجزائية بقولها: " عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 أعلاه، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبنية، فالقصد من هذا الإجراء هو الوصول إلى الحقيقة، الوصول إلى الأدلة القانونية والموضوعية.

---

[1]- المادة 65 مكرر 11 من قانون الإجراءات الجزائية الجزائري .

[2]- المادة 65 مكرر 15 من قانون الإجراءات الجزائية الجزائري .

[3]- انظر الفقرة 3 من المادة 65 مكرر 15 من قانون الإجراءات الجزائية الجزائري.

[4]- تنص الفقرة 5 من المادة 65 مكرر 15 على أنه :" ... ويجوز للقاضي الذي رخص بإجرائها أن يأمر، في أي وقت، بوقفها قبل انقضاء المدة المحددة ..."..

وحسب المشرع الجزائري وطبقا للمادة 65 مكرر 5 فإن إجراء التسرب، يتخذ في حال التحقيق أو التحري، في الجرائم المنصوص عليها في هذه المادة والتي من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

وما يجدر الإشارة إليه أن نجاح عملية التسرب تحكمها مسألة غاية في الأهمية وهي السرية، بحيث يكون مصيرها الفشل ما لم يتحقق هذا الشرط، وهكذا فإنه يقع واجبا على الضابط المسؤول عن العمل أن يحيطها بالسرية التامة، كما نصت المادة 65 مكرر 16 من قانون الإجراءات الجزائية على جزاءات عقابية مشددة في حالة الكشف عن الهوية الحقيقة للمتسرب.[1]

وفي الأخير يمكننا القول أن القواعد القانونية ليست الوحيدة التي تحكم وسائل البحث عن الجريمة، فهناك ما يسمى بمبدأ النزاهة أو مبدأ الأمانة الذي يساهم في تحديد الأطر التي تجري في حدودها عملية البحث عن الجريمة الالكترونية وأدلة إثباتها وهو مبدأ يستند إلى الأخلاق ومتطلبات العدالة، وفي هذا الصدد يثور الإشكال حول مدى مشروعية التسرب الالكتروني باعتباره صورة من صور الحيلة والخديعة ؟

من الناحية القانونية إن المشرع لم يحدد الوسائل التي يمكن اللجوء إليها بصدد كشف الجرائم عموما، إلا أن أغلب التشريعات الجنائية تعاقب على الحيلة باعتبارها منافية للأخلاق ومبادئ الصدق والأمانة، أما من الناحية الفقهية فإن أغلب الفقه في فرنسا ومصر متفقون على جواز لجوء جهات الضبط القضائي إلى وسائل تحمل في طياتها معنى الحيلة بغية اكتشاف الجرائم وليس التحريض على

[1]– تنص المادة 65 مكرر 16 من قانون الإجراءات الجزائية الجزائري على أنه :" لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذي باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات – يعاقب كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 50,000 دج إلى 200,000 دج

– وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح على أحد هؤلاء أحد الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس (5) إلى عشر (10) سنوات والغرامة من 200,000 دج إلى 500,000 دج

– وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من عشر (10) سنوات إلى عشرين (20) سنة والغرامة من 500,000 دج إلى 1,000,000 دج دون الإخلال عند الاقتضاء بتطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات ".

ارتكابها.[1]فالتسرب الالكتروني يشكل وسيلة إجرائية أكثر فاعلية في كشف الجرائم الالكترونية، لكنه في الوقت ذاته يضيق من مساحة النزاهة التي يجب أن تتصف بها عملية البحث عن الأدلة، ومن هذا نجد أن مبدأ النزاهة هنا في إطار حقين متناقضين بين حق الدولة في متابعة المجرم المعلوماتي، وفي حق هذا الأخير في احترام حياته الخاصة.

ويرى الباحث في هذا الصدد أنه ورغم الجدال الدائر حول مدى مشروعية هذه العملية، فإننا نؤيد ما ذهب إليه أغلب الفقه في جواز اللجوء إلى الحيلة في كشف هذا النوع من الجرائم التي تتم في بيئة رقمية مرتكبها مجرم يتمتع بذكاء فائق، ولا سبيل لإزالة الغموض عند هذه الجرائم إلا بحيلة، وهذا لمقتضيات المصلحة العامة، ما يدفع المشرع إلى التضحية بحقوق الأفراد لاسيما الحق في حياته الخاصة، وهنا يتراجع مبدأ الشرعية أمام عنصر الفعالية في مواجهة هذا النوع من الجرائم.

2- اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

استحداث المشرع الجزائري هذا الإجراء بموجب القانون رقم 22/06 المؤرخ في ديسمبر 2006 المعدل والمتهم لقانون الإجراءات الجزائية وهذا في المواد 65 مكرر 5 إلى 65 مكرر 10 من قانون الإجراءات الجزائية، ونص عليه المشرع الفرنسي في المواد 95/706 إلى 102/706 من قانون الإجراءات العقابية المعدلة بقانون 09 مارس 2004 المتعلق بكيفيات تكييف القضاء مع التطورات الإجرامية. [2]

وسنحاول في هذا المقام التطرق إلى المقصود بالاعتراض وبيان أحكامه وهذا على النحو الآتي:

2-1: مفهوم إجراء اعتراض المراسلات:

كرس المشرع الجزائري هذه التقنية من خلال نص المادة 65 مكرر 05 من قانون الإجراءات الجزائية والذي نص على ضرورة اللجوء إلى اعتراض المراسلات، أو تسجيل أو نسخ المراسلات التي

[1]- توفيق محمد المنشاوي، حرمة الحياة الخاصة ونظرية التفتيش، دون طبعة، منشأة المعارف، الإسكندرية، 2006، ص 216.

[2] - Christian Féral-Schuhl, op.cit, p660.

تتم عن طريق قنوات الاتصال السلكية واللاسلكية[1]، وهذه المراسلات هي عبارة عن بيانات قابلة للإنتاج، التخزين، الاستقبال والعرض.

فنجد المادة 9 فقرة 6 من القانون 03/2000 المؤرخ في 05 أوت 2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات، اعتبرت أن مادة المراسلات هي كل اتصال مجسد في شكل كتابي يتم عبر كافة الوسائل المادية التي يتم ترحيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه ،ولا تعتبر الكتب والجرائد والمجلات واليوميات كمادة مراسلات، وعليه فحسب مفهوم هذه المادة فإن المراسلات الخاصة تصبح محصورة في الرسائل المكتوبة في الشكل التقليدي.

وقد عرف البعض الاعتراض بأنه عملية مراقبة سرية المراسلات السلكية وللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه في ارتكابهم أو مشاركتهم في ارتكاب الجريمة،أما تسجيل الأصوات والتقاط الصور فيقصد بها تسجيل المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة في مكان عام أو خاص، وكذلك التقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص.[2]

وبالرجوع إلى القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتحديدا المادة 02 فقرة و منه نجدها قد عرفت الاتصالات الالكترونية على أنها أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية.

وتختلف وتتنوع المراسلات عبر وسائل الاتصالات الالكترونية والتي من أهمها التراسل عبر البريد الالكتروني، فهذه التقنية تم ابتكارها ليتمكن مستخدموها من تبادل الرسائل والصور وغيرها من

---

[1]– تنص المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري على أنه :" إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن كما يأتي :" اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية وضع ترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص ...."

[2]– عبد الرحمان خلفي، محاضرات في قانون الإجراءات الجزائية، المرجع السابق، ص 73.

المواد القابلة للإدخال الرقمي في صندوق الرسالة، أو القابلة للتحميل الرقمي بصفتها ملحقات بالرسالة ثم ترسل تلك الرسالة من بريد شخص إلى آخر عبر عنوان بريد الكتروني دونما إبطاء.[1]

وإذا كانت هذه المراسلات تتمتع بالخصوصية حمى المشرع سريتها بسن قوانين تعمل على توفير قدر كبير من الحماية الإجرائية لها، إلا أن هذا الأمر ليس على إطلاقه فإذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في الجرام الماسة بأنظمة المعالجة الآلية للمعطيات، فإنه يجوز اعتراض هذه المراسلات وكشف السرية عنها في سبيل البحث عن الدليل، وهو السند الشرعي المبرر لإباحة هذا الإجراء التي يتضمن اعتداءا جسيما على حرمة الحياة الخاصة وسرية الاتصالات.

ورغم إجازة القانون الفرنسي والجزائري لهذا الإجراء، إلا أنهما أحاطاه بعدة ضوابط وشروط تكون بمثابة ضمانات، نوجزها فيما يلي:

2-2: الشروط والضمانات المقررة لاعتراض المراسلات:

مما لا شك فيه أن أسلوب اعتراض المراسلات السلكية واللاسلكية دون علم أصحابها بقدر ما يفيد في كشف الحقيقة ويسهل إثبات كثير من الجرائم الغامضة كتلك المتعلقة بالجرائم الالكترونية فهو من جانب آخر يمثل انتهاكا لحرمة الحياة الخاصة، لما فيه من اعتداء على سرية مراسلاتهم.

والمشرع الجزائري في هذا الصدد كما أعطى لسلطة التحقيق إمكانية اعتراض المراسلات كأسلوب مستحدث للبحث عن الدليل يتماشى مع الأساليب المتطورة التي يلجأ إليها الجناة في تنفيذ جرائمهم وإخفاء أي أثر يدل عليهم، فمن ناحية لم يفتح الباب على مصرعيه في اللجوء إلى هذه الوسيلة بل أحاط استخدامها بشروط قانونية تعمل على منع التعسف وتضون الحرية الفردية وتتمثل هذه الشروط في:

[1]-محمد أبو العلاء عقيدة، مراقبة المحادثات التلفونية، دراسة مقارنة، دون طبعة، دار النهضة العربية، 2008، ص 192.

-ترخيص السلطة القضائية ومراقبتها لعملية التنفيذ:

طبقا للمادة 05 مكرر 05 من قانون الإجراءات الجزائية فإنه لا يمكن لضابط الشرطة القضائية اللجوء إلى إجراء اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب وحسب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح قضائي، فالسلطة القضائية هي وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمانة لازمة لمشروعية هذا الإجراء. وعلى وكيل الجمهورية أو قاضي التحقيق قبل منح هذا الإذن تقدير قائدة إجراء الاعتراض وجديته وملاءمته ليسر إجراءات الدعوى من خلال معطيات التحريات التي قامت بها الضبطية القضائية مسبقا.

وحسب المادة 65 مكرر 7 فإنه يجب أن يتضمن الإذن مكتوب كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها.

وقد نصت المادة 65 مكرر 09 على أن عملية تنفيذ إجراء اعتراض المراسلات تتم تحت رقابة السلطة القضائية التي أذنت به وذلك من خلال قيام ضابط الشرطة القضائية المأذون أو المناب من طرف القاضي المختص بإعداد محضر تاريخ وساعة بداية هذه العمليات والانتهاء منها.

-تحديد طبيعة المراسلة ومدة الاعتراض:

يفهم صراحة من نص المادة 65 مكرر 07 التي توجب أن يتضمن الإذن باعتراض المراسلات كل العناصر التي تسمح بالتعرف على الاتصالات أو المراسلات المطلوب اعتراضها، كما استوجب المشرع أن لا تتجاوز مدة الإجراء أربعة أشهر قابلة للتجديد حسب تقدير نفس السلطة مصدره الإذن وفقا لمقتضيات التحري والتحقيق. أما المشرع الفرنسي في هذا القيد وطبقا للمادة 95/706 في فقرتها الأولى جعل مدة الاعتراض شهر قابلة للتجديد مردة واحدة بنفس الشروط الشكلية والزمنية.

2-2-3: اللجوء إلى الاعتراض حيال جرائم محددة حصرا:

يجب أن يتخذ إجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور حيال جرائم محددة على سبيل الحصر والتي سبق ذكرها بمناسبة البحث في التسرب والتي أوردها المشرع في المادة 65

مكرر 5، والتي تشمل جرائم المخدرات والجريمة والمنظمة العابرة للحدود الوطنية والجرائم الماسة بأنظمة المعالجة للمعطيات وجرائم أخرى منصوص عليها في هذه المادة. [1]

وهناك استثناء آخر نص عليه المشرع الفرنسي من خلال الفقرة 03 من المادة 96/706 أورده على إجراء الاعتراض في كل الأماكن العامة والخاصة ،ويتمثل هذا الاستثناء في عدم إمكانية القيام بإجراء الاعتراض في بعض الأماكن والمتمثلة في مكاتب القضاة والمحامين ومكاتب الأطباء والموثقين والمحضرين القضائيين ومحلات المؤسسات الإعلامية أو الصحفية ومؤسسات السمعي البصري ومؤسسات الاتصال المباشر مع العامة.[2] في حين لم يورد المشرع الجزائري هذا الاستثناء في مواد الاعتراض وأشار إلى إمكانية الدخول إلى كل الأماكن العامة والخاصة بغير علم أصحابها وموافقتهم وفي كل وقت حسب نص المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري ".

ب- المراقبة الالكترونية والتزامات مقدمي الخدمات:

نصت الاتفاقيات الدولية والتشريعات الداخلية على إجرائي المراقبة الالكترونية والتزامات مقدمي الخدمات كإجراءات مستحدثة تتلاءم وخصوصية الجريمة الالكترونية وسنحاول فيما يلي التطرق إلى هذين الإجراءين:

1-مراقبة الاتصالات الالكترونية:

تعد الاتصالات واحدة من أهم المسائل المتعلقة بحق أساسي، وهو الحق في الخصوصية الذي أكدت عليه جميع المواثيق[3] والدساتير[4]، ولأن التقنية مكنت المجرم من الإفلات عن أعين سلطات

[1]- انظر المادة 65 مكرر 05 من قانون الإجراءات الجزائية الجزائري .

[2]- الهام بن خليفة، المرجع السابق، ص313.

[3]- على سبيل المثال المواد 12 من الإعلان العالمي لحقوق الإنسان لعام 1948 والمادة (17 ف 2،1) من العهد الدولي الخاص بالحقوق المدنية والسياسية لعام 1966، المادة 17 من الميثاق العربي لحقوق الإنسان لعام 2004، والمادة 08 من الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية لعام 1950، وكذا المادة 11 من الاتفاقية الأمريكية لحماية حقوق الإنسان لعام 1969.

[4]- كما نصت على المادة 39 من الدستور الجزائري لسنة 1996 المعدلة بموجب الأمر 01/16 المتضمن التعديل الدستوري.

الأمن كان لابد من منح هذه الجهات سلطة المراقبة الالكترونية للاتصالات رغم ما تحتويه من كشف للسرية.وسنحاول في هذا المقام في مفهوم هذا الإجراء وبيان أحكامه وقواعده.

1. 1: مفهوم المراقبة الالكترونية:

استحدث المشرع إجراء المراقبة الالكترونية بموجب القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقد جاء في عرض أسباب هذا القانون أن هذا الإجراء يعتبر من القواعد الوقائية التي تسمح بالرصد المبكر للاعتداء المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها،ولم يتعرض المشرع الجزائري لتعريف المراقبة الالكترونية، وقد تصدى الفقه لذلك وعرفها بأنها مراقبة شبكة الاتصالات.[1]كما عرف إجراء المراقبة الالكترونية للاتصالات بأنه ذلك العمل الذي يقوم به المراقب باستخدام التقنية الالكترونية لجمع بيانات أو معلومات عن المشبه فيه، سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن (التاريخ، الوقت) لتحقيق فرض أمني أو لأي غرض آخر.[2]

وتتم مراقبة الاتصالات الالكترونية من خلال تقنيات وبرامج تقوم بالتقاط تلك المحادثات عن بعد، ومن ثم يتم التصنت عليها والإطلاع على محتواها أو ضبطها من قبل الجهة المراقبة، وهذا الأمر يفترض فيه أن يتم دون أن يشعر به أطراف الاتصال، كما وأنه ينبغي أن يتم أيضا من دون أن يؤدي إلى قطع الاتصال أو المحادثة، وإلا سينتفي الغرض من إجراء المراقبة، ولذلك فإننا نرى أن هذه العملية لا تتم من خلال اعتراض المحادثة، وإنما تتم من خلال التقاطها عبر تلك التقنيات والأجهزة، وأنه من غير الصائب استعمال عبارة الاعتراض (interception) للدلالة على مراقبة الاتصالات الالكترونية والتصنت عليها، فاستعمال هذه التسمية أو العبارة للدلالة على عمليات المراقبة السرية الالكترونية للاتصالات الالكترونية، لا يخلو من الخطأ من الناحية العملية ينبغي أن يتم اعتراض المحادثة وقطع الطريق عنها ومنعها من الوصول إلى وجهتها، إلا أن ذلك غير متحقق في الحقيقة من الناحية العملية، فأنظمة المراقبة هذه لا تؤثر في محتوى وجهة الاتصال الالكتروني المراقب، وإنما تقوم فقط بالتصنت والتجسس على الحزم الناقلة لتلك الاتصالات ثم أخذ نسخة من محتوى تلك

[1]– رشيدة بوكر، المرجع السابق، ص 370.

[2]– نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 198.

الاتصالات وخط سيرها لتقوم بتسجيلها فيما إذا كانت محادثة الكترونية، وتخزينها إذا كانت مراسلة الكترونية.[1]

2. 2- أحكام المراقبة الالكترونية:

مما لاشك فيه أن مراقبة الأحاديث الخاصة تمس بحق الإنسان في الخصوصية وما يتفرع عنه من سرية الأحاديث الخاصة، وهو حق لصيق الصلة بالإنسان، بل هو على حد قول أحد الفقهاء – الإنسان نفسه ، وهذا الحق أصبح مهددا بدرجة كبيرة نتيجة للتطور التكنولوجي الذي أدى إلى إفراز أجهزة للمراقبة ذات تقنية تلتقط أحاديث الإنسان دون أن يشعر، الأمر الذي أدى بعض الفقهاء إلى القول بأن أجهزة المراقبة تعد نكسة للتقدم المذهل للتقنيات الحديثة.[2]

ومن هذا المنطلق نجد أن المشرع الجزائري كرس حماية جزائية للمراسلات وعقاب لأول مرة ا على عتراض الاتصالات السلكية واللاسلكية دون إذن وذلك بموجب القانون (06-23) المؤرخ في (2006/12/20) المعدل لقانون العقوبات الجزائرية عن طريق تجريمه لكل سلوك من شأنه الاعتداء على حرمة الحياة الخاصة للأشخاص، بأي تقنية كانت وذلك بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه أو التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص.[3]ولم يقتصر الحماية عند تجريم الأفعال الخاصة بالاعتراض، بل شملتها أيضا إلى عقاب كل من احتفظ أو وضع أو سمح بأية وسيلة كانت التسجيلات المتحصل عليها بأحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون.

ويشمل مصطلح المراسلات، الاتصالات السلكية واللاسلكية مثل المحادثات التليفونية سواء التي تتم في الهاتف الثابت أو الهاتف المحمول، وكذا الاتصالات الالكترونية التي تشمل معظم اتصالات الانترنت بما في ذلك مراسلات البريد الالكتروني.[4]

---

[1]- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دراسة مقارنة، الطبعة الأولى، دار المطبوعات الجامعية، 2009، ص 11 .

[2]- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 168.

[3]- انظر المادة 303 مكرر من قانون العقوبات الجزائري.

[4]- عمر بن يونس، المرجع السابق، ص 361.

وتجدر الإشارة هنا أن الحماية التي كفلها المشرع الجزائري للمراسلات والاتصالات لازالت قاصرة، إذ أن النص المذكور تجاوزه الزمن بفعل المستجدات التقنية الحاصلة في مجال التقنية الاتصالات، أين باتت أغلب المراسلات والاتصالات تتم عن طريق البريد الالكتروني أو في شكل المحادثة الفورية ،[1] فهي الأكثر استخداما فيما يقتصر النص على بسط الحماية فقط للمحادثات الخاصة التي تتم عن طريق خطها تقني، ما يدفعنا إلى القول أن هذه المراسلات الالكترونية بمعزل عن الحماية القانونية.

وفي هذا الصدد نرى ضرورة تدخل المشرع الجزائري بالنص على تجريم سلوك انتهاك المراسلات التي تتم عبر شبكة الانترنت، التي يمكن أن تأخذها هذه المراسلات أو المحادثات لكن تطبيق مبدأ عدم جواز انتهاك سرية المراسلات والاتصالات يجد حدوده عندما يكون الكشف عنها ضرورة لتحقيق المصلحة العامة، وهذه الضرورة تجد محلها في الجرائم الالكترونية بعدما أثبتت الإجراءات التقليدية فشلها في إزالة الستار عن غموضها، ما تطلب كشفها وجوب اعتراض المراسلات والاعتداء بذلك على هذه الحرمة، وهذا ما أخذ به المشرع الجزائري في المادتين 3 و 4 من القانون 04/09 والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ولكن من خلال استقراء هذه المواد نجد أن المشرع أحاط هذه الإباحة ببعض الضمانات القانونية الفعالة لحماية الحرية الفردية، وحماية حق الإنسان في سرية اتصالاته.وتشمل هذه الضمانات في:

-إباحة المراقبة بإذن القانون:

لقد نصت المادة 03 من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال السابق ذكرها، على إباحة المراقبة الالكترونية، إلا أنه وطبقا لنص المادة 65 مكرر 5 من قانون الإجراءات الجزائية لا يمكن لضابط الشرطة القضائية اللجوء إلى اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب وسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة تحقيق قضائي، ولا يشترط وفقا للقانون 04/09 إلى هذا الإجراء القسري أن تكون الجريمة متلبس بها كما هو

[1]- عائشة بن مصطفى قارة، حجية الدليل الالكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 169.

منصوص عليه في المادة 65 مكرر 5 بل حتى في الأحوال العادية بالنسبة للبحث والتحري في الجرائم الالكترونية.

وهكذا يجب أن يكون الإذن المسلم لضابط الشرطة القضائية مكتوبا ،كما يجب أن يستوفي الإذن جميع العناصر الضرورية فيكون موقعا عليه ممن أصدره ومحددا لمدة نفاذه تحت طائلة البطلان، فمن خلال التاريخ يمكن حساب المدة التي يجب تنفيذ العملية خلالها، إلا أن المشرع الجزائري لم يستوجب هذه البيانات بالرغم من حرصه على وجوب ذكر تاريخ المحضر المعد للاعتراض فكان عليه من باب أولى أن يشترط تاريخ الإذن حتى يبسط القضاء رقابته على شرعية هذه العملية.ويجب التنويه أيضا أن يرد في الإذن اسم الشخص المراد مراقبة اتصالاته، فلا يجوز أن تمتد الرقابة إلى اتصالات غيره، ومتى حصل ذلك فإن البطلان يطال إجراء المراقبة.[1]

2-2-2: فائدة المراقبة الالكترونية في إظهار الحقيقة:

قررت التشريعات المعاصرة أن ضابط فائدة المراقبة في ظهور الحقيقة يعتبر السند الشرعي المبرر للمراقبة والاعتراض، ذلك أن هذا الإجراء يتضمن اعتداء جسيما على حرمة الحياة الخاصة وسرية الاتصالات، فيباح في حدود ضيقة وذلك للفائدة المنتظرة منه، والتي تتعلق بإظهار الحقيقة بكشف غموض الجريمة وضبط الجناة[2] وبالنظر إلى التشريعات المعاصرة، والتي تجيز اللجوء إلى المراقبة، نجدها تقيد مباشرة المراقبة بكونها تفيد في كشف وظهور الحقيقة، على النحو الذي يمكن أن تقرر معه أن ضابط فائدة المراقبة في ظهور الحقيقة يعتبر السند الشرعي للمراقبة، بل إن هناك من

[1]- يثير تساؤل في هذا المجال عن مدح امتداد المراقبة إلى مراسلة موجهة إلى طرق آخر يستعمل البريد الالكتروني للمشتبه به أو عن طريق ربط الاتصال (Le raccordement de télécommunication) ، واتجه الفقه إلى جواز ذلك لأن المراقبة تشمل كل مراسلات المشتبه به ولو تعلقت بغيره أو كان المرسل مجهول الهوية حتى لا يفلت هذا الأخير من المراقبة لأن يمكن للطرف والثالث أن يلغي دور الوسيط في المراسلة : انظر، فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجنائية، مجلة العلوم الإنسانية جامعة منتوري، قسنطينة، الجزائر، العدد 33، جوان 2010، ص 239.

[2]- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 176

اشترط علاوة على ذلك أن لا يتم اللجوء إلى المراقبة إلا إذا كانت الإجراءات التقليدية عاجزة وغير كافية لإظهار الحقيقة.[1]

والرجوع إلى المشرع الجزائري وتحديد المادة 04 من القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وهذا بقولها: ". .. عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية. ... ".

2-2-3: قصر القيام بالمراقبة في جرائم الكترونية معينة:

إذا كانت الضرورة المتعلقة بصعوبة كشف الجريمة الالكترونية هي المبرر لشرعية مراقبة الاتصالات الالكترونية، فإن المشرع الجزائري حدد في المادة 04 فقر 01 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وهذا بقولها: " يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 أعلاه في الحالات الآتية:

أ- للوقاية ممن الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة.

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

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

د- في إطار تنفيذ طلبات المساعدة القضائية المتبادلة. .... ".

وعليه فالمشرع الجزائري رخص القيام بالمراقبة الالكترونية في تلك الجرائم التي تمس بالمصالح الأساسية في الدولة والجرائم الموصوفة بأفعال إرهابية أو تخريبية والماسة بأمن الدولة كما يرخص بالمراقبة في حالة عدم الحصول على الدليل إدانة وحالة المساعدة القضائية المتبادلة.

[1] - Ann Jacobs, la loi du 6 janvier 2003 concernons le méthodes particulière de recherche et quelque autres méthodes d'enquêtes, revue de la faculté de droit de l'université de liège, Canada, 2004, p 41.

كما أن الفقرة الأولى –أ– لم تحدد إن كانت تلك الجرائم ترتكب بواسطة تقنية المعلومات أو ترتكب كجريمة تقليدية، كما أن الفقرة الأولى ج–د تنص على أن المراقبة قد تكون عادية أو الكترونية ما دامت تهدف إلى الوصول إلى الحقيقة وحتى بالنسبة لكل الجرائم في إطار المساعدة القضائية الدولية المتبادلة.

وفي الأخير هنا نقطة ينبغي الإشارة إليها ونحن بصدد المراقبة الالكترونية، وهي أنه إذا كان القانون قد سمح بجواز المراقبة الالكترونية لمقتضيات التحريات بالنسبة للجريمة الالكترونية التي وقعت بالفعل، فإن تقرير شرعية المراقبة حتى بالنسبة لجريمة معلوماتية لم تقع بعد ولمجرد وقوع احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني، أو مؤسسات الدولة والاقتصاد الوطني كما فعل المشرع الجزائري هو مسلك محل نظر، خاصة وأن المراقبة الالكترونية هي إجراء استثنائي ينطوي على مساس خطير يحق السرية والخصوصية، وأن المشرع منح حق اللجوء إليها بشأن مجرد احتمال اعتداء على المنظومة المعلوماتية.

وكان على المشرع فرض قيود إجرائية أكثر صرامة للحياة الخاصة، على سبيل الاقتداء بالمشرع الألماني والسويسري اللذان لا يسمحان بالمراقبة الالكترونية إلا إذا وقعت الجريمة فعلا، لأن في ذلك زيادة في المساس بحرمة الحياة الخاصة.[1]

وفي تقديرنا أن شرعية اللجوء إلى المراقبة لمجرد وجود احتمال اعتداء على منظومة معلوماتية يشكل تعديا صارخا على قرينة البراءة من المشرع الجزائري، الذي ينبغي عليه إعادة التوازن بين عنصر الفعالية والمتمثل في ضرورة التحري وعنصر الشرعية.

2– التزامات مقدمي الخدمات:

نظرا لما تتطلبه ملاحقة الجرائم الالكترونية من تقنيات خاصة فقد أجازت التشريعات الجنائية الاستعانة بذوي الاختصاص سواء عن طريق تسخير من لديهم خبرة في مجال عمل المنظومة المعلوماتية بغية مساعدة الجهة القائمة بتفتيش المنظومة المعلوماتية وتزويدها بكل ما من شأنه تسهيل

[1] - Sylvian Métille Méssure de surveillance sécrètes, le rôle de l’information dans la protection des droits de l’individu, revue de plaidoyer, paris, France 2001, p 33.

مهمتها، وذلك عن طريق تكليف هؤلاء المختصين باستعمال الوسائل التقنية المناسبة والضرورية للحيلولة دون الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، ومنع القيام بأي استعمال لها أو نسخها أو الاطلاع عليه، والمقصود هنا تلك المعلوماتية التي تشكل محل الجريمة أو تحتوي على أدلة لها كل ذلك لمنع تهديدها أو تدمير تلك الأدلة المؤدية لها.[1]

ولكي يتسنى الوصول إلى تلك الأدلة كان من الضروري إلزام الأطراف المتدخلة في خدمات الانترنت بتقديم المساعدات الضرورية للجهات المكلفة بالتفتيش والسلطات القضائية المتخصصة والتي خصص لها القانون 04/09 المتضمن القواعد الخاص وللوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته في الفصل الرابع منه " وفيما يلي تفصيل ذلك:

2-1: مساعدة السلطات:

يقتضي التعرض لالتزامات مقدمي الخدمات في مساعدة السلطات التطرق أولا إلى تعريف مصطلح مقدمي الخدمات والذي عرفته المادة الأولى فقرة -د-

(**د- مقدمو الخدمات:** 1- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات.

2- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال أو لمستعمليها).[2]

وبالرجوع إلى المادة 10 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، نجدها قد ألزمت مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية والتفتيش.

---

[1]- زبيحة زيدان، المرجع السابق، ص 153.

[2]- وهو ذات التعريف الوارد في المادة 01 من اتفاقية بودابست المنعقدة في 23 نوفمبر 2001 وعرفته المادة 02 الفقرة 02 من الاتفاقية العربية لمكافحة تقنية المعلومات بأنه :" أي شخص طبيعي أو معنوي عام أ خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها ".

ومن المعلوم أن مقدمي الخدمات في مجال الانترنت عديدون ويطلق عليهم أحيانا الوسطاء في خدمة الانترنت، ودور هؤلاء في خدمة الانترنت، ودور هؤلاء هو تمكين مستخدم الانترنت من الدخول إلى الشبكة والإطلاع عما يبحث عنه، مزود الخدمة بإمكانه مراقبة جميع الخطوات التي يتبعها هذا المستخدم إذ بإمكانه معرفة المواقع التي زارها والمعلومات التي خزنها وكل الاتصالات التي أجراها.[1] ومن هنا فإن مزود الخدمة بإمكانه تمكين جهات التحقيق بكل المعلومات التي تساعدها أو التي تبحث عنها، بل هو ملزم بذلك وفقا لنص المادة 10 المشار إليها ثم يوجد أيضا متعهد توصيل الخدمات ودوره تقني يتجسد في إيصال المستخدم إلى شبكة الانترنت وذلك يربطه بالمواقع التي يريدها وليس له علاقة بالمعلومات أو بمحتواها، وهناك أيضا متعهد الإيواء الذي يعمل على إيواء صفحات () على حاسوبه لخادم مقابل أجر لصالح المستخدم الذي يعمل على نشر ما يريد من صور أو معلومات أو يقوم بربط علاقات على مواقع أخرى.[2]كما يتعين على مقدم الخدمة كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها.[3]

2-2: حفظ المعطيات المتعلقة بحركة السير:

عرف المشرع الجزائري المعطيات المتعلقة بحركة السير في الفقرة هـ من المادة 02 من القانون 04/09 السابق الذكر، وهذا بقوله: ". .. المعطيات المتعلقة بحركة السير أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسلة إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم مدة الاتصال ونوع الخدمة ".

وتنص المادة 11 من القانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه: " مع مراعاة طبيعة ونوعية الخدمات يلزم مقدمو الخدمات بحفظ:

أ- المعطيات التي تسمح بالتعرف على مستخدمي الخدمة.

---

[1]- زبيحة زيدان، المرجع السابق، ص 154.

[2]- للمزيد أنظر : عبد الفتاح بيومي حجازي، النظام القانوني للتجارة الالكترونية ، مرجع سابق، ص 135.

[3]- من المادة 10 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

ب- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

ج- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

هـ- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكور في فقرة أ من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه. ..".

ويفهم من المادة أعلاه إجراء الحفظ يتم قيام مقدمي الخدمات بإجراء التجميع والتسجيل ثم الحفظ في النهاية إلى يد السلطات المكلفة بالتحريات القضائية، وتكتسي هذه الإجراءات أهمية بالغة من حيث كونا أداة تنقيب وتحري مفيدة من أحل تحديد مصدر الاتصال ومآله عن طريق أرقام الهاتف، كما توفر بيانات مرتبطة بالساعة والتاريخ والمدة المتعلقة بأنواع الاتصالات غير المشروعة.[1]

ويعتبر إجراء الحفظ إجراء وقتي، حدده المشرع الجزائري في المادة 02 أعلاه في الفقرة 03 بمدة سنة، ابتداء من تاريخ التسجيل، وتأتي تحديد هذه المدة احتراما للحق في الخصوصية، إذ يلزم مقدم الخدمات بمسح المعطيات التي يتم حفظها ويقع تحت طائلة العقوبات كل ما يؤدي إلى عرقلة حسن سير التحريات القضائية.

2-3: التزامات خاصة بمقدمي خدمة الانترنت:

إضافة إلى الالتزامات المقررة في المادة 11 السابق ذكرها يتعين أيضا على مقدمي الخدمات القيام كما يلي:

(أ- التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

[1]- هلالي عبد الله احمد، الجوانب الإجرائية والموضوعية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، المرجع السابق، ص 259.

ب- وضع ترتيبات تقنية تسمح بحر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها).

الفصل الثاني

الجهود الدولية لمكافحة جريمة التزوير الالكتروني

الفصل الثاني:الجهود الدولية لمكافحة جريمة التزوير الإلكتروني

نظرا لما تستمر به الجريمة الالكترونية في كونها ذات طابع عالمي عابر للحدود، حيث يمكن لأحد مستخدمي شبكة الانترنت وهو في مكانه، ومن خلال حاسوبه الشخصي التنقل الكترونيا من شبكة إلى أخرى و قواعد البيانات في دول أو قارات مختلفة، فضلا عن إمكانية إخفاء هويته على الشبكة وسهولة تدمير وإتلاف الدليل الالكتروني الناتج عنها.

تلك الصفة العالمية العابرة للحدود والتي تمثل عقبة أمام سلطات التحري والتحقيق ظهرت من خلالها مبررات وأهمية التعاون الدولي في مجال التحقيق الجنائي في الجريمة، باعتباره خطوة على تدويل القانون الجنائي وإحداث تشابه وتقارب بين القواعد الموضوعية والإجرائية على المستوى الدولي.

فضلا عن أن البعد الدولي للجريمة الالكترونية يستدعي ضرورة وجود تعاون دولي فعال متزايد وسريع في المسائل العقابية والإجرائية، وذلك للحد من الفراغ التشريعي المنظم لها.

ومن هنا تظهر أهمية استحداث آليات جديدة بشأن التعاون الدولي ووضع قواعد جديدة لأحكام الجنائي والإجرائي لتواكب هذا النوع المستحدث من الإجرام وللتعاون الدولي صور عديدة تتمثل في التعاون الشرطي الدولي، والتعاون في المجال القضائي إلا أن هذه المظاهر أو الصور تواجهها العديد من التحديات التي تحول دون مواجهة الجرائم الالكترونية، وهذه الآليات والمظاهر والصور والتحديات التي تواجهها في محل دراستنا في هذا الفصل.

وبناء على هذا سوف نقسم هذا الفصل إلى مبحثين نتناول في المبحث الأول الجهود الدولية لمكافحة جريمة التزوير الإلكتروني في إطار الأجهزة الدوليةأ ما المبحث الثاني سنخصصه لدراسة التحديات التي تواجه التعاون الدولي في مجال مكافحة جريمة التزوير الالكتروني.

المبحث الأول: الجهود الدولية لمكافحة جريمة التزوير الإلكتروني في إطار الأجهزة الدولية:

إن ثورة المعلومات والتقنيات الحديثة التي لم تشهد لها البشرية مثيلا من قبل قد فرضت نفسها على واقع الحياة والمعاصرة، فقد دخلت التكنولوجيا جميع مجالات الحياة، أدى إلى ظهور جرائم مستحدثة لم تكن معروفة من بينها الجرائم الالكترونية، ونظرا للطابع الدولي عبر الوطني التي تتميز به هذه الأخيرة تجعل من الصعب على أي دول بمفردها ومهما كانت الوسائل والموارد المتوفرة لديها أن تتصدى لها

بشكل كافي دون أن تعتمد على أشكال التعاون الدولي والذي يقصد به بتبادل المساعدة وتضافر الجهود المشتركة بين دولتين أو أكثر لتحقيق نفع أو خدمة في مجال مواجهة الإجرام وكل ذلك يكون في إطار إبرام الاتفاقيات الدولية سواء كانت جماعية أو ثنائية[1].

ويشمل التعاون الدولي في المجال الأمني الذي لا يعتبر مطلبا رئيسيا فحسب لضبط الحياة وتسليمهم للعدالة بل يعتبر أهم التدابير المانعة من ارتكاب الجريمة قبل وقوعها، ويشمل كذلك التعاون بين البلدان في المجال القضائي حتى يتم ملاحقة وتتبع الجناة وكذا تتبع اثر النشاط الإجرامي، وكذا التعاون في مجال تسليم المجرمين، حيث فبغير التعاون الدولي سيزداد معدل ارتكاب هذه الجريمة ويطمئن مرتكبوها من عدم إمكانية ملاحقتهم إذ يكون من السهل عليهم التنقل من دولة إلى أخرى تتيح القوانين المطبقة بها بما ارتكبوه من جرائم وعليه سيحاول من خلال هذا المبحث تسليط الضوء على هذه الصور في المطالب الآتية:

المطلب الأول: التعاون الأمني والدولي لمكافحة جريمة التزوير الالكتروني :

تعد جريمة التزوير الالكتروني كغيرها من الجرائم الالكترونية التي تتميز بالعالمية وبكونها عابرة للحدود وعليه فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي حيث يستحيل على الدولة بمفردها القضاء على هذه الجرائم، ومن هنا أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة، وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة خاصة وفيما يتعلق بتبادل المعلومات المتعلقة بالجريمة بأقصى سرعة ممكنة، بالإضافة إلى تعقب المجرمين الفارين من وجه العدالة.

وتتمثل أوجه هذا التعاون الأمني في إنشاء المنظمة الدولية للشرطة الجنائية على الصعيد الدولي، إضافة إلى إنشاء وحدات متخصصة على المستوى الأوروبي، ناهيك عن مجهودات على المستوى العربي وتتناول هذه الصور في الفروع الآتية :

[1]– سليمان احمد إبراهيم، القواعد الجنائية للجريمة المنظمة والتعاون الدولي في سبيل مكافحتها، دون طبعة، دار الكتاب الحديث، مصر، 2008، ص 294.

الفرع الأول: التعاون الأمني في إطار الأجهزة العالمية:

يتمثل التعاون الأمني على الصعيد الدولي في إنشاء ما يسمى باللجنة الدولية للشرطة الجنائية الأنتربول، وقد غير اسمها ليصبح المنظمة الدولية للشرطة الجنائية وتضم في عضويتها أكثر من 189 دولة عضو، وتعد اكبر منظمة شرطة دولية، أنشأت عام 1923 مقرها باريس.

ترجع البدايات الأولى للتعاون الدولي الشرطي إلى عام 1904 عندما تم إبرام الاتفاقية الدولية الخاصة لمكافحة الرقيق الأبيض بتاريخ 1904/05/18 الخاصة بمكافحة الرقيق الأبيض، بعد ذلك أخذ التعاون الشرطي الدولي يأخذ صور المؤتمرات الدولية أو لها وأسبقها تاريخ مؤتمر موناكو (14-1914/18) والذي ضم رجال الشرطة والقضاء والقانون من 14 دولة الذي وضع أسس التعاون الدولي في المسائل الشرطية، ولم يحقق النجاح نتيجة لقيام الحرب العالمية الأولى.
وبنهاية 1923 نجح الدكتور "رجوهانو سويرا" مدير شرطة فينا في عقد مؤتمر دولي للشرطة الجنائية (3-1923/9/7) تمخض عنه ولادة اللجنة الدولية للشرطة الجنائية مقرها فينا، تعمل على التنسيق بين أجهزة الشرطة من اجل التعاون في مكافحة الجريمة إلا انه باندلاع الحرب العالمية الثانية توقفت اللجنة عن إهمالها إلى غاية 1946، حيث عقد ببروكسل بلجيكا في الفترة الممتدة (6-1946/9/4) مؤتمر دولي يهدف إحياء مبادئ التعاون الأمني وانتهى الاجتماع إلى إحياء اللجنة الدولية للشرطة الجنائية ونقل مقرها إلى باريس وغير اسمها ليصبح المنظمة الدولية للشرطة الجنائية،وتسعى هذه الأخيرة االى توطيد التعاون البوليسي في العالم بفضل مكاتب مركزية وطنية في 189 بلد، وهذه المكاتب عبارة عن مصالح شرطة دائمة تتكون من رجال شرطة يعملون في إطار قانوني، وهو الوسيط الوطني في العمليات البوليسية المطلوبة من باقي الدول الأعضاء [1]

ويتمثل دور الأنتربول في تسهيل تبادل المعلومات من اجل مكافحة فعالة لجميع أنواع الجريمة، لاسيما الجريمة، إذ تملك نظام اتصال معلوماتي مشترك بين جميع الدول الأعضاء تعمل طوال الساعة، وطيلة أيام الأسبوع، ومجموعة قاعدة بيانات لمعلومات الشرطة ومصالح مختصة في تحليل المعلومات

[1]- Michael Moran. Interpol et la lutte contre la cybercriminalité ;actes du séminaire internationales sur la lute cotre la cybercriminalité. Organise par la centre de recherche juridique et juridiciare a Alger le 5-6 mai 201 ; 1ére édition. 2011, P 163.

حول الجرائم الالكترونية ولا يمكن لأعضاء هذا الجهاز التدخل إلا بطلب مساعدة من الدولة من الدولة المعنية وفقا للإجراءات القانونية[1].

وتستهدف هذه المنظمة تأكيد وتشجيع التعاون بين السلطات والشرطة في الدول الأطراف على نحو فعال يحقق مكافحة الجريمة، وذلك بتجميع البيانات المتعلقة بالمجرم والجريمة وتبادل المعلومات والبيانات فيما بين الدول والتعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف ومدها بالمعلومات المتوفرة لديها على إقليمها أي أن عضو الأنتربول لا يقوم بنفسه بإجراء القبض على المجرم، بل أن الأمر منوط بجهاز الشرطة الوطنية في الدولة التي يتواجد على إقليمها.[2]

وفي مجال الإجرام المعلوماتي يعد الأنتربول أداة متميزة لتبادل المعلومات المتعلقة بالجريمة في فضاء الانترنت بين جبهات الضبط القضائي، وهي ناقل أساسي لجميع المعلومات في إطار البحث والتحري عن الجرائم، فيقوم الأنتربول باطلاع مصالح البحث والتحري الوطنية عبر المكاتب المركزيين الوطنية على بعض المعلومات المتعلقة بالجرائم المعلوماتية، وفي هذا الصدد تقوم هذه المكاتب بإعداد بيانات وصفية دولية، تتعلق خاصة بأشخاص متابعين بغرض تسليمهم [3].

وقد أكدت المنظمة في عدة مؤتمرات لها، إذ ينظم الأنتربول مدة كل عامين مؤتمرا دوليا بشأن الإجرام الالكتروني لمواجهة أحدث التقنيات في مجال مكافحة الجرائم الالكترونية، ولعل أهمها المؤتمر المقام في لندن في 2009/10/09 وفي القاهرة بتاريخ 13-2005/04/15 الذين تم فيه التأكيد على ضرورة إيجاد تعاون دولي لمكافحة هذا النوع المتميز من الإجرام، بحيث تعين كل دولة الإدارة المكلفة بالسهر على هذا النوع من القضايا لتلقي البلاغات واتخاذ الإجراءات المناسبة حسب قوانين بلادها.[4]

ولا يقتصر عمل الأنتربول في مجال مكافحة الجريمة الالكترونية في صور عقد واحتضان المؤتمرات الدولية بل يعمل الأنتربول لأجل تجسيد ذلك ميدانيا وهذا من خلال العمل ماس دعم إجراءات البحث والتحقيق بشأنها من خلال:[5]

---

[1]- Michael Moran. O cit. p 161.

[2]- جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالانترنت، المرجع السابق، ص77.

[3]- Queemener Myriam، Févry Joél. Op cit. p 236.

[4]- جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالانترنت، المرجع السابق، ص 77.

[5]- Myriam Queemener –Yves Chupenel. La cybercriminalité. Op cit. p 208.

– جمع وتخزين وتحليل المعلومات المتعلقة بالجرائم المعلوماتية مع توفيرها لكافة الدول الأعضاء بواسطة منظومة 24/7 للأنتربول، وهي عبارة عن شبكة اتصالات شرطية مأمونة تربط بين الدول الأعضاء.

وتم تطوير هذه الشبكة من خلال دعمها لمنظومة I–LINK التي تعتبر المركز الرئيسي لتبادل المعلومات الجنائية والتواصل بين الدول الأعضاء وهي منظومة اتصالات محسنة مقارنة بمنظومة I24/7 وتضمن عدة من الوظائف التي تضمن نقل وتبادل المعلومات الشرطية تبادلا المعلومات الرطية تبادلا فعالا من خلال استحداث معيار منسق للاتصالات تسهيلا لتبادل المعلومات الشرطية وإمكانية التحكم المباشر في البيانات والتدقيق فيها مع تسجيل أحدث المعلومات في قاعدة البيانات الجنائية.

– تقديم الدعم لمصالح الشرطة على المستويين الدولي والداخلي.

– تكوين وتأطير أعوان الشرطة من خلال تنظيم دورات تكوينية تسمح لأعوان الشرطة تحسين قدراتهم علة التعامل مع منظومة الاتصال I LINK/7 I 24 في إطار التعاون الدولي لمكافحة الجرائم الالكترونية.

وتحقيقا للتعاون بين الدول أيضا، أنشأت المنظمة الدولية للشرطة الجنائية وحدة خاصة لمكافحة جرائم التكنولوجيا، كما وضعت استراتيجيات محكمة لمكافحة هذا النوع مع مجموعة الدول الثمانية الكبرى وذلك بإنشاء مركز اتصالات أمني عبر الشبكة يعمل على مدار 24 ساعة و7 أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأطراف مع تزويد هده المصالح بوسائل حديثة في سبيل مكافحة هذه الجرائم والتحقيق فيها.[1]

وتبدو أهمية الأنتربول من خلال الإحصاءات الصادرة عن الأمانة العامة، وذلك من خلال قيامها بجهود كبيرة في مجال نشر أوصاف المجرمين، وكشف الكثير من القضايا الدولية وضبط مرتكبيها، وبعد أن أصبحت المنظمة تضم معظم دول العالم فلقد لاقت انجازاتها احترام وتقدير المنظمات الدولية الأخرى.[2]

[1]– نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص ص153–154.

[2]– الهام بن خليفة، المرجع السابق، ص 341.

الفرع الثاني: التعاون الأمني على المستوى الأوروبي

من أهم أجهزة التعاون الأمني المكلفة بمساعدة السلطات الإجرائية الداخلية في البحث والتحري عن الجرائم بصفة عامة والإجرام المعلوماتي بصفة خاصة في القارة الأوروبية الأوروبول والمركز الأوروبي للجريمة الالكترونية، كما تم إنشاء فضاء جماعي من غير حدود أطلق عليه معاهدة شنجن، وكذا إنشاء جهاز لمواجهة جميع أنواع الجرائم الخطيرة المتمثل في الأوروجست.

أولا: الأوروبول أو مركز الشرطة الأوروبية.

الأوروبول هو أحد الأجهزة المتواجدة على المستوى الأوروبي، مقره لاهاي، وقد تم إنشاؤه بموجب اتفاقية 26 جويلية 1995، وهو جهاز مكلف بمكافحة الإجرام عن طريق معالجة المعلومات المرتبطة بالأنشطة الإجرامية على مستوى الإتحاد الأوروبي ودعم وتشجيع سلطات التحقيق وذلك بتكميل وسائلهم وتحديثها من اجل مكافحة جميع أنواع الإجرام المنظم الدولي الخطير، وكذا تسهيل تبادل تلك المعلومات عن طريق تزويد المحققين بتحاليل عملية وإستراتيجية، وبدعمهم بخبراتهم ومساعداته التقنية [1].

ويقدم جهاز الأوروبول خبرته ودعمه الفني في التحقيقات والعمليات التي تتم داخل الاتحاد الأوروبي، كما تقوم الوحدة الوطنية الأرووبول بتامين التواصل بين الأوروبول والدول المنشأة ضمن الإدارة المركزية للشرطة القضائية بحيث يقع على دول الاتحاد إنشاء هيئات مركزية تكفل تأمين الاتصال بينه وبين السلطات الإجرائية للدول الأعضاء.[2] ويغطي عمل جهاز الشرطة الأوروبية الدول 27 الأعضاء في الاتحاد الأوروبي، لمكافحة الجرائم العابرة للحدود ومنها جرائم الحاسب الآلي والانترنت، وأصبح لهذا الجهاز صلاحيات واسعة في تجميع المعلومات والأدلة ويقوم جهاز الشرطة الأوروبية بإقامة العديد من الدورات التدريبية المتعلقة بمكافحة الجريمة والتي يشارك فيها ممثلون عن الدول الأوروبية وغيرها[3].

[1]– نبيلة هبة هدوال، الجوانب الإجرامية لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 160.

[2]– Queminer Myrain , Fervy Joél.op cit. p 237.

[3]– أسامة بن غانم العبيدي، الجهود الدولية في مكافحة الجريمة المعلوماتية، مجلة الحقوق العدد4، الكويت 2015، ص ص124-125.

ثانيا: المركز الأوروبي للجريمة الالكترونية

إلى جانب مركز الشرطة الأوروبية سعت الدول الأوروبية إلى تعزيز التعاون الشرطي بينها وذلك من خلال آلية مختصة على وجه التحديد بمكافحة الجريمة الالكترونية التي لا يمكن بحال معرفة حدودها إلى جانب قدرة منفذيها على التوالي إلى استجابة مرنة وكافية، لذا تم تصميم المركز الأوروبي للجريمة الالكترونية، للدر على الجرائم الالكترونية بالإضافة إلى قدرته على تعبئة كل مصادر الدول الأعضاء في الاتحاد الأوروبي التي من شأنها تقليص والحد من آثار تهديدات المجرمين الإلكترونين أينما حلوا [1].

ويهدف هذا المركز إلى زيادة التعاون الدولي لحماية الدول الأوروبية ومواطنيها من الجرائم الالكترونية ويعمل المركز على تزويد الشرطة ووكالات إنفاذ القانون في الدول الأعضاء بمعلومات حول اتجاهات الجرائم الالكترونية الجارية، وكذا تقديم الخبرة التقنية عالية المستوى والتحليلية والقضائية عند وجود تحقيقات مشتركة بين دول الاتحاد وسيقوم بإنشاء أدوات قضائية تساعد الدول الأعضاء على البحث والتحري في الجرائم الالكترونية بكفاءة أكثر والنجاح في محاكمة المسؤولين عن الجرائم [2].

ويضع المركز الأوروبي للجريمة الالكترونية والذي يتم تمويله من قبل وكالة الشرطة الأوروبية التي يتخذ من لاهاي مقرا له مجموعة من الأهداف وهي الاختيال المصرفي عبر الانترنت والاعتداء على الأطفال، والجرائم التي تستهدف البنية الحسية وتظم تقنية المعلومات التابعة للاتحاد الأوروبي، وبعدها إلى هذا المركز مهمة إعداد تقرير سنوي عن الجرائم الالكترونية في دول الاتحاد، ومن مهامه أيضا تبادل مع المعلومات مع أجهزة الشرطة الأوروبية وغيرها من مرتكبي هذه الجرائم والأساليب التي يستخدمونها في ارتكاب جرائهم. [3]

ثالثا: معاهدة شنجن:

استحدثت معاهدة شنجن نظام شنجن المعلومات الذي يعد من الأنظمة الجيدة للتعاون الأمني الدولي واحترام الحقوق والحريات الأساسية ،ويتكون من قسم مركزي مقره مدينة ستراسبورغ وأقسام وطنية

[1]– Commission européenne communiqué de presse. Le centre européen de lutte contre la cyber criminalité (EC3) Bruxelles le 9 janvier 2013 disponible a l'adresse suivante http// europa eu /rapid/ press- release IP-13-13-FRhtm. Consulté le 13/ de /2018.)

[2]– أسامة غانم، العبيدي، المرجع السابق، ص 126.

[3]– حسين الغافري، المرجع السابق، ص 635.

في كل دولة من دول المنظمة ،وبنك معلومات كبير تسجل عليه كل المعلومات التي ترسلها قوات الشرطة والسلطة القضائية في كل دولة وتتمثل هذه المعلومات في عناوين الأفراد سواء أولئك المطلوب تسليمهم من قبل دول أخرى أو الممنوعين من دخول أراضي دولة ما، أو المعلن عن اختفائهم أو المطلوب تقديمهم للعدالة بأمر قضائي لأي سبب كان [1].

وتعزيزا للتعاون الشرطي الأوروبي استحدثت المعاهدة وسيلتين لمكافحة الإجرام المنظم وذلك لمراقبة المشتبه فيهم عبر الحدود، إذ يحق لرجل الشرطة في إحدى الدول الأطراف وعلى سبيل الاستدلال أن يراقب الشخص المشتبه به الموجود على إقليم دولة أخرى واتخاذ جميع الإجراءات اللازمة من معاينة واقتفاء أثر المشتبه به. كما يحق لرجل الشرطة أن يتجاوز حدود إقليم دولته ليلاحق الجناة على إقليم دولة أخرى طرف وهذا في حالات التلبس بإحدى الجرائم الجسمية على سبيل الحصر وفي حالة في فرار الشخص المحبوس[2].

رابعا: الأورجست

إلى جانب الأوروبول يتواجد على المستوى الأوروبي الأورجست كجهاز يساعد على التعاون القضائي والشرطي في مواجهة ومكافحة جميع أنواع الجرائم الخطيرة، وهو جهاز تابع للاتحاد الأوروبي مكلف بتحسين فعالية السلطات المختصة للدول الأعضاء في مكافحتهم للجريمة المنظمة العابرة للحدود كالجريمة المعلوماتية عبر الوطنية من خلال تنسيق التحريات والتحقيقات، وهي تساعدهم على تعزيز فعالية المتابعات وقد تم إنشاؤه بموجب القرار الصادر عن مجلس الاتحاد الأوروبي بتاريخ 28 فيفري 2002 [3].

وتجدر الإشارة إلى أن الأورجست يمثل دعامة في فعالية التحقيقات والمطاردات المتبعة من قبل السلطات القضائية وخصوصا فيما يتعلق بالأنشطة المرتبطة بالجرائم الالكترونية وتتلخص في :

- ✓ تعزيز وتحسين التنسيق بين السلطات المختصة في الدول الأعضاء فيما يتعلق بالتحقيقات والملاحقات القضائية في الدول الأعضاء، مع الأخذ بعين الاعتبار أي طلب يصدر من السلطة

[1]– إلهام خليفة، المرجع السابق، ص ص 342–343.

[2]– نبيلة هبة هروال، الجوانب الإجرامية لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 163.

[3] Queminer, Myrain fervy joél.op cit. p 238.

المختصة في الدولة العضو، وأي المعلومات المقدمة من أي جهة من السلطة المختصة بموجب الأحكام المعتمدة للمعاهدات.

- ✓ تحسين التعاون بين السلطات المختصة في الدول الأعضاء، ولاسيما من خلال تسهيل تنفيذ المساعدة القانونية الدولية وتنفيذ طلبات تسليم المجرمين.
- ✓ تقديم الدعم للسلطات المختصة في الدول الأعضاء وعلى تعزيز فعالية التحقيقات والملاحقات القضائية [1].

وبالرغم من الدور العظيم الذي تلعبه هذه الهيئات لمساعدة البحث والتحري في الجرائم الالكترونية العابرة للحدود إلا أن هذا التعاون الدولي لا يزال تعترضه عقبات تحد من فاعليته لاسيما وأن الكثير من الدول لا تفضل التعاون مع الأنتربول كجهة تعاون عالمية، وتحبذ المساعدات الثنائية كالولايات المتحدة الأمريكية. [2]

فضلا عن ذلك فإن التطور الذي لازم هذه الهيئات كاعتماد وسائل للاتصال بها بدلا من ولوج وسائل تقليدية أكثر بطئا، غلا أن الإجراءات المعمول بها في سبيل التنقيب لا تتلاءم وطبيعة الجرائم الالكترونية مما يحملنا القول بأن عمل هذه الأجهزة يظل من غير فعالية في كثير من الأحوال لا سيما وان هذه الأجهزة ليست متخصصة قد تؤدي إلى نتائج مخيبة للآمال فقد صدرت أن حاولت نقطة اتصال في بلجيكا الاتصال بمراكز اتصال في ايطاليا لكن الأشخاص الذي رد على الاتصال لم يكن يتحدث غير اللغة الإيطالية. [3]

وهذا ما يتطلب الحاجة إلى تحديث آليات التعاون الدولي في التحري عن الجرائم الالكترونية خاصة وأن عددا كبيرا من اتفاقيات المساعدة القانونية المتبادلة القائمة يستند إلى إجراءات رسمية معقدة ومستهلكة للوقت غالبا، إذ أن الاستجابة لطلبات المساعدة تستغرق أشهرا وتطرح هذه الفترة الزمنية

---

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 160.

[2]– جون فرانسوا هركوت، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، بحيث مقدم ضمن أعمال الندوة الإقليمية حول جرائم المتصلة بالكومبيوتر، الفترة ما بين 19–20 يونيو 2007، الدار البيضاء المملكة المغربية، ص 101 منشور على الموقع الالكتروني http// undp–pogar–org/localuser/ progarp/ rule of / cybercrime –09 pdf. تاريخ الاطلاع على الموقع 2018/09/13.

[3]– نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 160.

تحديات على صعيد جمع الأدلة الالكترونية السريعة الزوال والتغيير [1]، وهو ما يدعو إلى إعادة النظر في آليات التعاون الدولي في البحث والتنقيب عن الجرائم الواقعة في الفضاء السيبيراني، بحثا عن وسائل تعاون دولي تضمن تامين المساعدة المطلوبة في الوقت المناسبة بشكل يتلاءم من طبيعة الأدلة التي تستمر بسرعة زوالها شرطية مأمونة تربط بين الدول الأعضاء.

الفرع الثالث: التعاون الأمني على المستوى العربي

إن التعاون الأمني العربي يعتبر امتداد للتعاون الإقليمي والدولي، وتعمل الدول العربية مع بعضها البعض جاهدة من أجل مواجهة الإجرام المنظم لاسيما الالكتروني في النطاق العربي.

وتتجلى مظاهر التعاون الأمني على المستوى العربي في مجلس وزراء الداخلية العرب تحت مظلة جامعة الدول العربية، إضافة إلى الاتفاقية الأمنية التي أبرمها أعضاء دول مجلس التعاون لدول الخليج.

أولا: مجلس وزراء الداخلية العرب

يعتبر مجلس وزراء الداخلية العرب أهم المنظمات الدولية الأمنية المتخصصة التابعة لجامعة الدول العربية، ويهدف إلى مكافحة الجريمة وتحقيق الأمن الداخلي والأمن الإقليمي فيما بين الدول العربية وذلك عن طريق دعم التعاون وتحقيق التكامل الأمني العربي[2].

ولقد برزت فكرة إنشاء مجلس وزراء الداخلية خلال المؤتمر الأول الذي عقد بالقاهرة في 1977، وتقرر هذا المجلس في المؤتمر الثالث لوزراء الداخلية بالدول العربية الذي عقد بمدينة الطائف بالمملكة العربية السعودية عام 1980 واتخذت الإجراءات اللازمة لوضع مشروع النظام الأساسي للمجلس وتم التصديق على نظامه الداخلي من قبل مجلس جامعة الدول العربية ليحل محل المنظمة العربية للدفاع الاجتماعي ضد الجريمة في ممارسة الاختصاصات المتعلقة بمجال الأمن العربي بمفهومه الشامل ومكافحة الجريمة، ويعد مجلس وزراء الداخلية العرب أعلى سلطة أمنية عربية مشتركة بعد مؤتمر القمة مؤتمر قادة رؤساء الدول العربية [3].

[1]– للمزيد أنظر: هلالي عبد الله أحمد، اتفاقية بوادبست لمكافحة الجرائم المعلوماتية، مرجع سابق، ص 397.

[2]– نادية دردار، الجهود الدولية لمكافحة الجريمة، الطبعة الأولى، المركز القومي للإصدار القانونية، مصر، 2017، ص 230.

[3]– غانم مرضي الشهري، المرجع السابق، ص 97.

ويهدف المجلس إلى تنسيق الجهود بين الدول العربية في مجال الأمن الداخلي ومكافحة الجريمة وتشمل اختصاصاته حسب المادة 04 من القانون الأساسي للمجلس في:[1]

أ- إنشاء الهيئات والأجهزة اللازمة لتنفيذ أهدافها.

ب- دعم الأجهزة الأمنية العربية ذات الإمكانيات المحدودة.

ت- تعزيز رسائل التعاون مع الهيئات الدولية المعنية باختصاصه.

وعقد المجلس عدة مؤتمرات في معالجة الظواهر الإجرامية المستحدثة التي أفرزها التطور الهائل الذي يعرفه العالم مع التركيز على جرائم محددة لاسيما الجرائم الالكترونية في المجال الأمني على غرار الدورة 17 للمجلس التي احتضنتها الجزائر في 2000، والتي من خلالها أنشئت في كل دولة من الدول الأعضاء شعبة اتصال بهدف التنسيق بين هذه الدول، وذلك بوضع نظام اتصالات عصري يربط الدول العربية وأجهزة المجلس.

كما أنشأ مجلس وزراء الداخلية العرب عدة مكاتب متخصصة في مكافحة الجريمة المنظمة العابرة للحدود وهي: المكتب العربي لمكافحة الجريمة ببغداد، المكتب العربي للشرطة الجنائية بدمشق، المكتب العربي لشؤون مكافحة المخدرات بالعاصمة الأردنية عمان، والمكتب العربي للحماية المدنية والإنقاذ بالدار البيضاء المغربية، وكذا المكتب العربي للإعلام الأمني بالقاهرة وذلك بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء بشأن مكافحة الجريمة وملاحقة المجرمين فيما يتعلق بالجرائم المنظمة العابرة للحدود والتي يمكن الاستفادة منها[2] في مجال مكافحة الجرائم الالكترونية، بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء[3].

ثانيا: الاتفاقية الأمنية لدول مجلس التعاون الخليجي.

وتعتبر الجهود العربية في مجال دعم وترقية سبل التعاون فيما بينها من أجل التصدي ومكافحة الجرائم المعلوماتية، جهودا محتشمة مقارنة بجهود الدول العربية، فقد كانت البدايات تتمحور حول دعم

---

[1]- الهام بن خليفة، المرجع السابق، ص 345.

[2]- بوحنة محمد، التعاون العربي في مجال الإعلام الأمني، مجلة الشرطة الجزائرية العدد 100، 2011، ص ص 70، 71. للمزيد اطلع على الموقع الالكتروني للمديرية العامة للأمن الوطني المتاح على الرابط www.dagsm.dz تاريخ الاطلاع: 13/06/2018.

[3]- محمد كمال عبد السميع شاهين، المرجع السابق، ص 144.

المواجهة الأمنية ضد الاعتداءات الماسة بحق المؤلف على أساس عدم انتشار الجرائم المعلوماتية بعد في الأقطار العربية.[1]

ولعل من بين الآليات على المستوى الأمني عربيا، نجد الاتفاقية الأمنية بين دول مجلس التعاون الخليجي، والتي تمر التوقيع عليها في مدينة الرياض بالمملكة العربية السعودية وهذا بتاريخ 2012/10/13، وهذا رغبة من الدول الأعضاء* في المحافظة على أمن واستقرار دول مجلس التعاون الخليجي، وتحقيق أكبر قدر من التعاون من أجل مكافحة الجرائم بجميع أشكالها لاسيما المعلوماتية، ورفع كفاءة الأجهزة الأمنية [2]

وتتمثل الأهداف المسطرة من خلال هذه الاتفاقية في:[3]

أ- تبادل المعلومات والخبرات التي تساهم في تطوير سبل منع مكافحة الجريمة على اختلافها وأنواعها، لاسيما المنظمة المستجدة، وتقديم الدعم الفني في جميع الشؤون الأمنية بما يحقق التكامل المنشود.

ب- توحيد القوانين والأنظمة والإجراءات بما يكفل مكافحة الجريمة بمختلف أشكالها وأنواعها وتحقيقا لأمن الدول الأطراف.

ت- تبادل القوانين والأنظمة واللوائح المتعلقة بعمل بعض الوزارات الداخلية وأجهزة الأمن الأخرى ذات الصلة، وكذلك الأبحاث والكتب والمطبوعات والنشرات التي تصدرها الوزارات والأجهزة المماثلة ووسائل الإيضاح والأفلام التربية الموجهة لديها.

ث- تقديم التسهيلات اللازمة في مجالات التعليم والتدريب لمنتسبي وزارات الداخلية والأجهزة المماثلة في الدول الأطراف في المعاهد والكليات والمؤسسات المخصصة لديها.

ج- إنشاء مراكز تدريب أمنية متخصصة في الفروع المختلفة التي تحتاج إليها أجهزة الأمن في الدول الأطراف.

---

[1]- حسين ربيعي، المرجع السابق، ص 140.

* تتمثل الدول الأعضاء في الإمارات العربية المتحدة، مملكة البحرين، المملكة العربية السعودية، سلطنة عمان، دولة القطر والكويت.

[2]- الهام بن خليفة، المرجع السابق، ص 346.

[3]- المادة 06 من الاتفاقية الأمنية لدول مجلس التعاون الخليجي نص الاتفاقية منشور على الموقع الالكتروني www.alanbar.com ثم الاطلاع على الموقع بتاريخ 2018/06/24.

ح- تزويد الدول الأطراف ببرامج المؤتمرات والندوات والحلقات الدراسية التي تعقدها في مجال اختصاص وزارات الداخلية وأجهزة الأمن.

خ- دعم الأجهزة الأمنية بأحدث التقنيات وتدريب العاملين من خلال دورات تدريبية مشتركة.

د- عقد اللقاءات الدورية وتبادل الزيارات الميدانية بين العاملين في وزارات الداخلية وأجهزة الأمن على جميع المستويات وفي مختلف الأنشطة بهدف يعيق الصلات وتوثيق التعاون والاطلاع على النظم المطبقة.

المطلب الثاني: جهود هيئة الأمم المتحدة والاتفاقيات والمعاهدات والجهود الدولية الأخرى في مكافحة جريمة التزوير الالكتروني.

لم يعد أثر الجرائم الالكترونية مقتصرا على بعض الدول أو على دول معينة بذاتها، بل أخذ يشمل المجتمع الدولي برمته مما أدى إلى إبرام اتفاقيات دولية متعددة في هذا الشأن، بالإضافة إلى عقد مؤتمرات دولية ذات أهمية ملحوظة في مجال مكافحة هذا النوع من الجرائم لتكون أكثر فاعلية في ملاحقة الجناة وردعهم ليس على الصعيد الوطني فقط بل كذلك الصعيد الدولي.

وسنبين في هذا المطلب جهود هيئة الأمم المتحدة والاتفاقيات والمعاهدات الدولية الأخرى في مكافحة الجرائم الالكترونية وهذا كالنحو الآتي:

الفرع الأول: جهود هيئة الأمم المتحدة.

لقد أكدت جميع المؤتمرات التي عقدتها الأمم المتحدة والمتعلقة بمنع الجريمة والعدالة الجنائية على أهمية التعاون في مكافحة الجريمة، إذ صدر عن مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين والمنعقد في فينا عام 2000 التركيز على مواجهة الجريمة، كما برز اهتمام هيئة الأمم المتحدة بالجرائم الالكترونية من خلال ما دعت إليه الجمعية العامة للأمم المتحدة بخصوص التطورات في مجال المعلومات والاتصالات حيث دعت الدول الأعضاء بضرورة إبلاغ الأمين العام للأمم المتحدة بأدائها وتقييماتها بشأن ما يلي: [1]

- ✓ التقييم العام لمسائل أمن المعلومات.
- ✓ تحديد المفاهيم الأساسية المتعلقة بأمن المعلومات.

[1]- أسامة العبيدي، المرجع السابق، ص ص 137-138.

✓ مضمون المفاهيم الدولية ذات العلاقة الهادفة إلى تعزيز وتدعيم أمن النظم العالمية للمعلومات والاتصالات، كما دعت الجمعية العامة إلى تعزيز دراسة الأخطار القائمة والمتحملة لأمن المعلومات والتدابير التعاونية التي يمكن للدول اتخاذها للتصدي لهذه الأخطار.

وسنخص بالدراسة في هذا الفرع القواعد الإجرائية الموصى بها من طرف مؤتمر هيئة الأمم المتحدة المنعقد في هافانا سنة 1990 وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات.

أولا: القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء المنعقد في هافانا عام 1990.

أقر مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء الذي أقر في عام 1990 إطارا دوليا في مكافحة جرائم الحاسب الآلي، كما أكد على ضرورة تطوير سبل ووسائل التعاون في المسائل الجنائية، كما ربط المؤتمر بين الجريمة المنظمة وما يتصل بها من إساءة استخدام الحاسب الآلي خاصة وأن الحاسب الآلي يستخدم من قبل الجريمة المنظمة، لارتكاب جرائم مثل غسيل الأموال أو في إدارة الأصول المحصلة بطريقة غير مشروعة.[1]

وتمكن إجمال توصيات مؤتمر هافانا في المبادئ الآتية:

✓ التأكيد على وضع إطار قانوني دولي ملائم يتطلب بذل جميع الدول الأعضاء جهدا جماعيا مشتركا.

✓ الطلب من الدول الأعضاء تكثيف جهودها في مكافحة الجرائم ذات الصلة بالحاسب الآلي، ومكافحة عمليات إساءة استخدام الحاسب الآلي والتي تستدعي تطبيق جزاءات جنائية على المستوى الوطني بما في ذلك النظر إذا دعت الضرورة إلى ذلك في اتخاذ التدابير الآتية:[2]

أ- تحديث القوانين وأغراضها الجنائية كما في ذلك التدابير المتخذة لضمان تطبيق الجزاءات والقوانين المعمول بها بشأن سلطات التحقيق وقبول الأدلة في الإجراءات القضائية على نحو ملائم وإدخال تعديلات ملائمة إذ دعت الضرورة إلى ذلك، إضافة إلى وضع أحكام وإجراءات تتعلق بالتحقيق والأدلة

[1]- خالد ممدوح ابراهيم، المرجع السابق، ص 401.

[2]- محمد الأمين البشري، محسن أحمد،معايير الأمم المتحدة في مجال العدالة الجنائيين ومنع الجريمة، أكاديمية نايف للعلوم الأمنية، السعودية، 1998، ص 19 .

والتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي، وكذا مصادرة و رد الأصول المتحصل عليها بطريق غير مشروع والناتجة عن ارتكاب جرائم ذات صلة بالحاسب الآلي.

ب- تحسين تدابير الأمن والوقاية المتعلقة بالحاسب الآلي مع وجوب مراعاة حماية الخصوصية واحترام حقوق الإنسان وحرياته الأساسية.

ت- اعتماد تدابير لزيادة وعي الجماهير والعاملين في الأجهزة القضائية وأجهزة إنفاذ القانون بالمشكلة وبأهمية مكافحة الجرائم ذات الصلة بالحاسب الآلي.

ث- اعتماد تدابير مناسبة لتدريب القضاة والموظفين والأجهزة المسؤولة عن منع الجرائم الاقتصادية والجرائم ذات الصلة بأجهزة الحاسب الآلي والتحقيق فيه، ومحاكمة مرتكبيها وإصدار الأحكام المتعلقة بها.

ج- ضرورة التعاون مع المنظمات المعنية بهذا المجال في وضع قواعد للآداب في استخدام أجهزة الحاسب الآلي والدخول إلى الشبكات.

ح- اعتماد سياسات بشأن ضحايا الجرائم المتعلقة بالحاسب الآلي تتناسب مع إعلان الأمم المتحدة بشأن مبادئ العدل المتعلقة بضحايا الإجرام والتعسف في استعمال السلطة وتتضمن إعادة الممتلكات التي يتم الحصول عليها بطرق غير مشروعة وتدابير لتشجيع الضحايا على إبلاغ السلطات المتخصصة بهذه الجرائم.

ثانيا: توصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات.

تم عقد المؤتمر الخامس للجمعية الدولية لقانون العقوبات في ريو دي جانيرو في البرازيل عام 1994 بشأن جرائم الحاسب الآلي وقد أوصى المؤتمر المذكور بأن تتضمن قائمة الحد الأدنى للأفعال المتعين تجريمها واعتبارها من قبيل جرائم الحاسب الآلي، وسوف تستعرض فيما يلي القواعد الموضوعية والإجرامية لهذه القائمة.

أ- **القواعد الموضوعية:**

تضمنت القواعد الموضوعية النص على قائمة الحد الأدنى للأفعال المتعين تجريمها واعتبارها من قبيل جرائم الحاسب الآلي وهي تلك المتضمنة فيما يلي:[1]

1- جريمة الاغتيال أو الغش بالحاسب الآلي

[1]- أسامة العبيدي، المرجع السابق، ص 140.

ويشمل ذلك الإدخال والإتلاف والمحو لمعطيات الحاسب الآلي أو برمجة أو القيام بأية أفعال تؤثر بمجرى المعالجة الآلية للبيانات وتؤدي إلى إلحاق خسارة أو فقدان الحيازة أو ضياع ملكية شخص وذلك بقصد جني الجاني منافع مادية له أو للغير.

2- جريمة التزوير التي تطال برامج الحاسب الآلي:

ويشمل ذلك إدخال وإتلاف أو محو أو تحوير المعطيات أو البرامج أو أية أفعال تؤثر على المجرى الطبيعي لمعالجة البيانات ترتكب باستخدام الحاسب الآلي وتعد فيما لو تم ارتكابها بغير هذه الطرق من قبيل أفعال التزوير المنصوص عليها في القوانين الوطنية.

3- جريمة الإتلاف:

ويشمل المحو والإتلاف والتعطيل والتخريب لمعطيات الحاسب الآلي وبرامجه.

4- جريمة تخريب وإتلاف الحاسب الآلي:

وتشمل الإدخال أو المحو أو الإتلاف أو التخريب أو فعل آخر بقصد تعطيل وظيفة من وظائف الحاسب الآلي أو نظم الاتصالات (الشبكات).

5- جريمة الدخول غير المشروع:

وهو التوصل أو الوصول دون تصريح إلى نظام أو مجموعة نظم عن طريق انتهاك إجراءات الحماية.

6- جريمة الاعتراض غير المشروع:

وهو الاعتراض عن طريق وسائل فنية للاتصال توجد لنظام حاسب آلي أو نظم أو شبكة اتصالات.

ب- القواعد الإجرائية:

وضع هذا القرار الأسس الواجب إتباعها في مكافحة الجرائم الالكترونية والمتمثلة في:

1-وجوب تحديد السلطات القائمة بإجراء التفتيش والضبط في بيئة تقنية المعلومات، وخاصة ضبط الأشياء غير المحسوسة وتفتيش شبكات الحاسب الآلي.

2-وجوب وجود قدر كبير من التعاون الفعال من قبل المجني عليهم والشهود وغيرهم من مستخدمي تقنية المعلومات، لكي تكون المعلومات متاحة في صورة تمكن استخدامها للأغراض القضائية بالنسبة لهذه الجرائم.

3-السماح للسلطات العامة باعتراض الاتصالات داخل نظام الحاسب الآلي ذاته، أو بينه وبين نظم الحاسبات الآلية الأخرى، مع استخدام الأدلة التي يتم الحصول عليها في الإجراءات أمام المحاكم.

4-يجب أن يوضع في الاعتبار كل المسائل المرتبطة ببيئة تقنية المعلومات، مثل ضياع الفرص الاستثمارية، التجسس، انتهاك حرمة الحياة الخاصة، مخاطر الخسائر الاقتصادية، كلفة إعادة بناء قواعد البيانات كما كانت من قبل وإرجاعها إلى الوضع السابق قبل إجراء أي تفتيش أو تحقيق.

5-احترام القواعد القائمة في مجال الإثبات الالكتروني ومصداقية الأدلة، والمشاكل التي يمكن أن تثيرها عند تطبيقها.[1]

الفرع الثاني: الاتفاقيات والمعاهدات الدولية في مجال مكافحة جريمة التزوير الالكتروني.

تعد المعاهدات والاتفاقيات الدولية من أهم صور التعاون الدولي بشكل عام وفي مكافحة الجرائم الالكترونية بشكل خاص، وهذا بهدف التقريب بين القوانين الجنائية والوطنية، والذي يظهر معالمه في قبول حالات تفويض الاختصاص في القيام بإجراءات التحقيق وجمع الأدلة وتسليم المجرمين والاعتراف بالأحكام القضائية الأجنبية.

وتشمل هذه الاتفاقيات جملة من القواعد الإجرائية الموصى بها بمكافحة الجرائم المعلوماتية وهذا من خلال توصيات المجلس الأوروبي واتفاقية بوداسبت إضافة إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ومؤتمر الفضاء الالكتروني والتي سنوضحها فيما يلي:

أولا: توصيات المجلس الأوروبي :

نظرا للتطور الهائل في مجال تقنية المعلومات قررت الدول الأوروبية كما سبق بيانه إعادة النظر في الإجراءات فأصر المجلس الأوروبي على ضرورة مراجعة وتعديل قوانينها الجنائية الوطنية حتى تلائم التطور الحاصل في هذا المجال [2]. ومن أهم توصيات المجلس الأوروبي ما يلي:[3]

---

[1]- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت الجرائم الالكترونية، دون طبعة، منشورات الحلبي الحقوقية، لبنان، 2007، ص 112.

[2]- تم تأسيس المجلس الأوروبي في 1949 ويتألف من 46 دولة يهدف إلى مكافحة جرائم الحاسب الآلي الانترنت وهذا بإقراره العديد من التوصيات المتعلقة بحماية البيانات، للمزيد أنظر: هلالي عبد الله أحمد، اتفاقية بوداسبت لمكافحة الجرائم المعلوماتية، المرجع السابق، ص 298 وما بعدها.

[3]- سليمان أحمد فاضل، المرجع السابق، ص 427 وما بعدها.

أ- وجوب توضيح القوانين في دول المجلس لإجراءات تفتيش أجهزة الحاسب الآلي وضبط المعلومات أثناء انتقالها.

ب- ضرورة أن تسمح الإجراءات الجنائية في دول المجلس لجهات التحقيق بتفتيش وضبط برامج الحاسب الآلي والمعلومات والبيانات المخزنة في أجهزة الحاسب الآلي وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية، كما يتعين إبلاغ الشخص القائم على الأجهزة بأن النظام كان محلا للتفتيش مع بيان المعلومات والبيانات التي تم ضبطها.

ج- السماح للجهات القائمة بالتفتيش باحترام الضمانات المقررة بمد التفتيش إلى أنظمة الحاسب الآلي في دائرة اختصاصهم.

د- تطبيق إجراءات المراقبة والتسجيل في مرحلة التحقيق الجنائي في حالة الضرورة مع مراعاة السرية واحترام المعلومات والبيانات التي يعطيها القانون حماية خاصة وإلزام العاملين بالمؤسسات العامة والخاصة بالتعاون مع سلطات التحقيق لإجراء المراقبة والتسجيل.

هـ- تطوير وتوحيد أنظمة التعامل مع الأدلة الالكترونية حتى يتم الاعتراف بها في الدول المختلفة، وكذا تطبيق النصوص الإجرائية الخاصة بالأدلة التقليدية على الأدلة الالكترونية.

و- تشكيل وحدات خاصة لمكافحة جرائم الحاسب الآلي، وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تقنية المعلومات[1].

ثانيا: اتفاقية بوداسبت لمكافحة الجرائم المعلوماتية لعام 2001.

تعد اتفاقية بوداسبت لمكافحة الجرائم المعلوماتية لعام 2001 أول اتفاقية دولية شاملة تتعلق بجرائم الحاسب الآلي والجرائم المرتكبة على شبكة الانترنت وأجهزة تقنية المعلومات الأخرى، وتسعى هذه الاتفاقية إلى التعاون والتضامن الدولي في محاربة الجرائم المعلوماتية ومحاولة الحد منها، وإتباع سياسة جنائية موحدة ترمي للحد من مخاطر هذه الجرائم والاتفاق على ملاحقة مرتكبيها [2].

كما تسعى هذه الاتفاقية إلى تحقيق وحدة التدابير الشرعية بين الدول الأوروبية والدول المنضمة للاتفاقية من غير الدول الأوروبية، ويعد التوقيع على هذه الاتفاقية الخطوة الأولى في طريق تكوين

[1]- للمزيد أنظر: أسامة العبدلي، المرجع السابق، ص 141 وما بعدها.

[2]- نعيم مغبغب، مخاطر المعلوماتية والانترنت ،دون طبعةمنشورات الحلبي الحقوقية،لبنان ،2002 ، ص 221.

تضامن دولي مناهض لجرائم الحاسب الآلي والانترنت، وقد وقعت على هذه الاتفاقية 62 دولة أوروبية إضافة إلى كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية[1].

وجاءت هذه الاتفاقية حصيلة جهود في حقل جرائم الحاسب الآلي من قبل الأمم المتحدة ومنظمة التعاون الاقتصادي والاتحاد الأوروبي ومجموعة الدول الصناعية (مجموعة الثمانية G8).

وتتضمن هذه الاتفاقية 48 مادة موزعة على أربعة فصول ،تضمن الفصل الأول تعريفات خاصة ببعض المصطلحات الفنية، وجاء الفصل الثاني تعريفات لابد من اتخاذها على المستوى الوطني، جاء بالقسم الأول الجوانب الجنائية الموضوعية بشأن الجرائم ضد الخصوصية وسلامة وتواجد معلومات الحاسب ونظم الحاسب ويشمل وصفا لأنواع متعددة من الجرائم الأصلية بالحاسب الآلي شاملة استخدام الحاسب الآلي في التزوير وفي ارتكاب الأفعال الاحتيالية والجرائم المتعلقة بالمحتوى، إضافة إلى الجرائم المتصلة بالتعدي على الملكية الفكرية والحقوق المجاورة.[2]

أما القسم الثاني فتضمن الجوانب الإجرائية لجرائم المعلوماتية وتشمل التحفظ العاجل على البيانات المعلوماتية المخزنة والأمر بإنتاج بيانات معلوماتية وتفتيش وضبط البيانات المعلوماتية المخزنة وتجميع البيانات المعلوماتية واعتراض بيانات المحتوى، وتضمن الفصل الثالث مسائل التعاون الدولي وتسليم المجرمين والمساعدة القضائية والمتبادلة والمساعدة المتبادلة في مجال سلطات التحقيق، وأخيرا جاء الفصل الرابع متضمنا الأحكام المتعلقة بالانضمام والانسحاب من الاتفاقية وفض المنازعات بين الأعضاء في الاتفاقية[3].

وعلى الرغم من أن هذه الاتفاقية هي في الأصل أوروبية إلا أنها دولية النزعة، وهي مفتوحة للدول الأخرى لطلب الانضمام إليها لتعم فائدتها الدول كافة لاسيما بعد تأكيدها على أهمية التعاون الدولي في مجال مكافحة الجرائم الالكترونية، و بدون هذا التعاون لن يكون هناك أي أثر لأي مجهود تقوم به أية دولة بمفردها، حيث أن تلك الجرائم تكون غالبا عابرة للحدود[4].

وقد نصت المادة 23 من هذه الاتفاقية على أهمية الالتزام بالتعاون، فقررت أن التعاون يجب أن يمتد نطاقه ليشمل كل الجرائم الجنائية المعلوماتية، وأن هذا التعاون يجب أن ينفذ وفقا للأصول الدولية

---

[1]– هلالي عبد الله أحمد، اتفاقية بوداسبت لمكافحة الجرائم المعلوماتية، مرجع سابق، ص 298.

[2]– هلالي عبد الله أحمد، جرائم المعلوماتية عابرة الحدود ، الطبعة الأولى، دار النهضة العربية، مصر، 2007، ص 63.

[3]– للتفصيل أكثر أنظر: هلالي عبد الله أحمد، اتفاقية بوداسبت لمكافحة الجرائم المعلوماتية، مرجع سابق، ص 298.

[4]– هلالي عبد الله أحمد، جرائم المعلوماتية عابرة الحدود، المرجع السابق، ص 63.

المتصلة بالتعاون الدولي في المواد الجنائية، والاتفاقيات المعتمدة في التشريعات المماثلة أو القانون الوطني[1].

كما أكدت هذه الاتفاقيات على ضرورة الالتزام بمعاهدات تسليم المجرمين في الجرائم المعلوماتية[2]، كما تناولت مسألة المساعدة القضائية المتبادلة سواء لأغراض التحقيق أو لأغراض جمع الأدلة الالكترونية وأكدت على أهمية هذه المساعدة وأنه يجب على كل طرف أن يعين هيئة مركزية أو هيئات تكون مسؤولة عن إرسال أو الرد على طلبات المساعدة المتبادلة أو تنفيذ هذه الطلبات وإرسالها إلى السلطات المختصة[3].

كما أكدت هذه الاتفاقية على أنه يمكن لأي طرف أن يطلب من طرف آخر أن يأمر أو يفرض بطريقة أخرى التحفظ العاجل على البيانات المخزنة بواسطة نظام معلوماتي يوجد داخل أراضي ذلك الطرف، والتي بخصوصها ينوي الطرف الملتمس أن يرسل طلبا للمساعدة المتبادلة من اجل تفتيش هذه البيانات أو الوصول إليها، أو ضبطها أو الحصول عليها أو إنشاء سريتها[4].

وحرصت هذه الاتفاقية على أهمية التكامل والتعاون الشامل وتطبيق التشريعات الدولية فيما يتعلق بمجالات التحقيق في الجرائم الالكترونية ،كسرقة البيانات والمعلومات واعتراضها وإتلافها، كما أكدت على أهمية تبادل المعلومات بين الدول الأطراف موجبة ضرورة التزام الدول الأطراف بأحكام هذه الاتفاقية ضرورة أن تكون قوانينها الداخلية متماشية معها[5].

ثالثا: مؤتمر الفضاء الالكتروني لعام 2011.

تم عقد المؤتمر الدولي للفضاء الالكتروني في لندن عام 2011 بمشاركة حكومات ومنظمات دولية غير حكومية وشركات عالمية، وشاركت أكثر من 60 دولة في هذا المؤتمر منها الولايات المتحدة

---

[1]– أسامة العبيدي، المرجع السابق، ص 146.

[2]– تنص المادة 25 من اتفاقية بوداسبت على انه "يجب على كل الأطراف أو تو توفر لبعضها البعض مساعدة قضائية متبادلة إلى أقصى مدى ممكن لأغراض التحقيقات الإجراءات بالنسبة للجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو بغرض جمع الأدلة الالكترونية للجريمة الجنائية .

[3]– المادة 27 من اتفاقية بوداسبت لمكافحة الجرائم المعلوماتية .

[4]– المادة 29 اتفاقية بوداسبت لمكافحة الجرائم المعلوماتية.

[5]– للمزيد أنظر: هلالي عبد الله أحمد، اتفاقية بوداسبت لمكافحة الجرائم المعلوماتية، مرجع سابق ص 298. وما يليها.

الأمريكية ودول الاتحاد الأوروبي والصين وروسيا ودول أخرى، وذلك بهدف تطوير فهم مشترك أفضل لكيفية حماية الإمكانات والفرص الكبيرة التي يدمها الفضاء الالكتروني للجميع [1].

ويهدف هذا المؤتمر إلى محاربة الجرائم العابرة لحدود، ومساعدة الدول الأخرى على بناء قدراتها في فرض تطبيق القانون والتعاون بين الدول من أجل القضاء على التهديدات المنتشرة في الفضاء الالكتروني وذلك بابتكار أساليب جديدة، إذا لم تعد الأساليب القديمة كافية لمواجهة الإجرام، وتحديد الإجراءات الفعالة وبناء الثقة في مجال الفضاء الالكتروني.

وقد أجمعت الدول المشاركة في هذا المؤتمر على أن الانترنت أداة رئيسية وحيوية في النمو الاقتصادي لاسيما الدول النامية، وعلى القواعد الايجابية الجمة للانترنت في تحسين حياة المواطنين، وقدرتها على كشف انتهاكات حقوق الإنسان عند حدوثها، واتفق على ضرورة ألا تكون جهود تحسين أمن الانترنت على حساب حقوق الإنسان، حيث أبدى المشاركون تأييدا قويا لمبدأ وجوب أن يبدي مستخدمو الانترنت تسامحا واحتراما لتنوع اللغات والأفكار والثقافات، مع التشديد على ضرورة ألا تكون حماية المبدأ ذريعة لمحاولات الإخلال بحق حرية التعبير عن الرأي [2].

وأشار مؤتمر الفضاء الالكتروني أن جرائم المعلوماتية تمثل تهديدا كبيرا للدفاع الاقتصادي والاجتماعي، كما أنها تتطلب بذل جهود دولية عاجلة ومتكاثفة لمواجهة هذه التهديدات، وضمان عدم وجود ملاذ آمن لمجرمي الانترنت، كما حث المشاركون الدول على النظر في إمكانية الانضمام لاتفاقية بوداسبت لمكافحة الجرائم المعلوماتية كونها أفضل شكل من أشكال الاتفاق الدولي في هذا المجال.[3]

رابعا: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

في إطار تعزيز التعاون بين الدول العربية لمكافحة جرائم تقنية المعلومات واقتناعا منها بضرورة الحاجة إلى تبني سياسة جنائية لمكافحة جرائم مشتركة تهدف إلى حماية المجتمع من هذا النوع من الجرائم أبرمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لجمهورية مصر العربية بتاريخ 2010/10/21 والتي دخلت حيز النفاذ في 2014/02/06.

وقد تبنت الاتفاقية جملة من القواعد الإجرائية التي تهدف إلى التعاون القانوني القضائي لملاحقة المجرمين ضمانا لعدم إفلاتهم من العقاب، ومنها ما جاءت به المادة 22 من الفصل الثالث بأن تلتزم كل

[1]– أسامة العبيدي، المرجع السابق، ص 147.

[2]– هلالي عبد الله أحمد، اتفاقية بوداسبت لمكافحة الجرائم المعلوماتية، مرجع سابق، ص 160.

[3]– أسامة العبيدي، المرجع السابق، ص 149.

دولة طرف بأن تتبنى في قانونها الداخلي التشريعات والإجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة في هذا الفصل وتطبيق هذه الإجراءات على الجرائم المنصوص عليها في هذه الاتفاقية بما فيها جريمة التزوير الالكتروني وأكدت الاتفاقية على التعاون القانوني والقضائي بين الدول، لاسيما فيما يتعلق بقواعد تسليم المجرمين والمساعدة المتبادلة بين الدول الأطراف سواء أثناء مرحلة التحقيق أو جمع الأدلة الالكترونية وكذا طلبات الحفظ العاجل للمعلومات المخزنة على أنظمة المعلومات كما أوصت الاتفاقية على أن تكفل كل دولة طرف وفقا لنظامها القانوني وجود جهاز متخصص لضمان المساعدة الفورية سواء في مرحلة التحقيق أو في مرحلة جمع الدليل الالكتروني[1].

المطلب الثالث: الجهود الدولية لمكافحة جريمة التزوير الالكتروني في إطار التعاون القضائي.

نظرا لما تحقق من تقدم تقني وتشابك في العلاقات الدولية، وسهولة المواصلات ويسر الاتصالات أصبح الإجرام دوليا، ما يستوجب تدويل إجراءات الملاحقة القضائية من أجل مكافحة الأنشطة الإجرامية عندما تتجاوز النطاق الوطني ولا سبيل لمواجهة هذه الظواهر الإجرامية إلا من خلال سياسة جنائية تتسم بالطابع الدولي.

ففعالية مكافحة الجريمة تستوجب تضامن الدول وتعاونها في صور عديدة تنصب في مجملها حول تبادل المعلومات الأمنية والقضائية، وهذا من خلال المساعدة القضائية الدولية أو تسليم الجانحين الهاربين والنيابة القضائية، وغير ذلك من صور التعاون القضائي.

ويعد التعاون القضائي الدولي في المجال الجنائي هو إجراء قضائي تقوم به الدولة من شأنه تسهيل مهمة المحاكمة في دول أخرى بصدد جريمة من الجرائم [2] أي هو البحث عن الوسائل التي تمكن دولة ما من الاستفادة من السلطات العامة أو الهيئات القضائية لدولة أخرى، والذي يهدف إلى مكافحة الجريمة. [3]

وتعرض فيما يلي صور التعاون القضائي في المجال الجنائي في ظل ما أفردته الممارسة العملية في هذا المجال، أين سنتطرق إلى المساعدة القضائية الدولية في الفرع الأول في حين تخصص الفرع الثاني لنظام تسليم المجرمين وهذا على النحو الآتي بيانه.

---

[1]– انظر المادة 30 وما يليها من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .

[2]– أمجد قطيفان الخريشة، جريمة غسيل الأموال، دراسة مقارنة، الطبعة الأولى، دار الثقافة ، لبنان، 2006، ص 216.

[3]– نادية دردار، المرجع السابق، ص 15.

الفرع الأول: المساعدة القضائية الدولية

تعرف المساعدة القضائية بأنها: " كل إجراء قضائي تقوم به دولة ما شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم [1]، وتتخذ المساعدة القضائية صورا عدة من بينها ما سنتناوله كالتالي:

أولا: تبادل المعلومات.

يشمل إجراء تبادل المعلومات تقديم البيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما من الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، كما يشمل تبادل السوابق القضائية للجناة ومن خلالها تتعرف الجهات القضائية الأحكام الخاصة بالعود، وعدم الأهلية ووقف تنفيذ العقوبة.[2]

وقد تم إيراد تلك الصور من صور المساعدة القضائية الدولية في المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة القضائية في المسائل الجنائية [3] كما تم إيرادها أيضا في المادة الرابعة من المعاهدة منظمة لمؤتمر الإسلامي لمكافحة الإرهاب الدولي [4] وذات الصورة نجدها أيضا في المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي [5] والمادتين الأولى والثانية من النموذج الاسترشادي لاتفاقية التعاون القانوني القضائي الصادر عن مجلس التعاون الخليجي [6].

---

[1]– غانم مرضي الشمري، المرجع السابق، ص ص98–99.

[2]– أسامة العبيدي، المرجع السابق، ص 128.

[3]– صدرت هذه المعاهدة في 1990/12/14 في الجلسة العامة (68) للجمعية العامة للأمم المتحدة وتقضي بإنفاق أطرافها أن يقدم كل طرف أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات وإجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلا في اختصاص السلطة القضائية في الدولة الطالبة للمساعدة، عن أسامة العبيدي، المرجع السابق، ص 129.

[4]– صدرت هذه الاتفاقية في عام 1999 من قبل مؤتمر وزراء خارجية دول المتضامنة في اجتماعهم المنعقد في واغادوغو.

[5]– صدرت هذه الاتفاقية في 1993/4/6 بمدينة الرياض بالمملكة العربية السعودية/ أنظر في ذلك، يوسف حسن يوسف، المرجع السابق، ص 151.

[6]– تم اعتماد هذا النموذج من المجلس الأعلى لمجلس التعاون الخليجي في دورتها الرابعة المنعقدة في دولة الكويت في الفترة ما بين 21–2003/12/22 /للمزيد انظر سليمان أحمد الفضل، المواجهة التشريعية والأمنية للجرائم الناتجة عن استخدام شبكة المعلومات الدولية،دار النهضة العربية،مصر،2012، ص 422 وما بعدها، انظر أيضا، حسين سيد الغافري، المرجع السابق، ص 642 وما بعدها.

أما بخصوص المشرع الجزائري فقد أكد القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على أنه في إطار التحقيقات والتحديات القضائية التي تمت مباشرتها وتتبع الجرائم المنصوص عليها في هذا القانون والكشف عن مرتكبيها فإن السلطات الجزائية المختصة بإمكانها تبادل المساعدات القضائية على المستوى الدولي [1].

وفي النقطة المتعلقة بجمع الأدلة الخاصة بالجريمة الالكترونية وجمع الأدلة من إجراءات التحقيق القضائي، فإن المشرع أجاز في حالة الاستعجال قبول طلبات المساعدة القضائية الدولية، وان ورد عن طريق وسائل الاتصال السريعة مثل الفاكس أو البريد الالكتروني شريطة التأكد من صحتها.[2]

ثانيا: نقل الإجراءات الجزائية.

يقصد بنقل الإجراءات الجزائية قيام دولة بناء على اتفاقية باتخاذ إجراءات جنائية بصدد جريمة ارتكب في إقليم دولة أخرى ولمصلحة هذه الدولة، وذلك في حالة توافر شروط معينة من أهمها أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات، بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها في قانون الدولة المطلوب إليها، كما يجوز للدولة المطلوب إليها أن ترفض نقل الإجراءات في الحالات الآتية:[3]

أ- إذا كان طلب نقل الإجراءات ليس له ما يبرره كأن تكون الأسباب التي ذكرتها الدولة الطالبة لا تدعو لاتخاذ مثل هذه الإجراءات.

ب- إذا ثبت أن الدافع وراء طلب نقل الإجراءات اعتبارات سياسية أو دينية عنصرية.

ج- إذا كانت الدولة المطلوب إليها قد طبقت قوانينها على الجريمة قبل استلامها من الدولة الطالبة، وكان الإجراء الذي سبق اتخاذها مطابقا للقانون.

د- إذا كانت الإجراءات التي تطلبها الدولة الطالبة مخالفة لواجبات تلتزم بها الدولة المطلوب إليها.

هـ- إذا كانت الإجراءات المطلوبة مخالفة لقوانين الدولة المطلوب إليها.

---

[1]- تنص المادة 16 من القانون 04/09 على أنه: "في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني ".

[2]- تنص الفقرة الأخيرة من المادة 16 من القانون 04/09 على أنه " إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني، وذلك بقدر ما توفره هذه الوسائل من شروط تكن كافية للتأكد من صحتها".

[3]- أحمد سليمان الفضل، المرجع السابق، ص ص 222-223.

ومن التطبيقات العملية في هذا الصدد قيام المجلس الأوروبي بإقرار اتفاقية الإجراءات الجنائية التي تعطي للأطراف المنضمة إمكانية محاكمة الجاني طبقا لقوانينها، بناء على طلب دولة أخرى طرف في هذه الاتفاقية، شريطة أن يكون معاقبا عليه في الدولتين.[1]

ثالثا: الإنابة القضائية الدولية:

يقصد بالإنابة القضائية الدولية طلب إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك في الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها. وتهدف هذه الصورة إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المهتمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة الأعمال القضائية داخل أقاليم الدول الأخرى، كسماع الشهود أو إجراء التفتيش وغيرها.[2]

ويتم إرسال طلب الإنابة القضائية عبر القنوات الدبلوماسية وهذا من شأن النيابة العامة وذلك من خلال قيام المحكمة الوطنية بتوقيف الطلب في الدولة الطالبة لتقوم هذه الأخيرة بإرساله بعد ذلك إلى السلطات القضائية المختصة في الدولة متلقية الطلب وما أن يتم تلبية الطلب ينعكس الاتجاه الوارد في سلسلة العمليات.[3]

إلا أن مرور إجراءات التعاون القضائي الدولي بالطرق الدبلوماسية يجعلها تتسم بالبطء وكثرة التشكيلات وهو ما يتعارض مع طبيعة شبكة الانترنت التي تتميز بسرعة مرور وتبادل المعلومات، لذلك فان مكافحة الجرائم الالكترونية تتطلب تعاملا سريعا تجنبا لاحتمالية التلاعب في البيانات التي قد تشكل دليلا ضد المتهم.[4]

وسعيا وراء الحد من الروتين والتعقيد والبطء الذي تتميز به الإجراءات الدبلوماسية يحدث وبدرجة متزايدة أن تشترط المعاهدات والاتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن تعين سلطة مركزية عادة ما تكون وزارة العدل ترسل إليها الطلبات مباشرة بدلا من الولوج إلى القنوات الدبلوماسية والتي من شأنها تسريع الإجراءات التي قد تأخذ وقتا طويلا فيما تم عبر تلك القنوات [5].

---

[1]– جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، المرجع السابق، ص 80.

[2]– سليمان أحمد فضل، المرجع السابق، ص 425.

[3]– يوسف حسن يوسف، المرجع السابق، ص 152.

[4]– أسامة العبيدي، المرجع السابق، ص 131.

[5]– يوسف حسن يوسف، المرجع السابق، ص 152.

ومن بين الاتفاقيات التي أبرمت في مجال الإنابة القضائية تلك التي عقدتها فرنسا مع ألمانيا في أكتوبر 1977، ومع الجزائر في 28 أغسطس 1963 ،ومع مصر في 15 مارس 1982، والاتفاقية الأوروبية للتعاون القضائي في المواد الجنائية سنة 1962 [1] وتتضمن الاتفاقيات شروط وأساليب تنفيذ الإنابة القضائية، وغالبا ما تتضمن شرط باستبعاد تنفيذ الأحكام في المجال السياسي والضريبي والعسكري، أو إذا قدرت الدولة المطلوب منها أن التنفيذ المطلوب من شأنه المساس بسيادة الدولة، أو النظام العام أو المصالح الأساسية الأمر الذي يترك للدولة سلطة تقديرية لتنفيذ أو عدم تنفيذ ما يطلب إليها وذلك خشية قيام مسؤوليتها دوليا عن إهمالها، بالمقابل فإنه في ظل عدم وجود اتفاقية فإن الإنابة القضائية لا يمكن تنفيذها، إلا إذا وافقت الدولة المطلوب إليها على ذلك، وفقا للإجراءات والشروط المنصوص عليها في القانون الداخلي لها.[2]

ويثار في هذا الصدد التساؤل الآتي: **هل هذه الاتفاقيات الدولية بوضعها الحالي يمكن أن تساهم في الحد ومكافحة الجرائم الالكترونية ؟.**

نظرا لأن عامل السرعة يعتبر من العوامل الرئيسية في مكافحة الجرائم الالكترونية كما سبق بيان فإن العديد من الاتفاقيات الجديدة ساهمت في تقصير الوقت واختصار الإجراءات عن طريق الاتصال المباشر بين السلطات المعينة بالتحقيق، ومثال ذلك الاتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفويا في حالة الاستعجال، ونفس الشيء نجده في البند الثاني من المادة 30 من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999 والمادة 53 من اتفاقية شنغن عام 1990 والخاصة باستخدام الاتصالات المباشرة بين السلطات القضائية في الدول الأطراف، وكذا الفقرة 13 من المادة 46 من اتفاقية الأمم المتحدة لمكافحة الفساد [3].

إلا أن هذه الاتفاقيات تنظم مسألة التعاون الدولي أو تبادل المساعدات الفضائية بخصوص الجرائم التقليدية، إلا أنه من الصعب تطبيق الآليات التقليدية في مجال التحقيق الجنائية في مجال التحقيق الجنائي في الجرائم الالكترونية وذلك لأمرين:

الأمر الأول: أن تلك الآليات غير مؤهلة من الناحية العملية لأن تطبيق على التحقيقات الجنائية للجرائم المرتكبة عبر الانترنت، وهو ما أكدته لجنة الخبراء المكلفة بتقييم الوصية رقم 10-85 من اتفاقية التعاون

[1]- سليمان أحمد فضل، المرجع السابق، ص 425.

[2]- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، مرجع سابق، ص 85.

[3]- يوسف أحمد يوسف، الجرائم الدولية للانترنت ،المصدر القومي للإصدارات القانونية،مصر 2011، ص 153.

القضائي للمجلس الأوروبي لسنة 1959 فيما يتعلق بإمكانية تطبيق تلك الوصية على تفتيش الشبكات المعلوماتية والتنصت على الاتصالات، إذ انتهت اللجنة إلى أن هذه التوصية لا تصلح للتطبيق على التنصت الذي يتم في إطار الشبكة المعلوماتية.[1]

كما أدرك المجلس الأوروبي عام 1993 عجز تلك الآليات التقليدية أمام المشاكل التي تمكن أن تثيرها التكنولوجيا الحديثة في مجال الإجراءات الجنائية والذي أكد بوضوح قصور على مستوى التعاون الدولي بالنسبة لإجراء التفتيش عبر الحدود.[2]

الأمر الثاني: تتطلب مكافحة الجريمة الالكترونية السرعة والدقة في مباشرة إجراءاتها وهو ما لا يتم بتحقيق إذا ما تم إتباع الطرق التقليدية المتسمة بالبطء وكثرة التشكيليات كما سبق ذكره.

أمم تلك الأسباب فإن تعيين إعادة النظر في إطار التعاون القضائي الدولي لاسيما في مجال التحقيق الجنائي من أجل صياغة تشكل جديد لهذا التعاون يتماشى والطبيعة الخاصة للجريمة الالكترونية والتي تتطلب إقامة نوع من التماثل بين التشريعات العقابية والإجراءات بين الدول ولا يتأنى ذلك إلا من خلال صياغة اتفاقيات دولية جديدة بشأن التعاون الدولي في مجال مكافحة الجريمة الالكترونية كالاتفاقية الأمريكية الكندية السابق ذكرها ،والاتفاقية الأوروبية بوادسبت 2001 التي وضعت العديد من القواعد المنظمة للتعاون القضائي الدولي بين الدول الأعضاء في مجال مكافحة الإجرام المعلوماتي والتي جاء في طياتها وضع تشريعات جنائية موحدة لأقصى درجة ممكنة بغرض إجراء التحقيقات التي تتعلق بجرائم ونظم بيانات الكمبيوتر، أو من أجل تجميع أدلة الجريمة في شكلها الإلكتروني الجديد.[3]

كما تحيز الاتفاقية في الظروف العاجلة أن تطالب الدول الأطراف من بعضها تبادل المساعدة القضائية في مجال التحقيقات الجنائية باستعمال وسائل الاتصال العاجلة كالفاكس أو البريد الالكتروني شريطة توفير وسائل الأمن وضمان سلامة المعلومات المتبادلة بين الطرفين [4].

أما المشرع الجزائري وفي إطار العلاقات مع الدول الأجنبية نص على تنفيذ الإنابة القضائية إذا كان لها محل في القانون الجزائري وهذا وفقا للمادة 721 من قانون الإجراءات الجزائية [1] ويتم طلبها

[1]– محمد كمال عبد السميع شاهين، المرجع السابق، 146.

[2]– جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، مرجع سابق، ص 82.

[3]– شيماء عبد الغني عطا الله، المرجع السابق، ص 207.

[4]– محمد كمال عبد السميع شاهين، المرجع السابق، ص 147.

بالطريق الدبلوماسي الذي يرسل إلى وزارة العدل إلا أنه لا يوجد أي نص سواء في قانون الإجراءات الجزائية أو في القانون 04/09 المتضمن القواعد المتعلقة بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها يبين من خلالها تعيين السلطة المركزية والرد على الطلبات وكذا إرسالها وتنفيذها.

الفرع الثاني: نظام تسليم المجرمين.

قد يرتكب الجاني جريمة في دولة معينة أو عدة جرائم في عدة دول ويلجأ إلى دولة أخرى هربا من المحاكمة أو تنفيذ العقوبة وبالتالي فإن نشاطه الإجرامي يتصل بأكثر من دولة مما يؤدي إلى ضرورة تسليمهم من الدولة التي لجأ إليها التي ارتكب جريمته على أرضها، بناء على طلب هذه الأخيرة ويهدف التسليم إلى الحيلولة دون إفلات المجرم من العقاب، في الحالة التي يكون فيها القانون الداخلي للدولة المتواجد على إقليمها المتهم لا يسمح لها بمحاكمته على جريمته وهو ما يعرف بمبدأ الحق في العقاب [2]حتى لا تصبح كل دولة عرضة لأن تكون ملجأ الهاربين إليها من دول أخرى.

وقد حرصت أغلب دول المجتمع الدولي عن سن التشريعات الخاصة بتسليم المجرمين بالإضافة إلى عقد العديد من الاتفاقيات الإقليمية والدولية التي تعني بعملية التسليم استنادا إلى فكرة التعاون الدولي لمكافحة الإجرام وتحقيق العدالة.

وفي إطار حديثنا عن هذا الموضوع سوف نبينه في تفصيل أكثر في العناصر الآتية:

أولا: مفهوم تسليم المجرمين:

يعتبر تسليم المجرمين شكلا من أشكال التعاون بين الدول في مكافحة الجريمة الالكترونية وحماية المجتمعات من أثرها الخطير، والتعاون الدولي في هذا المجال هو نتيجة طبيعية للتطورات التي حدثت في كافة المجالات، فلم تعد الحدود القائمة بين الدول التي تشكل عائقا أمام مرتكبي هذه الجرائم ولم يعد نشاطهم الإجرامي قاصر على اقليم دولة واحدة بل يمتد أثره ليشمل عدة دول.

---

[1]– تنص المادة 721 من قانون الإجراءات الجزائية الجزائري على أنه :في حالة المتابعات الجزائية غير السياسية في بلد أجنبي تسلم الإنابات القضائية الصادرة من السلطة الأجنبية بالطريق الدبلوماسي وترسل إلى وزارة العدل بالأوضاع المنصوص عليها في المادة 703 وتنفذ الإنابات القضائية إذا كان لها محل وفقا للقانون الجزائري وكل ذلك بشرط المعاملة بالمثل.".

[2]– حسين المحمدي، الإرهاب الدولي تجريما ومكافحة، الطبعة الأولى، دار المطبوعات الجامعية، مصر 2007، ص 143.

ويعد مصطلح تسليم المجرمين بعد الترجمة العربية لكلمة Extradition الفرنسية والتي استعملت لأول مرة في مرسوم 19 فيفري 1791 في فرنسا، ولكلمة Extradition الإنجليزية التي اشتقت من الفرنسية واستعملت لأول مرة في بريطانيا في قانون التسليم لسنة 1870.[1]

عند التدقيق في تسمية هذا النظام بـ"تسليم المجرمين" نجد أن هذه التسمية غير دقيقة ويعود ذلك إلى أن التسليم هو عمل تقوم به الدولة المراد منها التسليم ،أما عمل الدولة الطالبة للتسليم هو الاسترداد أو الاستلام، وبالتالي تم حصر تسمية التسليم على الدولة المطلوب منها التسليم فقط دون الدولة الطالبة.

عند التدقيق في كلمة "المجرمين" نلاحظ أنها تسمية غير دقيقة، حيث أن وصف الشخص محل التسليم بالمجرم، يفيد أنه قد تمت محاكمته وإدانته سلفا بحكم قضائي مع أن التسليم قد ينصب أيضا على شخص لم تتم محاكمته بعد ومازال في طور الاتهام [2].

وبالرغم من هذه الانتقادات الموجهة إلى تسمية هذا النظام بـ "تسليم المجرمين" والتي تعتبر غير دقيقة للتعبير عن النظام المرجو منها، إلا أننا نلاحظ أنها الأكثر شيوعا بالمقارنة مع تسمية "تسليم الأشخاص" أو استلام واسترداد الأشخاص، ولم يتفق أغلب الفقهاء على وضع تعريف واحد لتسليم المجرمين، ويعود ذلك لأسباب أهمها الاختلاف حول طبيعة التسليم، ومدى تسليم الرعايا من عدمه ولكن هذا الاختلاف يكون في التفصيلات فقط.

ويعرف تسليم المجرمين بأنه تخلي دولة عن شخص موجود على إقليمها إلى دولة أخرى بناء على طلبها، لتحاكمه عن جريمة يعاقب عليها قانونها، أو لتنفيذ فيه حكما صادرا عليه من إحدى محاكمتها[3].

وهناك تعريفات أخرى توسع من مفهوم "تسليم المجرمين" كالتعريف الذي خلصت إليه المحكمة العليا الأمريكية من أن التسليم هو الإجراء القانوني المؤسس على معاهدة أو معاملة بالمثل، أو قانون وطني تسلم بمقتضاه دولة ما من دولة أخرى شخص متهم أو مرتكب مخالفة جنائية ضد القوانين الخاصة بالدولة الطالبة، أو مخالفة القانون الجنائي الدولي، حيث يعاقب على ذلك في الدولة الطالبة.

من التعاريف السابقة يمكن التوصل إلى أن تسليم المجرمين هو أحد مظاهر التعاون الدولي لمكافحة الجريمة، وهو عبارة عن إجراء قانوني مؤسس على معاهدة أو معاملة بالمثل أو قانون وطني

---

[1]– نادية دردار، المرجع السابق، ص 18.

[2]– سليمان عبد المنعم، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين، دراسة مقارنة، دار الجامعة الجديدة للنشر، مصر، 2007، ص 7.

[3]– مفيد نايف الدليمي، غسيل الأموال في القانون الجزائي، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2006، ص 184.

توافق بموجبه دولة تسمى الدولة المطلوب إليها على أن تسلم إلى دولة أخرى تسمى الدولة الطلبة شخصا يتواجد على إقليمها، حتى يتيح للدولة الطالبة أن تحاكم الشخص المطلوب تسليمه، أو تنفذ عليه العقوبة إذا كانت قد تمت محاكمته من قبل.

ثانيا: شروط وإجراءات تسليم المجرمين

هناك شروط لتسليم المجرمين لابد من وجودها وإجراءات لا يتم التسليم بدونها وذلك ما سنبينه فيما يلي:

أ- شروط التسليم:

أهمية شروط التسليم تكمن في كونها تفصل حدود العلاقة بين الدول الأطراف في عملية التسليم وتضع الأحكام العامة التي على أساسها سيتم التسليم من عدمه وذلك متى توافرت هذه الشروط حال البث في قرار التسليم، وتكاد تتفق هذه الشروط في جميع حالات التسليم من حيث العناصر، أما من حيث الموضوع فهي محل خلاف بين الدول وذلك بحسب حاجتها للتسليم، واعتبارات المصالح الدولية التي تراعيها كل دولة وهي كالتالي:

1/ التجريم المزدوج:

ويقصد به أن يكون الفعل المطلوب التسليم من أجله مجرما في تشريع الدولة طالبة التسليم وكذلك في تشريع الدولة المطلوب إليها التسليم والمطلوب هنا أن يكون الفعل مجرما أيا كانت الصورة التشريعية المعاقب عليها، فلا عبرة للوصف أو التكييف القانوني الذي يطلق على الفعل عند تقرير توافر هذه الشروط والمعاقبة عليه، فقد تختلف تشريعات الدول في التكيف القانوني الذي توصف فيه الجريمة.[1]

وشرط التجريم المزدوج يجد أساسه في أن الدولة الطالبة التسليم تبتغي من وراء طلبها محاكمة من نسب إليه ارتكاب السلوك الإجرامي أو تنفيذ العقوبة المحكوم بها عليه وهذا يفترض بداهة أن السلوك مجرم في تشريعها، حيث أنه إذا لم يكن مجرما فلا يتصور وجود دعوى عمومية أو ملاحقة جزائية ضد المتهم كما لا يتصور قيام حكم جزائي يقضي بعقوبة عليه هذا من ناحية، ومن ناحية أخرى لا يجوز مطالبة الدولة المطلوب إليها التسليم بإيقاع عقوبة على ارتكاب سلوك ما هو في الأساس غير مجرم وفقا لقانونها.[2]

[1]- حسين بن سعيد بن سيف الغافري، المرجع السابق، ص 523.

[2]- غانم مرضي الشمري، مرجع سابق، ص ص 106،107.

2/ الشروط المتعلقة بالأشخاص المطلوب تسليمهم:

من المبادئ السائدة والمستقر عليها في المجتمع الدولي والتي نصت عليها معظم التشريعات الوطنية والاتفاقيات مبدأ جواز تسليم الرعايا أيا كان نوع الجريمة المرتكبة من قبلهم في أي إقليم خارج دولتهم.

كما لا يجوز تسليم من تم منحهم حق اللجوء السياسي، وهذا أيضا مبدأ سائر في أغلب التشريعات والاتفاقيات الدولية والإقليمية المتعلقة بتسليم المجرمين.

ويضاف إلى ذلك شرط آخر يتمثل في عدم جواز تسليم من تمت محاكمته عن تلك الجريمة المطلوب تسليمهم لأجلها، وذلك متى كان الشخص المطلوب تسليمه وقد ثبت محاكمته عن الجريمة المطلوب تسليمه لأجلها فظهرت براءته أو عوقب عنها، فإنه لا يجوز تسليمه ولا يجوز أيضا التسليم إذا كان الواقع أو الجريمة قيد التحقيق وذلك حتى لا يتعرض الشخص المطلوب تسلمه العقوبة مزدوجة.[1]

3/ الشروط المتعلقة بالجريمة المطلوب التسليم لأجلها:

إن تحديد طبيعة الجرائم التي تخضع لنطاق التسليم يعتبر في غاية الأهمية كونه يحدد دعما إذا كان يجوز التسليم أولا، فطبيعة تلك الجرائم هي الدعائم التي تقوم عليها شروط التسليم بصفة أساسية، وتتبع الدول في تحييد الجرائم التي يجوز التسليم فيها ثلاثة اتجاهات هي:

الاتجاه الأول: وهو ما يسمى بأسلوب الحصر أو نهج القائمة، ويعتمد هذا الأسلوب على إدراج مجموعة من الجرائم على سبيل الحصر في قائمة تضمن القانون أو تلحق بالاتفاقية لتكون هذه الجرائم دون غيرها هي التي يتم التسليم لأجلها، ويعتبر هذا الأسلوب الأقل شيوعا وانتشارا بين الدول حيث يؤدي إلى إفلات بعض المجرمين من العقاب متى كانت الجريمة المرتكبة غير واردة في القائمة. [2]

الاتجاه الثاني: ويتمثل في ما يسمى بأسلوب جسامة الجريمة أو الحد الأدنى للعقوبة وهذا الأسلوب هو الأكثر شيوعا في تحديد الجرائم التي يجوز التسليم فيها وهو يعني أن تحدد الدول في تشريعاتها الداخلية أو المعاهدات الثنائية أو متعددة الأطراف إلى الحد الأدنى للعقوبة المقررة للجرائم التي يمكن أن يتم التسليم لأجلها.[3]

---

[1]– يوسف حسن يوسف، المرجع السابق، 165.

[2]– نفس المرجع ،ص 166.

[3]– غانم مرضي الشمري، المرجع السابق، ص 109.

ويشترط للتسليم أن يكون الفعل المنسوب للشخص المطلوب تسليمه بشكل جريمة كل من قانون الدولة الطالبة وفي قانون الدولة المطلوب إليها، كما يجب أن يكون الفعل على درجة معينة في الجسامة (جناية أو جنحة) وأن يكون معاقب عليه بعقوبة سالبة للحرية.[1]

الاتجاه الثالث: النظام المختلط وهو من الأساليب الشائعة أيضا في تحديد الجرائم التي يجوز التسليم فيها وهو تحقق فائدتين: فمن جهة يضمن درجة معينة من جسامة الجريمة المعاقب عليها في البلدين ليتم التسليم وفقا لها، ومن جهة أخرى يضمن خضوع جرائم محددة تمثل خطرا على الدول الأطراف التسليم دون النظر لدرجة جسامتها أو العقوبة المقررة لها.

ومما تجدر الإشارة في هذا المقام أنه يسود المجتمع الدولي اتجاه عام يقضي بعدم جواز التسليم في الجرائم السياسية، وذلك راجع إلى أن المجرم السياسي لا يعتبر مجرما بالمعنى الذي يحمله هذا الاصطلاح في علم الإجرام أو علم الاجتماع، إذ غالبا ما يرتكب السلوك يهدف أغراض وأهدافه قومية، قد تنطوي على أعمال بطولية لتحرير الأرض واستقلال الوطن والدفاع عن مبادئ سامية.[2]

وفي هذا الصدد نصت الاتفاقية العربية لمكافحة تقنية المعلومات في المادة 31 فقرة 4 وكذا المادة 24 فقرة 04 على أن كل الجرائم المنصوص عليها في الاتفاقية تكون الأطراف غير انه لا يجوز حسب الاتفاقيات الدولية التسليم في الجرائم السياسية حيث يكون الغرض منه اتخاذ إجراءات انتقامية ضد الشخص المطلوب وهو عمل لا يليق بالدولة المطلوب منها أن تساهم في تنفيذه. [3]

وقد اتبع المشرع الجزائري هذا النهج وهذا من خلال المادة 698 فقرة 4 من قانون الإجراءات الجزائية الجزائري، إذ لا يقبل التسليم إذا كانت الجريمة ذات صبغة سياسية. [4] وفي هذا المقام يثور إشكال حول بعض الجرائم الالكترونية تشكل جرائم سياسية كجريمة الدخول غير المشروع إلى قواعد وإلى قواعد البيانات الإستراتيجية العلمية أو الاقتصادية أو الدفاعية أو المالية للدولة، وبالتالي يكون هناك تعارض بين نص اتفاقية بودابست والاتفاقية العربية وما منصوص عليه في الاتفاقية الدولية، ونص قانون الإجراءات الجزائية الوطني.[5]

---

[1]– جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، المرجع السابق، ص 89.

[2]– يوسف حسن يوسف، المرجع السابق، ص 167.

[3]– جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، المرجع السابق، ص 89.

[4]– تنص المادة 698 فقرة 4 من قانون الإجراءات الجزائية على أنه: "لا يقبل التسليم في الحالات الآتية: "... إذا كانت للجناية أو الجنحة صيغة سياسية أو إذا تبين من الظروف أن التسليم مطلوب لغرض سياسي..."

[5]– الهام بن خليفة، المرجع السابق، ص 365.

في حين يرى الفقه أن رفض التسليم في حالة الجرائم السياسية يعتبر عقبة تحول دون التعاون الدولي في هذا المجال.[1]

ب-إجراءات التسليم:

يقصد بإجراءات التسليم القواعد الإجرائية التي تتبع الدول الأطراف في عملية التسليم بهدف المحافظة على حقوق الإنسان وحريته وتأمين الصالح العام، وهذه الإجراءات تتقاسمها الدولتان الطالبة والمطلوب منها التسليم، وتعتبر هذه الإجراءات مقيدة ببعض الالتزامات الدولية أو التعاهدية.

ويعد تقديم الطلب لسلطات الدولة المطلوب منها هو الخطوة الأولى لإجراء التسليم ويكون الطلب كتابيا [2] سواء نصت التشريعات الوطنية أو الاتفاقيات الدولية والإقليمية على شرط الكتابة صراحة أو ضمنا ويجب إرفاق طلب التسليم بالوثائق التي تسهل على الدولة المطلوب منها لتسليم التعرف على هوية المطلوب تسليمه وعرض موجز للوقائع المتابع من اجلها، كما يرفق بنسخة مصادق عليها للنص القانوني المطبق على تلك الوقائع ونسخة من مستندات التحقيق إن وجدت ،أما إذا كان الطلب خاصا بتنفيذ عقوبة فإن الوثائق الواجب إرفاقها هي نسخة أصلية أو مطابقة للأصل من الحاكم الذي يقضي بالعقوبة، وتشترط بعض الدول التوقيع على هذه الوثائق من الجبهات الرسمية، في حين تكتفي دول أخرى بورود هذه الوثائق عبر الطريق الدبلوماسي الذي يعد ضمانة لرسميتها.[3]

بالرجوع إلى المشرع الجزائري وتحديدا للمادة 703 من قانون الإجراءات الجزائية يتولى وزير الخارجية تحويل طلب التسليم بعد فحص المستندات ومعه الملف إلى وزير العدل الذي يتحقق من سلامة الطلب ويعطيه خط السير الذي يتطلبه القانون،و يتولى النائب العام استجواب المطلوب تسليمه (الأجنبي) للتحقق من شخصيته وتبليغه المستند الذي قبض

عليه بموجبه[4]، لينقل بعض هذا الأجنبي في أقصر أجل ويحبس في سجن العاصمة[5].

وتقدم المستندات إلى النائب العام لدى المحكمة العليا الذي يقوم بدوره باستجواب الأجنبي المطلوب تسليمه[1] لترفع المحاضر والمستندات إلى الغرفة الجنائية بالمحكمة العليا وتمثل الأجنبي أماما في ميعاد

---

[1]- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت،المرجع السابق، ص 89.

[2]- لم يشترط المشرع الجزائري، الكتابة صرحه في طلب التسليم ،ولكن ضمن في نص المادة 702 من قانون الإجراءات الجزائية، والتي تنص على أنه " ... يرفق الطلب بحكم صادر بالعقوبة أو كل الوثائق التي تثبت متابعة القضائية"

[3]- نادية درادار، المرجع السابق، ص 60.

[4]- المادة 703 من قانون الإجراءات الجزائية الجزائري.

[5]- المادة 704 و705 من قانون الإجراءات الجزائية الجزائري.

قضاه 8 أيام من تاريخ تبليغ المستندات، ليتم استجوابه وتسمع أقوال النيابة مع السماح للأجنبي الاستعانة بمحام وبمترجم وجواز الإفراج عنه في أي وقت أثناء سير الإجراءات [2].

وفي حالة قبول المطلوب تسليمه رسميا تسليمه إلى سلطات الدولة تثبت الدولة هذا الإفراج وتحول نسخة منه بواسطة النائب العام غلى وزير العدل [3] وفي حالة عدم وجود هذا الإقرار، فإن المحكمة تبدي رأيها حول طلب التسليم فإذا رفضته بسبب وجود خطأ أو أن الشروط القانونية غير مستوفاة فإنها، تصدر رأيا مسببا نهائيا برفض طلب التسليم [4] ،وفي الحالة العكسية يعرض وزير العدل التوقيع إذا كان هناك محل لذلك مرسوما بالإذن بالتسليم، وإذا انقضى ميعاد شهر من تاريخ تبليغ هذا المرسوم إلى حكومة الدولة الطالبة دون أن يقوم ممثلو تلك الدولة باستلام الشخص المقرر تسليمه، فيفرج عنه ولا يجوز المطالبة به بعد ذلك لنفس السبب [5].

وبناءا على طلب مباشر من السلطات القضائية للدولة الطالبة يجوز لوكيل الجمهورية لدى المجلس القضائي وفي حالة الاستعجال أن يأمر بالقبض المؤقت على الأجنبي وذلك إذا أرسل إليه مجرد إخطار بالبريد أو بأي طرق الإرسال السريعة التي يكون لها أثر مادي مكتوب يدل على المستندات المبنية في المادة 702 السالفة الذكر مع وجوب إرسال إخطار قانوني إلى وزارة الخارجية بالطريق الدبلوماسي أو البريد أو البرق أو بأي طريق من طرق الإرسال التي لها أثر مكتوب مع وجوب أو إحاطة وزير العدل والنائب العام لدى المحكمة العليا لهذا القبض [6].

ثالثا: آثار التسليم

عند بيان الآثار المترتبة عن التسليم يفترض أن الطلب قد تم قبوله وتم فعلا تسليم الشخص إلى الدولة التي تطلبه، وبالتالي فإن الدولة المطلوب منها التسليم قد أتمت عملها، ومن ثم يأتي دور الدولة الطالبة في تنفيذ عملية التسليم وتقيد سلطتها القضائية بالجريمة المطلوب بشأنها التسليم فقط وهذا ما سنوضحه فيما يلي:

---

[1]– المادة 706 من قانون الإجراءات الجزائية الجزائري.

[2]– المادة 707 من قانون الإجراءات الجزائية الجزائري.

[3]– المادة 708 من قانون الإجراءات الجزائية الجزائري.

[4]– المادة 709 من قانون الإجراءات الجزائية الجزائري.

[5]– المادتان 710 و 711 من قانون الإجراءات الجزائية الجزائري.

[6]– المادة 712 من قانون الإجراءات الجزائية الجزائري.

أ- تنفيذ التسليم:

إن صدور أمر الموافقة على التسليم من طرف الدولة المطلوب منها ذلك يعطي الحق للدولة الطالبة في تسلم هذا الشخص وأن أغلب المعاهدات والنصوص القانونية حددت مدة زمنية يجب أن يجري خلالها التسليم وغالبا ما تحدد بشهر، وإذا لم يتم خلالها جاز للدولة المطلوب منها التسليم إطلاق سراح الشخص المطلوب إضافة إلى هذا ذهبت قوانين أخرى إلى رفض تسليم ولوجود الطلب مرة أخرى عن نفس الجريمة.[1]

أما بالنسبة لمكان تنفيذ طلب تسليم المجرم، فقد جرى العمل عن أن يكون إحدى الموانئ أو مطارات الدولة المطلوب منها التسليم، أو أحد نقاط الحدود بالنسبة للتسليم الذي يتم بين دول متجاورة، وفي بعض الأحيان يقتضي تنفيذ التسليم المرور على إقليم دولة أو عدة دول تتوسط الدولة الطالبة والمطلوب منها التسليم، أو أحد نقاط الحدود بالنسبة الذي يتم الدول المتجاورة.

كما يقتضي تنفيذ التسليم المرور على إقليم دولة أو عدة دول تتوسط الدولة الطالبة والمطلوب منا التسليم وفي هذه الحالة هناك إجماع على وجوب الحصول على موافقة الدولة التي سيتم العبور عبر إقليمها ،وهنا ثار خلاف حول شروط التسامح بالعبور فمنهم من يرى أن توفر شروط التسليم كفيلة لإحداث الموافقة على العبور، ودول أخرى تشترط إضافة إلى ذلك عدم حمل الشخص المراد تسليمه لجنسية دولة العبور.[2]

أما بخصوص المشرع الجزائري فقد نص في المادة 719 من قانون الإجراءات الجزائية على أنه "يجوز الإذن بتسليم شخص من أي جنسية كانت مسلم إلى حكومة أخرى بناء على طلب بالطريق الدبلوماسي مؤيد بالمستندات اللازمة لإثبات أن الأمر لا يتعلق بجنحة سياسية وذلك بطريق المرور عبر الأراضي الجزائرية أو بطريق بواخر الخطوط البحرية الجزائرية.

أما بخصوص نفقات التسليم فقد نصت الفقرة الأخيرة من المادة أعلاه على أن النقل الذي بواسطة المندوبين الجزائريين يتم على نفقة الحكومة الطالبة كما أن الاتفاقيات التي أبرمتها الجزائر سواء الثنائية أو الجماعية تنص على أن النفقات التي تتحملها الدولة الجزائرية هي كل النفقات التي تتم على أراضيها إذا كانت طالبة للتسليم.

---

[1]- نادية دردار، المرجع السابق، ص 67.

[2]- تنص الفقرة 4 من المادة 719 من قانون الإجراءات الجزائية الجزائرية على أنه "... ويتم النقل بواسطة المندوبين، الجزائريين وعلى نفقة الحكومة الطالبة "

وبالرجوع إلى التطبيقات العملية نجد أن الدول قد سارت في اتجاهين لتحديد الجهة التي يجب أن تتحمل تكاليف التسليم، حيث ذهب اتجاه إلى إلقاء نفقات التسليم على عاتق الدولة طالبة التسليم مع إمكانية تعويض الدولة المطلوب منها التسليم عن كل ما أنفقته، في حين ذهب اتجاه آخر إلى تقسيم نفقات التسليم بين الدولتين الطالبة والمطلوب إليها التسليم، حيث تتحمل كل دولة النفقات التي قامت بها على إقليمها.

ثانيا: مبدأ التخصيص:

يعد مبدأ التخصيص مبدأ مقرر دولي وواجب التطبيق مفاده لا يجوز محاكمة الشخص الذي تم استرداده حضوريا أو معاقبته في البلد الذي طلب تسليمه إلا عن التهم أو الأحكام التي طلب التسليم من أجلها، ما لم تكن شروط المعاهدة المبرمة بين الدولتين تجيز المحاكمة أو المعاقبة عن وقائع أخرى فإذا حوكم المتهم أو عوقب عن جريمة أخرى سابقة على التسليم، وغير وارد في الطلب جاز له أن يدفع بعدم قبول محاكمته أو معاقبته ويجب على القاضي أن يقضي بعدم قبول الدعوى أو بإيقاف التنفيذ [1].

ولقد أخذت الجزائر شأنها شان سائر الدول بمبدأ التخصيص في تفسيرها الداخلي وكذلك الاتفاقيات التي أبرمتها مع بقية الدول [2]

إلا أنه توجد استثناءات واردة على خصوصية التسليم تتمثل في:[3]

1- الإقامة في الدولة الطالبة للتسليم لمدة تزيد عن المدة القانونية بعد متابعته أو تنفيذ الحكم عليه وتحدد غالبا بثلاثين (30) يوما، أو غادر الدولة ثم عاد إليها من جديد، فإن هذا الشخص بمقتضى إقامته الطوعية يعتبر قد رضخ الاختصاص هذه الدول، ورضي بالخضوع لقضائها دون أي تحفظ.

2- موافقة الدول المطلوب منها التسليم، حيث يجوز محاكمة الشخص المسلم عن جرائم أخرى غير التي تسلم من أجلها، وهذا في حالة تقدم الدولة التي استردت هذا الشخص طلبا للدولة التي سلمته، لتأذن بملاحقته من أجل الجرائم التي اكتشفت بعد تسليمه، وهذا في الجرائم التي يجوز فيها التسليم.

---

[1]- نادية دردار، المرجع السابق، ص 68.

[2]- من بين الاتفاقيات التي نصت على مبدأ التخصيص معاهدة الأمم المتحدة لتسليم المجرمين لسنة 1990 والتي تعد معاهدة نموذجية للتسليم لتشكيل بذلك إطار يساعد الدول بصدد التفاوض على اتفاقيات التسليم الثنائية، وتتكون من 18 مادة وملحق صدر عام 1997 كما أن مجلس وزراء الداخلية العرب أقر هو الآخر قانونا نموذجيا لتسليم المجرمين كذلك اتفاقية فينا 1988 لمكافحة الاتجار غير المشروع بإحداث المؤتمرات العقلية والتي صادقت عليها الجزائر ودخلت حيز التنفيذ عام 1990.

[3]- جندي عبد المالك، الموسوعة الجنائية، الجزء الثاني، الطبعة الأولى، لبنان، 2005/2004، ص ص 606- 607.

3- القبول الاختياري وهذا في حالة استجابة الشخص المطلوب تسليمه إلى الطلب بحريته التامة حيث يتم تسليمه اختياريا.

يتضح مما سبق أن نظام تسليم المجرمين من أنجع الأنظمة في مجال ملاحقة المجرمين ومكافحة الجريمة التي أصبحت تهدد كيان المجتمع، لاسيما بعد ظهور الجرائم المستحدثة العابرة للحدود ومنها الالكترونية إضافة إلى إجراءات أخرى فرضتها ضرورة تكاثف الجهود لمواجهة هذا النوع من الإجرام إلا أن هذه الجهود تعترضها جملة من التحديات والصعوبات والتي سيتم دراستها في المبحث الثاني من هذه الدراسة.

المبحث الثاني: التحديات التي تواجه التعاون الدولي في مجال مكافحة جريمة التزوير الالكتروني.

رأينا فيما سبق أن عملية البحث والتحقيق في الجرائم الالكترونية وملاحقة مرتكبيها العديد من العقبات لاسيما فيما يتعلق بالطبيعة المتميزة للجريمة الالكترونية، سواء تعلقت الصعوبة بجهات التحقيق أو بإجراءات جمع الأدلة في شكلها الالكتروني، ما ينعكس سلبا على مردود سلطات التحقيق والعدالة الجنائية ،بل وشجع ارتفاع معدل الجريمة الالكترونية في العالم بسبب إدراك المجرم الالكتروني أن وجود كل تلك العقبات سيعيق حتما الجهات الأمنية من اكتشاف أمره وملاحقته.

ولتدارك هذا الخطر باتت عملية البحث عن الحلول المناسبة للقضاء على ما تثيره الجهود الدولية في مكافحة الجريمة الالكترونية من مصاعب ضرورة حتمية ومن هذا المنطلق سنحاول من خلال هذا المبحث بيان الصعوبات التي تواجه التعاون الدولي في مواجهة جريمة التزوير الالكتروني في المطلب الأول، في حين نخصص المطلب الثاني من هذا المبحث لبيان كيفية القضاء على الصعوبات التي تواجه التعاون الدولي.

المطلب الأول: الصعوبات التي تواجه التعاون الدولي في مجال مكافحة جريمة التزوير الالكتروني.

يعد التعاون الدولي في مجال الجرائم الالكترونية بصفة عامة وجريمة التزوير الالكتروني بصفة خاصة ضرورة لا غنى عنها، وإن كان يعد مطلبا تسعى إلى تحقيق أغلب الدول إن لم يكن كلها إلا أنه هناك صعوبات ومعيقات تقف دون تحقيقه وتجعله صعب المنال.

وسنعرض فيما يلي أهم الصعوبات التي تحول دون تحقيق الهدف المنشود من التعاون الدولي، والتي يكون سببها الطبيعة الخاصة للجريمة الالكترونية وتدرسها في الفرع الأول، أو صعوبات بسبب ضعف قوانين مكافحة الجرائم الالكترونية ونوضحها في الفرع الثاني، إضافة إلى الصعوبات الناتجة عن عدم فعالية التعاون الدولي في هذا المجال والتي سندرسها في الفرع الثالث ،وفيما يلي تفصيل ذلك:

الفرع الأول: الصعوبات الناتجة عن الطبيعة الخاصة لجريمة التزوير الالكتروني.

تعتبر الجرائم الالكترونية من بين الجرائم المستحدثة التي ظهرت في ظل التطور التكنولوجي الهائل في مجال الاتصالات، والتي تختلف عن الجرائم التقليدية التي ترتكب في العالم العادي، بتميزها بجملة من الخصائص التي جعلت منها ظاهرة إجرامية جديدة لم تكن معروفة من قبل تتم في عالم افتراضي غير محسوس.

وقد نتج عن الطبيعة الخاصة للجريمة الالكترونية العديد من الإشكالات والصعوبات تعلق بعضها بالطابع العابر للحدود وللجريمة الالكترونية وبعضها الآخر بالصعوبات المتعلقة بسلطات التحري والتحقيق والاستدلال.

أولا: انعكاسات الطابع العابر للحدود لجريمة التزوير الالكتروني على التحقيق.

من أهم خصائص الجريمة الالكترونية أنها جريمة دولية وعابرة للحدود ولا تعرف إقليم أو حدود تمنع انتشارها مما يتطلب تكاثف الجهود والمساعي الدولية للحد من وقوعها والتنسيق على الوقاية منها وسرعة اكتشافها حال وقوعها، فالجريمة الالكترونية جريمة ذات وثيرة سريعة في الارتكاب وتحقق النتيجة الضارة، كما أنها لا تعرف حدا معينا لمسرح الجريمة، ولا يشترط فيها أن يكون الجاني والنتيجة الجرمية في ذات البلاد أو الموقع الذي ارتكب منه الجاني فعله [1].

ولقد ثار خلاف بين الفقه حول تحديد المحكمة المختصة في نظر هذه الجرائم على اعتبار أن تنازع الاختصاص بين الدول من أكبر التحديات التي تواجهها عملية التحقيق في الجرائم الالكترونية لاتسامها بالبعد الدولي، بالإضافة إلى تجرد السلوك الإجرامي فيها من الطابع المادي لارتباطه بالعالم الافتراضي الرقمي مما يجعلها ترتبط بأكثر من ولاية قضائية ويجمع فيها أكثر من معيار واحد من معايير إسناد الاختصاص، مما يؤدي إلى تنازع ايجابي في الاختصاص بين جهات قضائية عدة.[2]

فقد يحدث أن ترتكب جريمة من الجرائم الالكترونية من طرف أجنبي على إقليم دولة معينة فيؤول الاختصاص في هذه الحالة إلى الدولة التي ارتكبت الجريمة على إقليمها استنادا إلى مبدأ الإقليمية وإلى الدولة التي تحمل الجانب جنسيتها استنادا إلى مبدأ الشخصية، وقد تشكل هذه الجريمة تهديدا لأمن

[1]– حنان ريحان مبارك المضحكي، المرجع السابق، ص 373.

[2]– براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص قانون جامعة مولود معمري، تيزي وزو، الجزائر، 2018، ص 186.

وسلامة دولة أخرى أو تمس لمصالحها الأساسية، فتدخل في اختصاصها استنادا إلى مبدأ العينية، وهو ما يترتب عليه تنازع الاختصاص بين الدول كل واحدة حسب المعيار الذي يربطها بالجريمة.[1]

وقد ذهب جانب من الفقه إلى أن الاختصاص في الجرائم الالكترونية يعقد إلى محاكم الدولة التي تم فيها تحميل البيانات كون جميع البيانات والأدلة ستكون سهلة لكونها المصدر، كما أن بنك معلومات محل التحميل يكون أكثر ثباتا.[2]

وقد وجهت العديد من الانتقادات لأصحاب هذا الجانب لعل أهمها أن بعض الأفعال قد لا يكون معاقبا في دولة التحميل، وبالتالي تكون فعلا مباحا فلا يعاقب عليه القانون، لذلك ظهر جانب آخر من الفقه يتجه لإعطاء الاختصاص لمكان وقوع النتيجة الجرمية لتعدد دول التحميل مما يعقد الاختصاص لأكثر من دولة يؤدي لضياع المسؤولية خصوصا إذا كانت دولة التحميل لا تعاقب مثل هذه الأفعال[3].

لكن هذا الرأي مردود أيضا حيث لم يضع في الحسبان مصلحة المتهم بأن تطبق عليه قوانين غير قوانين الدولة التي يحمل جنسيتها مما يزيد من كلفة المحاكمات في هذه الجرائم، وزيادة مدة وأجل المحاكمة.[4]

كل هذه المبررات استدعت نشأة اتجاه ثالث يرى بانعقاد الاختصاص القضائي لمكان المعتدي كونه المكان الذي تحققت فيه الجريمة ومرتبطا بشخص المعتدي عليه، وهو يتجنب السلبيات والانتقادات التي وجهت للاتجاهين السابقين.[5]

وأمام عدم نجاعة الحلول الفقهية المقترحة لتجاوز مشكلة تنازع الاختصاص لجأت الدول إلى تنظيم مسألة الاختصاص بنصوص واضحة في اتفاقيات دولية ثنائية ومتعددة الأطراف يتم من خلالها تحديد الضوابط التي بموجبها توزع الولاية القضائية بين الإطراف يتم من خلالها تحديد الضوابط التي بموجبها توزع الولاية القضائية بين الأطراف المتعاقدة لتفادي التنازع. فقد نصت المادة 15 من اتفاقية منظمة الأمم المتحدة لمكافحة الجريمة المنظمة على أنه: "يتعين على كل دولة طرف أن تعتمد ما يلزم من تدابير

---

[1]– عبد محمد بحر، معوقات التحقيق في جرائم الانترنت، مذكرة مكملة لنيل شهادة الماجستير في العلوم الشرطية، جامعة نايف للعلوم الأمنية، دبي، 1999، ص26.

[2]– حنان ريحان مبارك المضحكي، المرجع السابق، ص 373.

[3]– محمد عوض محمد، مشكلات السياسة الجنائية المعاصرة من جرائم نظر المعلومات، بحث مقدم إلى مؤتمر القانون الكومبيوتر والانترنت، الفترة من 1–3 مايو 2000، كلية الشريعة والقانون، الإمارات العربية المتحدة، ص 21.

[4]– حنان ريحان مبارك المضحكي، المرجع السابق، ص 374.

[5]– للمزيد أنظر: جمال براهيمي، المرجع السابق، ص 188.

لتأكيد سريان ولايتها القضائية على الجريمة التي ترتكب في إقليم تلك الدولة أو حينما ضد أحد مواطني تلك الدولة أو حينما ترتكب الجريمة من طرف أحد مواطني تلك الدولة أو من طرف شخص عديم الجنسية اتخذ مكان إقامته المعتاد في إقليمها...".

وأضافت هذه المادة أنه إذا بلغت الدولة التي تمارس ولايتها القضائية عن سلوك إجرامي ما بموجب المعايير السالفة الذكر أو علمت بطريقة أن دولة واحدة أو أكثر باشرت إجراءات التحقيق والمتابعة القضائية في السلوك ذاته، فعلى السلطة المختصة في هذه الدول أن تتشاور فيما بينها بغرض تنسيق من تتخذه من التدابير.

في حين نصت المادة 22 من اتفاقية مجلس أوروبا لمكافحة الجريمة الالكترونية على مسألة الاختصاص وأكدت على ضرورة أن يلتزم كل طرف بوضع ما يلزم من تدابير تشريعية لإقرار الاختصاص بشأن جريمة الكترونية، وذلك عندما ترتكب الجريمة على إقليميها و عندما ترتكب الجريمة من طرف أحد مواطنيه إذا كانت الجريمة معاقب عليها بموجب القانون الجنائي لمن ارتكبها أو في حالة ارتكاب الجريمة خارج الاختصاص القضائي الإقليمي لأي دولة.

وحثت هذه الاتفاقيات الأطراف المتعاقدة في حالة وجود تنازع الاختصاص بين أكثر من طرف بشأن أي جريمة تقررها هذه الاتفاقية باللجوء إلى التشاور فيما بينها لغرض تحديد الاختصاص القضائي الأكثر ملائمة لمتابعة هذه الجريمة. [1]

واقتداء بهذه التشريعات حاول المشرع الجزائري بدوره تقديم حلا لمشكلة تنازع الاختصاص بنصه في المادة 15 من القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصالات ومكافحتها على أنه ". .بالإضافة إلى قواعد الاختصاص المنصوص عليها في قوانين الإجراءات الجزائية، فإن المحاكم الجزائرية تكون مختصة أيضا بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الوطن عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني".

ولكن بالتمعن في هذا النص يتبين أنه إعادة صياغة للمادة 588 من قانون الإجراءات الجزائية التي نصت على مبدأ العينية ولم يأتي بأية إضافة جديدة إلى قواعد اختصاص مثلما استهل به نص المادة 15 من القانون 04/09.

---

[1]– الفقرة 5 من المادة 22 من اتفاقية مجلس أوروبا لمكافحة الجريمة الالكترونية متاحة على الموقع:
http//:conventioncoe.im/TREaty/Fr/treatis/htm/185.html تم الاطلاع على الموقع بتاريخ 2018/10/19

ثانيا صعوبة إثبات جريمة التزوير الالكتروني.

تتميز الجرائم الالكترونية عن الجريمة التقليدية بكونها ترتكب في بيئة افتراضية غير مادية عبر نبضات وذبذبات الكترونية رقمية غير محسوسة، وتمحى آثارها في وقت قياسي وهذا ما يشكل صعوبة في اكتشاف هذا النوع من الجرائم وبالتالي صعوبة إثباتها، نظرا لما للمجرم الالكتروني من ذكاء ومعرفة فنية تحول دون ترك أي أثر للجرم المرتكب.

وتوصف جريمة التزوير الالكتروني بالهادئة كون ارتكابها لا يحتاج إلى استعمال العنف أو القوة ولا إلى سفك الدماء، وإنما يتطلب سوى عدد من اللمسات الخاطفة على لوحة المفاتيح وسجلات مخزنة على الحاسب الآلي وتزويرها أو محوها دون أن تختلف أي آثار خارجية ملموسة. [1]

ولعل ما يجعل اكتشاف جريمة التزوير الالكتروني وصعوبة إثباتها هو الوسيلة المستعملة في ارتكاب التزوير والتي تتميز في معظم الحالات بالطابع التقني الذي يضفي عليه العديد من التعقيد باستخدام وسائل ذات تقنية عالية، ما يؤدي إلى تجديد الكيانات الإجرامية من الآثار والمعالم المادية التي يمكن الاستدلال من خلالها على وقوع الجريمة وإسنادها إلى شخص معين.[2]

كما تعد سهولة إخفاء الدليل الذي تخلفه جريمة التزوير الالكتروني وسرعة محوه من الأسباب الجوهرية التي تحول دون اكتشاف الجريمة وإتباعها إذ يستخدم المجرم الالكتروني عدة تقنيات تسمح له بمحو كل آثار الجريمة والتستر عليها بسهولة كبيرة كأسلوب التغليط والتضليل الذي يتم إما عن طريق التلاعب بقواعد البيانات والبرامج أو إدخال بيانات مزيفة أو محرفة في نظام معلومات الحاسب.[3]

وقد يلجأ المتهم إلى تشفير البيانات المخزنة داخل حاسوبه للحيلولة دون وصول المحقق إلى الأدلة التي تدينه، وهذا باستعمال رموز أو إشارات غير متداولة تصرح بمقتضاها البيانات أو المعلومات المراد تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا تمكن الوصول إلى المعلومات المخزنة في الحاسوب بدونها علما أن عملية التشفير هذه تتم وفق معدلات رياضية معقدة تسمى بالخوارزميات وهنا أيضا يجد المحقق نفسه إما خيارين لحل مشكلة التشفير وهما إما أن يحصل مع مفاتيح الشفرات من المتهم مشعل الحاسوب، وإما أن يحاول على الشفرات بنفسه، إلا أن في الخيار الثاني يجب أن يكون المحقق ملم بعلم تحليل الشفرات أو ما يسمى بعلم استرجاع النص المرتكز على

---

[1]– حسين بن سعيد الغافري للتحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، ص19 مقال منشور على الموقع، www.eastlws.Com تم الاطلاع على الموقع بتاريخ .12/04/2018

[2]– جمال براهيمي، المرجع السابق، ص 197.

[3]– حسين بن سعد الغافري التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، مرجع سابق، ص 09.

الرياضيات التطبيقية، وفروعها المختلفة مثل نظرية الاحتمالية ونظرية الإعداد والإحصاء والجبر، وهو الأمر المفقود لدى المحقق.[1]

وما يزيد من صعوبة إثبات جريمة التزوير الالكتروني نقص مهارات السلطات القائمة بالتحقيق من رجال الضبطية وقضاة نقص مهاراتهم الفنية في استخدام وسائل تكنولوجيا الإعلام والاتصال الحديث والانترنت، وعدم الاهتمام بمتابعة المستجدات الحاصلة في مجال الإجرام الالكتروني، وعدم إلمامهم بأساليب ارتكاب الجرائم الالكترونية وعدم معرفتهم اللغة الرقمية، فالطبيعة الخاصة للجريمة الالكترونية والخصوصية اللامادية للدليل الالكتروني الرقمي الذي يتطلبه إثبات الجريمة الالكترونية ينعكس سلبا على الجهات المكلفة بالبحث والتحري، فنقص الخبرة لدى هؤلاء يؤدي إلى تدمير الدليل وإتلافه على اعتبار أن جهلهم بأساليب ارتكاب الجرائم الالكترونية يجعلهم في كثير من الأحيان يقعون في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها مثل إتلاف محتويات الأقراص الممغنطة وأوعية المعلومات التي تخزن بها البيانات [2].

ولقد دفع هذا العجز بعض الدول إلى استقطاب المختصين وذوي الكفاءات في مجال تكنولوجيا الإعلام والاتصال ضمن أجهزتها الأمنية والقضائية وتنظيم دورات تدريبية تخصصية للدفع من قدرات هذه الأخيرة في مكافحة الإجرام الالكتروني [3]،إلا أن أجهزة الأمن والقضاء لا تزال غير قادرة على مواكبة التطورات والمتغيرات السريعة التي تطرأ يوما بعد يوم على ظاهرة الإجرام الالكتروني نظرا لحداثة هذا النوع من الإجرام وعدم اكتساب خبرة التعامل معها.

الفرع الثاني: الصعوبات الناتجة عن ضعف قوانين مكافحة الجرائم الالكترونية.

[1]– إسماعيل عبد النبي شاهين، أمن المعلومات في الانترنت، بحث مقدم إلى المؤتمر القانون والكومبيوتر والانترنت، كلية الشريعة والقانون الإمارات العربية المتحدة، 200، ص 11.

[2]– محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، الطبعة الثالثة، كلية الشريعة والقانون، الإمارات العربية المتحدة الفترة من 1 إلى 3 ماي 2004، ص 1070.

[3]– جمال ابراهيمي، المرجع السابق، ص 211.

تتسم القواعد الجنائية الموضوعية منها والإجرائية بطابع تقليدي مفرط يميل إل الثبات والاستقرار، وقد ترتب على ذلك قصور هذه القواعد عن مواكبة التطور العلمي والتكنولوجي وبالتالي صعوبة مكافحة الجرائم الناشئة عنها وملاحقة مرتكبيها ما يصيب التعاون الدولي بالهوان وعدم الفعالية.

ولعل أهم الصعوبات الناتجة عن ضعف قوانين مكافحة الجرائم الالكترونية بصفة عامة هي عدم كفاية النصوص العقابية التقليدية عن مواجهة هذا النوع المستحدث من الإجرام وكذا صعوبات المعاينة التقنية في البيئة الالكترونية وفيما يلي تفصيل ذلك:

أولا: عدم كفاية النصوص العقابية التقليدية.

على الرغم من أن إرهاصات الثورة التكنولوجية في مجال الاتصال عن بعد قد أفرزت العديد من الجرائم المستحدثة ذات الطبيعة الخاصة، إلا أن مكافحة هذه الجرائم ما زال يتم في إطار النصوص العقابية المألوفة التي وضعت لكي تطبق على الجرائم التقليدية، وهذا الأمر يترتب عليه الكثير من المشكلات الملاحقة هذه الجرائم الالكترونية ويتعذر تبعا لذلك اتخاذ إجراءات جمع الدليل بالنسبة لها، أو قد تلحق عدم المشروعية بهذه الإجراءات [1].

كما أن تطور القوانين بنفس السرعة والوتيرة التي تتطور بها وسائل الإعلام والتكنولوجيا ومهارات الذهن البشري جعل القوانين التقليدية تقف عاجزة عن مواجهة العديد من الجرائم التي ارتبطت بظهور وانتشار الوسائل والأجهزة الالكترونية خاصة إذا علمنا أن القوانين الوضعية السائدة في أغلب دول العالم يحكمها مبدأ الشرعية الجزائية على أنه "لا جريمة ولا عقوبة إلا بنص" وأن نطاق التجريم بالقياس في ظل هذا المبدأ يكون ضيقا جدا.

فهناك أفعال جديدة كثيرة خاصة في الدول المختلفة، مرتبطة باستعمال الحاسب الآلي غير مجرمة لمنظور القوانين العقابية التقليدية، ولا تمتد إليها رغم تهديدها للمصالح العامة وتشكل خطورة على المجتمع، وتثور هنا العديد من الصعوبات أمام تطبيق نصوص التجريم التقليدية، مردها أن هذه النصوص وضعت أساسا لحماية الأشياء المادية في مواجهة صور الاعتداء الألوفة والتقليدية مما يتعذر معه أن يقع تحت طائلة العقاب الاعتداء على عناصر ومكونات والأنظمة المعلوماتية فضلا عن أن

[1]– جمال ابراهيمي، المرجع السابق، ص 220.

تطبيق مثل هذه النصوص قد يتعارض أحيانا مع طبيعة الوسائل المستخدمة لتنفيذ الجرائم التي يتكون محلها البيانات أو المعلومات بشتى أنواعها أو المصورة أو المكتوبة. [1]

ونظرا للعجز الكبير الذي أثبته القوانين العقابية في مواجهة الجرائم الالكترونية حاولت بعض الدول خاصة المتقدمة منها إلى استدراك الوضع للنصوص الجنائية التقليدية ليطال تطبيقها هذه الجرائم وهذا بمنح السلطات القضائية حرية تفسير هذه النصوص بشكل أكثر مرونة يسمح من وضع هذه الجرائم تحت طائلة التجريم والمتابعة تفاديا من إفلات الجناة من قبضة العدالة. [2]

ونرى في هذا الصدد أن الأخذ بمبدأ التفسير الضيق للنصوص العقابية من شأنه أن يمس بمبدأ الشرعية الجزائية إذا ترك الأمر بيد القضاء، ما قد يؤدي إلى ارتكاب خروقات واعتداءات على الحريات والحقوق الفردية بدون أساس قانوني مشروع.

ونظرا لهذا العجز الكبير للقوانين العقابية التقليدية في مواجهة الجرائم الالكترونية حاولت بعض الدول إلى استدراك هذا العجز، وهذا بسن تشريعات جديدة تتجاوب مع الطبيعة الخاصة لهذه الجرائم، وهذا إما باستحداث نصوص جديدة أو بتعديل قوانين العقوبات الخاصة بها لتتماشى مع هذا النوع المستحدث من الإجرام ،إلا أنه تبقى العديد من الدول يلجأ إلى تطبيق الأحكام التقليدية القائمة ربما لافتقارها الخبرة وعدم القدرة على التعامل مع البيئة الالكترونية.

ثانيا: الصعوبات المتعلقة بالتفتيش والضبط في البيئة الالكترونية.

لم يتوقف الأمر عند قصور النصوص العقابية في مواجهة الجرائم الالكترونية، بل تعد إلى القوانين الإجرائية ذلك أن معظم إجراءات التحقيق والمتابعة التي تتضمنها التشريعات التقليدية لا تتلاءم مع طبيعة هذه الجرائم لاسيما إجراءات التفتيش والضبط كآلية إجرائية تهدف إلى الحصول على الدليل المادي لإثبات الجريمة ونسبتها إلى مرتكبيها، وهذا يتنافى مع الطبيعة غير المادية لمكونات الحاسوب.

وقد ثار خلاف حول مدى جواز التفتيش الوسط الافتراضي، وظهر في ذلك ثلاث اتجاهات فذهب الاتجاه الأول إلى جواز تفتيش وضبط المكونات المعنوية للحاسوب بمختلف أشكالها وجواز تفتيش وضبط

[1]– بكري يوسف بكري، التفتيش من المعلومات في وسائل التقنية الحديثة، دون طبعة، دار الفكر الجامعي، مصر، 2011، ص 23.

[2]– جمال إبراهيمي، المرجع السابق، ص 222.

أي شيء يتعلق بالجريمة ويساعد في الكشف عن حقيقة وقوعها ليشمل كل مكونات المادية والعفوية للحاسوب معا.[1]

بالمقابل ذهب اتجاه فقهي آخر وهو الغالب إلى عدم إمكانية إخضاع المكونات المعنوية للحاسوب من برامج وبيانات لعملية التفتيش والضبط لأن الغرض الأساسي من التفتيش هو ضبط الأدلة المادية، ولما كانت هذه المكونات الالكترونية المنطقية تفتقر إلى مظهر مادي ملموس إلا إذا تم تعديل غاية التفتيش تلك بجعلها تشمل ضبط الأدلة المادية وغير مادية على حد سواء.[2]

وعكس ما ذهب إليه الاتجاهين الفقهيين الأول والثاني، هناك من يرى أنه لا يجب الخلط عند تحليل مدلول الشيء بالنسبة لمكونات الحاسب بين الحق الذهني للشخص على البرامج والبيانات والكيانات المنطقية الأخرى وبين طبيعة هذه البرامج والكيانات، إنما ينبغي الرجوع في ذلك إلى تحديد مدلول كلمة (المادة) في العلوم الطبيعية.

فلما كانت المادة تعرف أنها "كل ما يشغل حيزا ماديا في فراغ معين " وكان الحيز مما يجوز قياسه والتحكم فيه فإن البرامج والكيانات المنطقية باعتبارها تشغل حيزا ماديا في ذاكرة الحاسب الآلي وهو تمكن قياس حيزها بوحدات قياس خاصة، وتأخذ شكل نبضات الكترونية تتوفر على خصائص المادة وبالتالي فهي من قبيل الأشياء المادية.[3]

وباستقراء غالبية التشريعات الحديثة نجدها أخذت بالاتجاه الفقهي الأخير لتجاوز الاختلاف القائم حول مدى خضوع المكونات المعنوية للحاسوب للتفتيش والضبط ورفع الإبهام عن عبارة "**الشيء**" التي كانت محور جدل وذلك بتعديل الدول لتشريعاتها الجزائية التقليدية وذلك بالنص صراحة على أن تفتيش الحاسب الآلي يشمل البرامج والبيانات المعالجة الكترونيا والأخذ بما أخذت الاتفاقية الأوروبية حول مكافحة الجرائم الالكترونية ببوداسبت وهذا في مادتها 19.

إلا أنه وبالرغم من إحداث معظم الدول تعديلات في تشريعاتها الإجرائية التقليدية بما يصد من إجراء التفتيش والضبط لمكونات الحاسوب إلا أن الإشكال لا يزال قائما نظرا لاحتفاظ وتمسك بعض الدول لاسيما المختلفة بالإجراءات التقليدية للتفتيش والعديد من الضوابط وهذا من شأنه أن يشكل عائقا كبيرا أمام جهات التحقيق ما يحول دون ملاحقة الجاني.

---

[1]– نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت، المرجع السابق، ص 225.

[2]– علي محمود علي محمود، الأدلة المحصلة من الوسائل الالكترونية في إطار نظريات الجنائي بث مقدم إلى المؤتمر العلمي حول الجوانب القانونية للمعلومات الالكترونية، الإمارات العربية المتحدة، 2003، ص 13.

[3]– جمال إبراهيمي، المرجع السابق، ص ص 225–226.

الفرع الثالث: الصعوبات الناتجة عن عدم فعالية التعاون الدولي.

أثبت الواقع العملي أن أي دولة لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة، لاسيما في جانب التكنولوجيا الذي أبرز عن تطورها ظهور الجرائم الالكترونية.

وباعتبار أن الجرائم الالكترونية تتميز بالعالمية وبكونها عابرة للحدود، فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، كما أن التحقيقات في الجرائم الالكترونية وملاحقتها قضائيا تؤكد أهمية المساعدة القانونية المتبادلة بين الدول حيث يستحيل على الدول بمفردها القضاء على هذه الجرائم العالمية العابرة للحدود.

والتعاون الدولي كما سبق بيانه بكافة صوره في مجال مكافحة الجرائم الالكترونية وإن كان مطلبا تسعى إلى تحقيقه أغلب الدول إن لم نقل كلها، إلا أنه ثمة صعوبات ومعوقات تحول دون تطبيقه.

ولعل من بين هذه الصعوبات عدم وجود نموذج للنشاط الإجرامي، ناهيك عن تنوع اختلاف النظم القانونية الإجرائية وعدم وجود قنوات اتصال، إضافة إلى الصعوبات التي تثيرها المساعدة القضائية الدولية وفيما يلي تفضيل ذلك :

أولا: عدم وجود نموذج موحد للنشاط الإجرامي.

إذا نظرنا إلى الأنظمة القانونية في الكثير من الدول لمواجهة الجرائم الالكترونية يتضح لنا من خلالها عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الانترنت الواجب تجريمه، فما يكون مباحا في أحد الأنظمة قد يكون مجرما وغير مباح في نظام آخر، وتمكننا أن نرجع ذلك إلى عدة أسباب وعوامل كاختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لآخر، وبالتالي اختلاف السياسة التشريعية من مجتمع لآخر.[1]

ولعل السبب أيضا في هذا التباين يعود إلى قصور التشريع ذاته بلدان العالم وعدم مسايرته لسرعة التقدم التكنولوجي، ومن ثم الجريمة الالكترونية، فلنا أن تتصور مثلا أنه حتى الآن لم يصدر قانون في دولة عربية خاصة بالجوانب الموضوعية والإجرائية للجريمة الالكترونية، بل لازال دائر حول ما إذا كان من الأفضل تعديل التشريعات العقابية القائمة كي تستوعب نماذج الجريمة الالكترونية، أم إدراج هذه

[1]– غانم مرضي الشمري، مرجع سابق، ص 124.

الأخيرة في قوانين فرعية متخصصة كقانون حماية الملكية الفكرية أم يكون من الملائم استحداث تشريعات جديدة خاصة بالجرائم الالكترونية [1].

كما أن عدم وجود تعريف موحد للجريمة الالكترونية أدى إلى إحداث ثغرات في منظومة القانون الدولي في مجاز مكافحة هذه الجرائم وإبقاء أفعال إجرامية خطيرة دون تجريم أو عقاب، مما يسهل إفلات الجناة من المسؤولية الجزائية كون نص التجريم هو بمثابة الركن الشرعي لقيام الجريمة وانتقاؤه يؤدي حتما إلى انتقاء المسؤولية الجزائية.[2]

ثانيا: اختلاف النظم القانونية الإجرائية.

بسبب تنوع واختلاف النظم القانونية الإجرائية، نجد أن طرق التحدي والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها كما هو الحال بالنسبة للمراقبة الالكترونية والتسليم المراقب والعمليات المستترة، وغيرها من الإجراءات الشبيهة فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة قد تكون ذات الطريقة غير مشروعة في دولة أخرى، وبالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنفاذ القانون في الدولة الأخرى على استخدام ما تعتبره هي انه أداة فعالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق ترى هذه الدولة أنها طرق غير مشروعة، حتى وان كان هذا الدليل قد تم الحصول عليه في اختصاص قضائي ويشكل غير مشروع.[3]

ولعل أحسن مثال على ذلك التباين التشريعي القائم بين القوانين اللاتينية والانجلوساكسونية حول مدى حجية الدليل الرقمي في الإثبات الجنائي، ففي القوانين ذات الصياغة اللاتينية على نظم الإثبات الجنائي الحر، ومنها القانون الفرنسي والجزائري والسوري واللبناني، فإن القاضي الجزائي يتمتع بحرية مطلقة في تقدير الأدلة المطروحة أمامه والأخذ منها ما يراه مناسبا لتكوين قناعته.

[1]– عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 103.

[2]– جمال ابراهيمي، المرجع السابق، ص 235.

[3]– يوسف حسن يوسف، المرجع السابق، ص ص 186–187.

في حين أن النظم الأنجلوساكسونية مثل بريطانيا والولايات المتحدة الأمريكية، لا تعترف للدليل الرقمي بحجة الإثبات الجنائي إلا إذا أخذ أحد الأشكال التي حددها المشرع مسبقا في وسائل الإثبات وقدر قيمتها الاقناعية، وتم الحصول عليه وفق شروط محددة سلفا.[1]

ثالثا: عدم وجود قنوات اتصال.

إن تبادل المعلومات في مجال الجرائم الالكترونية والحصول على البيانات والمعلومات من أهم أهداف التعاون، والتحقيق هذا الهدف كان لزاما أن يكون هناك نظام اتصال ليسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع الأدلة والمعلومات المهمة، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العملية التي غالبا ما تكون مفيدة في التصدي لهذه الجرائم، وبالتالي تنعدم الفائدة من هذا التعاون.

رابعا: التحديات الخاصة بالمساعدات القضائية.

لما كانت جريمة التزوير الالكتروني جريمة عابرة للحدود فإن مكافحتها والعقاب عليها يعد أمرا احتماليا في ظل الوضع الراهن للأنظمة القانونية حيث من الصعب ملاحقة القضايا التي يشمل فيها، لتحقيق عناصر خارجية بسبب عدم القدرة على التوفيق بين المدة التي تتطلبها المتابعة القضائية والسرعة التي تتسم بها الجرائم الالكترونية[2].

كما أن محاكمة المجرم المتواجد على أراضي دولة أجنبية يحتاج إلى إجراءات طويلة ومكثفة كذلك الأمر بالنسبة لتنفيذ الأحكام الصادرة في الخارج لأن تطبيقها سوف يصطدم بالعديد من العقبات لا محال ومن أهم هذه التحديات على هذا الصعيد، الإشكالات التي تطرحها الإنابة القضائية وكذا إشكالية تسليم المجرمين، تعد الإنابة القضائية باعتبارها أهم صور المساعدات القضائية.

أ-إشكالية الإنابة القضائية:

تعد الإنابة القضائية الدولية باعتبارها أهم صور المساعدات القضائية في المجال الجنائي والتي تتم بالطرق الدبلوماسية إحدى إشكالات التعاون الدولي في مكافحة جريمة التزوير الالكتروني كون إجراءاتها تتسم بالبطء والتعقيد وهو ما يتعارض مع طبيعة الجرائم الالكترونية بصفة عامة وما تتميز به سرعته، وبالتالي يستحيل معها القيام بإجراءات فعالة تؤدي إلى كشف جريمة ونسبتها إلى مرتكبيها كون الجريمة

[1]- Vergucht Pascal. Op cit. pp 433-434.

[2]- أيمن رمضان محمد أحمد، المرجع السابق، ص 260.

محل الدراسة تستلزم ردود سريعة خشية التلاعب بالبيانات التي قد تشكل دليلا ضد المتهم، ويرجع البطء في الردود لأسباب عدة لعل أهمها نقص الموظفين أو الفوارق في الإجراءات التي تعقد الاستجابة [1].

ومن هنا نجد الحاجة الملحة إلى إيجاد وسيلة أو طريقة تتسم بالسرعة تسلم من خلالها طلبات الإنابة كتعيين سلطة مركزية مثلا أو السماح بالاتصال المباشر بين الجهات المختصة في نظر مثل هذه الطلبات للقضاء عبئ مشكل البطء والتعقيد في تسليم طلبات الإنابة وهذا ما أوصى به مؤتمر الأمم المتحدة الحادي عشر لمنح الجريمة والعدالة الجنائية المنعقد في بانكوك في الفترة من 18-2005/04/25 حيث أكد على ضرورة تعزيز فعالية السلطات المركزية المعنية الضالعة في أعمال المساعدة القانونية المتبادلة وإقامة قنوات نباشر للاتصال فيما بينها بغية ضمان تنفيذ الطلبات في الوقت المناسبة [2] ونفس الشيء نجده في المادة 27 من الاتفاقية الأوروبية بشأن الإجرام المعلوماتي، حيث نصت على ضرورة المساعدة المتبادلة بين الأطراف وتعاون الأطراف بالمساعدة المتبادلة في إجراءات التحقيق أو المكافحة.

أما بالنسبة للرد على طلبات المساعدة فإنه من الضرورة بمكان الاستجابة الفورية والسريعة على هذه الطلبات، لأجل ذلك نصت غالبية المعاهدات والاتفاقيات الخاصة بالمساعدات القضائية المتبادلة على ضرورة الاستجابة الفورية والسريعة على طلبات التماس المساعدة وهذا ما أكدته الفقرة 3 من المادة 25 من الاتفاقية الأوروبية للإجرام المعلوماتي، حيث نصت على انه يمكن لكل طرف في الحالات الطارئة أن يوجه طلبا للمعاونة أو للاتصالات المتعلقة بها طريق وسائل الاتصال السريعة مثل الفاكس أو البريد الالكتروني على أن تستوفي هذه الوسائل الشروط الكافية المتعلقة بالأمن وصحتها (ويدخل ضمن ذلك الكتابة السرية إذا لزم الأمر (مع تأكيد رسمي لحق إذا اقتضت الدولة المطلوب منها المساعدة في ذلك وتقوم الدولة بالموافقة على هذا الطلب والرد عليه عن طريق إحدى وسائل الاتصال السريع.

ب -إشكالية تسليم المجرمين:

تتمثل إشكالية تسليم المجرمين في مشكلة ما يسمى بالتجريم المزدوج والذي يعتبر من أهم الشروط الخاصة بنظام تسليم المجرمين والمنصوص عليه في أغلب التشريعات الوطنية فبالرغم من أهميته، إلا أنه من أهم العقبات التي تواجه التعاون الدولي في مجال تسليم المجرمين،[3]وهذا إذا كان قانون الدولة

[1]- حسين الغافري، المرجع السابق، ص 194.

[2]- يوسف حسن يوسف، المرجع السابق، ص 194.

[3]- محمود إبراهيم غازي، المرجع السابق، ص 61.

المطلوب منها التسليم لا يجرم الفعل الذي ارتكبه المطلوب تسليمه، إضافة مشكلة التزاحم في طلبات التسليم وهذا في الحالة التي يصل فيها إلى الدول المطلوب منها التسليم أكثر من طلب لتسليم نفس الشخص من عدة دول طالبة للتسليم سواء كان الطلب متعلقا بذات الجريمة أو بجرائم أخرى.[1]والقول بالتزاحم لا يكفي مجرد الادعاء أو التصريحات الشفوية أو إبداء الرغبة في استلام الشخص، بل لابد من تقديم الطلب ومرفقاته التي تثبت نسبة الجريمة للمطلوب، كما لا يشترط في التزاحم أن تكون الطلبات مرسلة في وقت واحد، بل يكفي تواليها على الدول المطلوب منها، فالمهم أن يكون المطلوب لم يتم تسليمه بعد إلى أية دولة.

وتزداد هذه الإشكالات أكثر في الجرائم الإلكترونية سيما وأن معظم الدول لا تجرم هذه الجرائم ،بالإضافة إلى أنه من الصعوبة أن نحدد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تطبق على الجرائم الالكترونية أم لا؟، الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، وتحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم.

توصلنا من خلال ما سبق في سبيل مكافحة جريمة التزوير الالكتروني وبالرغم من الترسانة الضخمة من هذه الاتفاقيات الدولية والإقليمية والثنائية، وكذا القوانين الداخلية، يتخللها العديد من المعوقات والعقبات الإجرائية نظرا لأسباب عدة منها ما يتعلق بطبيعتها المميزة وصعوبة إجراءات التحقيق وغيرها من الأسباب، ما قد ينعكس سلبا على مكافحة هذه الجريمة وملاحقة مرتكبيها وهذا ما يدعو إلى الإسراع في احتواء هذا النوع على مكافحة هذه الجريمة وملاحقة مرتكبيها ،وهذا ما يدعو إلى الإسراع في احتواء هذا النوع الجديد من الإجرام وهذا بضرورة تفعيل القوانين العقابية سواء من الناحية الموضوعية أو الإجرائية سعيا إلى التنسيق والملائمة مع تشريعات الدول الأخرى بهدف الكفاح الدولي المشترك ضد هذا الإجرام.

وسنحاول بيان أهم الحلول المقترحة لمواجهة هذه الجرائم في المطلب الثاني من هذه الدراسة.

المطلب الثاني: الحلول القانونية لمواجهة التحديات الخاصة لمكافحة جريمة التزوير الالكتروني.

رأينا فيما سبق أن مكافحة جريمة التزوير الالكتروني وملاحقة مرتكبيها تتخللها العديد من العقبات والصعوبات، لاسيما ما تعلق منها بالجانب الإجرائي، وهذا ما انعكس سلبيا على مردود سلطات التحقيق والقضاء في ملاحقة مرتكبي الجريمة، وما جعل الدول عاجزة عن أداء واجبها الدستوري والقانوني لحماية

[1]– الهام بن خليفة، المرجع السابق، ص 375.

الأفراد وتحقيق الأمن والاستقرار إزاء الفراغ التشريعي لمكافحة هذا النوع المستحدث من الإجرام، وهذا ما دفعهم إلى تدعيم تشريعاتها بنصوص أخرى جديدة تتلاءم مع هذه الجرائم.

وهذا ما سنوضحه في الفرع الأول كما أن الطابع الدولي العابر للحدود كجريمة التزوير الالكتروني، كما رأينا مما سبق يشكل أكثر العقبات التي تواجه مكافحة هذه الجريمة كمشكلة احترام السيادة ولاختصاص، مما جعل الدول تسعى جاهدة لمجابهة هذه العقبات بوضعها جملة من الحلول القانونية القضائية، وهذا ما سنفصله في الفرع الثاني من الدراسة.

الفرع الأول: الحلول القانونية لتدارك تحديات مكافحة جريمة التزوير الالكتروني على مستوى التشريعات الوطنية.

من المعلوم أن الاستثمار في مجال الحاسبات له شأن عظيم، فالبرامج أصبحت لها صناعة وأصبح لها سوق مثل أي سلعة وأصبحت مصدرا هاما للثروة لا يستهان به في مجال الاستثمار، لذلك كان لزاما وضع استراتيجيات وبرامج على المستوى الوطني بدرجة أولى وعلى المستوى العالمي، مع الأخذ بعين الاعتبار لحركة تقدم كل دولة في مجال المعلوماتية وتجربتها لمواجهة مخاطر هذه الظاهرة وفي هذا الإطار ظهر ما يسمى بأزمة القانون الجنائي في مواجهة واقع المعلوماتية.

والإشكال الذي يطرح في هذا المجال كيف كانت مواقف واتجاهات الدول وما هي الاستراتيجيات المتبعة للمواجهة الجنائية للظاهرة؟ خاصة وأننا نقف أمام صعوبة الترجيح بين الاختيارات بخصوص السياسة الجنائية الواجبة الإتباع، فهل يكفي الرجوع إلى بعض الجرائم الواردة في القانون الجنائي التقليدي والبحث عن حلول في إطارها، أم لابد من تجاوز ذلك البحث عن حل جذري بإيجاد قانون جنائي للمعلوماتية متميز؟.

بصدد هذا التساؤل انقسم الفقه الجنائي في هذا المجال، فهناك من يرى أن المواجهة الفعالة للتحديات الإجرائية لمواجهة جريمة التزوير الالكتروني، والجرائم الالكترونية عموما، تقتضي التصرف بحكمة وبدون تسرع وذلك بترشيد النصوص الجنائية التقليدية وتطبيقها على الجرائم الالكترونية، في حين يرى البعض الآخر أنه لا ينبغي التعويل كثيرا على القواعد التقليدية، إذ لابد من مراجعة هذه النصوص بصفة دورية وإرساء قواعد قانونية جديدة تواجه هذا النوع المستحدث من الإجرام، وفيما يلي تفصيل ذلك:

أولا: تطبيق النصوص الجنائية التقليدية على الجرائم الالكترونية:

يعد تطبيق النصوص الجنائية والموضوعية التقليدية على الجرائم المستحدثة، لاسيما الالكترونية إحدى الحلول التي يمكن الاستعانة بها لمواجهة هذا النمط المستحدث من الإجرام، لاسيما في ظل عدم تدخل المشرع الجنائي بإصدار تشريعات خاصة بهذا الجرم.

وتكون المكافحة في هذا المجال بالاعتماد على التفسير الموسع للنصوص العقابية التقليدية وتطبيقها على الجرائم الالكترونية، ويعطى للقاضي الجزائي حرية تفسير هذه النصوص تفسيرا يسمح بوضع هذه الجرائم تحت طاولة التجريم والمتابعة الجزائية مستعملا في ذلك سلطة النقد.[1] فعندما تعرض قضية جزائية على القاضي، فإن أول شيء يقوم به هو تكثيف الواقعة لمعرفة مدى تطابقها مع النص القانوني الذي يجرمها للوصول إلى هذه الغاية يقوم القاضي باستخلاص عناصر هذه الواقعة من النص، وقد يصادفه أثناء ذلك صعوبة أو غموض فيلجأ عندئذ إلى تفسير النص الجنائي [2].

وفي هذا الصدد لجأ القضاء الجنائي في العديد من الدول إلى تفسير النصوص الجنائية، وهذا ما اعتمده القضاء الفرنسي من خلال توسيعه من تفسير المادة 145 من قانون العقوبات في مجال تزوير المحررات التقليدية قبل تعديلها بالمادة 462 من قانون الغش المعلوماتي، كما سبق بيانه لتشمل كل أشكال التلاعب في البيانات والأنظمة المعلوماتية. وكذلك ما قام به القضاء الياباني، حيث لجأ في ملاحقة التزوير المعلوماتي إلى تبني المفهوم الموسع لجريمة التزوير واعتبر تغيير الحقيقة في الجزء الممتعض من بطاقات البيانات يقع تحت طائلة العقاب على التزوير في المحررات التقليدية.[3]

ولا يقتصر هذا العمل على تمديد النصوص الجنائية التقليدية الموضوعية إلى الجرائم الالكترونية، فحسب بل لابد أن تمتد إلى النصوص الإجرائية خاصة ما تعلق منها بإجراءات التحقيق وأدلة الإثبات، وهو ما أوصلت به اللجنة الأوروبية الخاصة بالمشكلات الإجرائية المرتبطة بتكنولوجيات الإعلام الدول الأعضاء في المجلس الأوروبي من خلال توصياتها رقم (89) الصادرة في عام 1990، وأكدته في توصياتها رقم (95) لعام 1995 بتصريحاته أنه: "إلى حين وضع نصوص إجرائية جديدة تخصص التفتيش والضبط

[1]– هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، الطبعة الأولى، دار النهضة العربية، مصر، 2012، ص72.

[2]– يوسف حسن يوسف، مرجع سابق، ص 126.

[3]– جمال إبراهيمي، المرجع السابق، ص 246.

واعتراض المراسلات في البيئة الالكترونية، يمكن السلطات القضائية المختصة في الدول الأعضاء الاستعانة بالنصوص الإجرائية القائمة في هذا الخصوص حتى لا تبقى الجرائم المتصلة بتكنولوجيات الإعلام بلا متابعة ولا عقاب"[1].

ثانيا: ضرورة إرساء قواعد قانونية لمواجهة جريمة التزوير الالكتروني:

اختلفت خطة التشريعات حول موضوع النص الذي يجرم التزوير ويرجع السبب في ذلك إلى الجدل الذي أثير حول مدى إمكانية تطبيق نصوص التزوير التقليدية على التزوير في المحررات الالكترونية، وقامت بإدخال تعديلات على النصوص العقابية القائمة على نحو يؤدي إلى استيعاب صور التزوير المستحدثة بوضع قوانين خاصة ببعض المجالات كتكنولوجيات الاتصال والتوقيع الالكتروني.

في حين ذهبت تشريعات أخرى إلى عدم إمكانية تطبيق نصوص التزوير على الإجرام الالكتروني المستحدث حيث أفردت شقا ختاميا يتعلق بالتزوير الالكتروني والعقوبات المقررة له، وهناك من التشريعات من وضعت قانونا خاصا، يجرم كل الاعتداءات على تقنية المعلومات.

وتأسيسا على ذلك فقد استدركت أغلب الدول بمختلف أنظمتها القانونية العجز في ملاءمة القوانين النافذة للاعتداءات الحاصلة على النظم المعلوماتية، وسنأخذ على سبيل الاستدلال ما جاء به المشرع الفرنسي والمغربي وصولا للمشرع الجزائري.

أ- **التشريع الفرنسي:**

يعد المشرع الفرنسي من أوائل المشرعين الذين يتقنوا بأن التصدي للجريمة الالكترونية لن يكون إلا من خلال نصوص عقابية وإجرائية خاصة بهذه الجرائم، وقد كانت أولى محاولاته لمد سلطان قانون العقوبات ليشمل المجال المعلوماتي من خلال قانون المعلوماتية والحقوق الشخصية الصادر عام 1978،

[1]- Conseil de l' Europe ,la criminalité informatique recommandation N R 89 ru la criminalité en relation avec l'ordinateur et rapport final du comité européen pour les problèmes criminels , Strasbourg ,1990, p19.

ليصدر من بعده المرسوم المؤرخ في 1981/12/23 الذي حدد فيه بعض المخالفات المرتبطة بالمعلوماتية وفي سنة 1988 صدر القانون 88/19 المعدل لقانون العقوبات بشأن الغش المعلوماتي[1].

وجاء في المادة 462 فقرة 5و 462 فقرة 6 أحكام تتضمن تجريم المستندات المعالجة آليا وكذا استعمال تلك المحررات، إلا أنه بعد صدور قانون العقوبات الفرنسي الجديد في 1992/12/16 قرر المشرع الفرنسي عدم ضرورة الإبقاء على التجريم الخاص بتزوير المستندات المعالجة آليا واستعمالها والاكتفاء بإضافته إلى جريمة التزوير العادية، وذلك بتعديل المادة 1/441 من الكتاب الرابع من قانون العقوبات[2].

وقد تواصلت جهود المشرع الفرنسي في هذا المجال بشكل مكثف بعد تصديق فرنسا في 23 نوفمبر 2001 على الاتفاقية الأوروبية الخاصة بالجرائم الالكترونية عام 2001، فقامت من جهة بتعديل تشريعاتها النهائية لتتجاوب مع أحكام هذه الاتفاقية ،ومن جهة أخرى استحدث ترسانة أخرى من نصوص أخرى خاصة لمواجهة الجريمة الالكترونية أهمها القانون رقم (1062/03) المتعلق بالأمن اليومي المؤرخ في 2001/11/15[3] والقانون رقم (239/03) المتضمن التوجيه والتخطيط للأمن الداخلي المؤرخ في 2003/03/18 [4]، وكذا القانون 204/04 المتضمن مواكبة العدالة لتطورات الإجرام [5] وكذا القانون رقم (575/04) المتعلقة بالثقة في الاقتصاد الرقمي المؤرخ في[6] 22/2004 والقانون رقم (669/04)

[1] –CHOPIN–Férédirique. Les politiques publiques de lutte contre la cybercriminalité, Aj pénal Pari, France ,p102.

[2]– Voir : Marc SegondS .op.cit ,p05.

[3]– Loi N 2001 .1062.15 nov– 2001 relative a la sécurité quotidienne. JORF 16nov –2001 p.18.215.

[4]– Loi N= 2003–239 18 marc 2003 pour la sécurité intérieure , JORF 19 mars 2003. P4761.

[5] –Loi N= 2004–204.9 mars 2004. Pourtant adaptation de la justice aux évolution de la criminalité ,JORF 19 mars , 2004. P4567.

[6]–Loi N=2004–575.21 juin 2004 pour la confiance a de l'économie numérique ,JORF 22 JUIN 2004, P11 568.

المتعلق بالاتصالات الالكترونية وخدمات الاتصال لعام 2004 [1]، وقانون الحماية الجنائية للملكية الأدبية والفنية عبر الانترنت (hadopi2) لعام 2009.

كما أدخل المشرع الفرنسي تعديلات على إجراءات المتابعة الجزائية والتحقيق والإثباتات التقليدية كإجراءات التحري والتفتيش والمعاينة بما يجعلها تناسب مع الجرائم المرتكبة في البيئة الالكترونية،كما استحدث إجراءات تحري للكشف عن الجرائم الالكترونية كاعتراض المراسلات والتسرب والتحفظ العاجل للمعطيات والكشف عن المعطيات المشفرة.[2]

ب المشرع المغربي:

اتخذت الجريمة الالكترونية في المغرب خلال العقود الأخيرة صورا متعددة، مما دفع المشرع إلى سن تشريع مهم كونه صدر لسد الفراغ التشريعي في مجال مكافحة هذا النوع من الإجرام، وهذا من خلال القانون رقم 07/03 المؤرخ في 11 نوفمبر 2003 المتمم لمجموعة قانون الجنائي المغربي المتعلق بتنظيم المعالجة الآلية للمعطيات ويحتوي هذا القانون على تسعة فصول (من الفصل 3 إلى الفصل 10) من مجموعة القانون الجنائي المغربي [3].

ولعل القراءة الشمولية لمقتضيات التشريع تمكننا من حصد الأفعال الجرمية التالية :

- ✓ الدخول الاحتيالي إلى مجموع أو بعض نظام المعالجة الآلية للمعطيات,
- ✓ البقاء في نظام المعالجة الآلية للمعطيات بعد الدخول خطأ فيه.
- ✓ حذف أو تغيير المعطيات المدرجة في نظام المعالجة الآلية للمعطيات أو التسبب في اضطراب سيره.
- ✓ العرقلة العمدية لسير نظام المعالجة الآتية للمعطيات أو إتلافها أو حذفها منه أو تغيير المعطيات المدرجة فيه، أو تغير طريقة معالجتها أو طريقة إرسالها بشكل اختيالي.

[1]-Loi N= 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux service de communication ,JORF du 10 juillet 2004. P 12483.

[2]-CHOPIN. Frédérique. Op .cit .p110.

[3]- السيد عبد الحميد أحمد ، جرائم الشبكة العنكبوتية وغسل الأموال في إطار الملاحقة الأمنية والقضائية الدولية، الطبعة الأولى، مكتب الوفاء القانونية، مصدر 2018، ص 404.

- ✓ التزوير أو التزييف لوثائق المعلومات أيا كان شكلها إذا كان من شأن التزوير أو التزييف إلحاق ضرر بالغير.
- ✓ استعمال وثائق معلومات مزورة أو مزيفة.

وأول ما يلاحظ على هذا القانون هو عدم قيام المشرع المغربي بوضع تعريف لنظام المعالجة الآلية للمعطيات، تاركا ذلك للفقه والقضاء، ذلك أن المجال المعلوماتي هو مجال حديث ومتجدد، وبالتالي فإن أي تعريف يتم وضع لتعريف خاص بنظام المعالجة الآلية للمعطيات، وهذا ما أخذ به المشرع الفرنسي في قانون الغش المعلوماتي لسنة 1988 كما سبق بيانه.

ج المشرع الجزائري:

إن ظهور المعلوماتية وتطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة في إطار ما يسمى بأزمة القانون الجنائي في مواجهة واقعة المعلوماتية، وهنا كانت الحاجة ملحة وضرورية لتخطي هذه الأزمة وقد استجابت عدة دول لهذا الاتجاه منها الولايات المتحدة الأمريكية، كندا ألمانيا، فرنسا... الخ,

وبالنسبة للتشريع الجزائري فقد تدارك الأمر مؤخرا ولو نسبيا – الفرع القانوني في مجال الإجرام المعلوماتي وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية المتضمن تعديل قانون العقوبات ،أين أدرج في الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر 66/ 156 القسم سابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" ويشمل المواد من 394 مكرر إلى 394 مكرر.

ولكن تجدر الإشارة هنا إلى أن المشرع الجزائري في هذا التعديل قد ركز على الاعتداءات الماسة بالأنظمة المعلوماتية. وأغفل الاعتداءات الماسة بمنتجات الإعلام الآلي والمتمثلة في التزوير المعلوماتي، كما أدرك المشرع الجزائري أن المواجهة الفعالة للإجرام الالكتروني لا تكون بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية فقط، ولابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية تحفظية، وهو ما استدركه بتضمين القانون رقم (06-22) المعدل لقانون الإجراءات الجزائية تدابير إجرائية جديدة تتعلق بالتحقيق في الجرائم الالكترونية كاعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب وتمديد الاختصاص.

وأضاف أيضا المشرع الجزائري القانون رقم (09-04) الذي تضمن جملة من النصوص القانونية لمواجهة الجرائم الناشئة عن الاستخدام غير المشروع لوسائل الإعلام والاتصال الالكتروني وشبكة الانترنت، والذي تضمن جملة من التدابير المستحدثة وغير المألوفة في القوانين السابقة وأكثر ملائمة مع

خصوصيات هذا الإجرام، تتنوع بين تدابير وقائية وأخرى إجرائية مكملة لتلك المنصوص عليها في قانون الإجراءات الجزائية كمراقبة الاتصالات الالكترونية وإقحام مزودي خدمات الاتصال الالكترونية.

ونخلص في الأخير إلى أن المشرع الجزائري رغم تداركه من خلال القانون 15/04 والمتضمن تعديل قانون العقوبات الفرع القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الاعتداءات الواردة على الأنظمة المعلوماتية باستحداث نصوص خاصة، إلا أنه أغفل تجريم الاعتداءات الواردة على منتجات الإعلام الآلي، فلم يستحدث نصا خاصا بالتزوير الالكتروني، ولم يتبنى الاتجاه الذي تبنته التشريعات الحديثة التي عمدت إلى توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث.

ورغم هذه المجهودات إلا أننا نأمل بصدور قانون للوقاية من الجريمة الالكترونية يعني بمحاربة أشكال جديدة من الجرائم ليتصدى لتلك المرتبطة بالتكنولوجيات الحديثة وكشف مرتكبيها من خلال جملة من التدابير كوضع ترتيبات تقنية لمراقبة وتجميع الاتصالات وإجراءات الحجز والتفتيش مع إمكانية اللجوء إلى السلطات الأجنبية المختصة للوصول إلى المعطيات المطلوبة.

الفرع الثاني: الحلول القانونية لتدارك تحديات مكافحة جريمة التزوير الالكتروني على مستوى التشريعات الدولية.

تصطبغ الجرائم الالكترونية بصبغة دولية وعابرة للقارات وعدم معرفتها حدودا أو إطارا واحدا لذا كان لزاما على المجتمع الدولي الالتفات إلى التكاثف وتوحيد الجهود لمكافحة هذه الجريمة، خصوصا بعد خروجها من الإطارات الشخصية وارتكابها من قبل أشخاص بدون تنظيم إلى وجود كيانات ومنظمات إجرامية تقوم بارتكاب هذه الجرائم، وقد لا يجمع بين أفراد هذه الكيانات عرق أو دين أو إقليم، وإنما يجتمعون تحت ظل الغاية أو الهدف المردود الناجم عن هذه العمليات سواء ما لي أو غير ذلك.

كل هذه المسائل تحتاج إلى تكثيف الجهود المبذولة على مستوى الإقليمي أو الدولي وإذا كانت الحلول التشريعية قد ارتبطت بشكل عام بالعقبات التي تشيرها عملية التحقيق في جريمة التزوير الالكتروني والجريمة لالكترونية عموما، فإن الحلول القضائية التي تقترحها ترتبط أكثر المشكلات والعملية التي تربطها الجريمة الالكترونية عبر الوطنية ما يجعل هذه الحلول أجدى الضروريات اللازمة لمواجهة هذا النوع من الإجرام.

وتتجلى هذه الحلول في تعزيز المساعدة القضائية الدولية، وكذا التعاون الدولي في مجال التدريب علة مواجهة هذا النوع من الإجرام.

أولا: تعزيز المساعدة القضائية الدولية.

فيما يتعلق بالصعوبات الخاصة بالمساعدات القضائية الدولية والتباطؤ في الرد فإننا نجد الحاجة ملحة إلى إيجاد وسيلة أو طريقة تتسم بالسرعة من خلالها طلبات الإنابة كتعين سلطة مركزية مثلا أو السماح بالاتصال المباشر بين الجهات المختصة في نظر في مثل هذه الطلبات لتقضي على مشكلة البطء والتعقيد في تسليم طلبات الإنابة [1].

وهذا بالفعل ما أوصى به مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية المنعقدة في بانكوك في الفترة من 18-2005/04/15 حيث أكد على ضرورة تعزيز فعالية السلطات المركزية المعنية الضالة في أعمال المساعدة القانونية المتبادلة وإقامة قنوات مباشرة للاتصال فيما بينها بغية ضمان تنفيذ الطلبات في الوقت المناسب، وهذا ما نجده في البند الثاني من المادة 27 من الاتفاقية الأوروبية بشأن الإجرام المعلوماتي، وكذا المادة 35 من ذات الاتفاقية التي أوجبت على الدول الأطراف فيها ضرورة تحديد نقطة اتصال تعمل لمدة 24 ساعة يوميا طوال أيام الأسبوع لكي تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشبكات، أو استقبال الأدلة في الشكل الالكتروني من الجرائم، كما أوجبت ذات المادة على الدول الأطراف ضرورة أن تتمكن نقطة الاتصال السريع بنقطة اتصال الطرف الآخر وأن يعمل كل طرف على أن يتوافد لديه الأفراد المدربين القادمين على تسهيل عمل الشبكة [2].

ولقد لقيت المساعدة القضائية صدى كبير في العديد من الاتفاقيات سواء كان ذلك على الصعيد الدولي أو الإقليمي كمعاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية، وكذا المادة 48 فقرة 18 من البند (5) من اتفاقية الأمم المتحدة لمكافحة الفساد والتعاون الدولي، والمادة الرابعة فقرة 1 من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي، وكذا ما جاء من الفقرات الثالثة والرابعة والخامسة من المادة الثامنة من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، التي فرضت على الدول الأطراف تسير بتبادل المعلومات المتعلقة بمكافحة جوانب النشاط الإجرامية، يضاف لها على المستوى الإقليمي ما أوصت به المادة الأولى من اتفاقية الرياض العربية، وما ورد في المادتين الأولى والثانية من القانون الاسترشادي لاتفاقية التعاون القضائي والقانوني الصادر عن مجلس التعاون الخليجي.[3]

---

[1]- يوسف حسن يوسف، المرجع السابق، ص 194.

[2]- غانم مرضي الشمري، المرجع السابق، ص 130.

[3]- جمال إبراهيمي، المرجع السابق، ص ص 317-318.

أما بالنسبة للرد على طلبات التماس المساعدة فإنه من الضرورة الاستجابة الفورية والسريعة على هذه الطلبات، لأجل ذلك نصت غالبية المعاهدات والاتفاقيات الخاصة بالمساعدات القضائية المتبادلة على ضرورة الاستجابة الفورية والسريعة على طلبات التماس المساعدة [1].

وبخصوص نقل الإجراءات كإحدى صور المساعدة القضائية فقد ازدادت إليها لاسيما مع إشاعة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال الحديثة، لكن ليس على الطريقة التقليدية والبطيئة القائمة على نقل الوثائق الخطية والمختومة عبر القنوات الدبلوماسية أو أنظمة البريد القديمة وإنما وفق وسائل جديدة فورية وسريعة وذات مصداقية ودقيقة بالقدر الكافي الذي يتطلبه التعامل مع هذه الجرائم [2] ،ولأجل هذا استحدث مجلس الاتحاد الأوروبي آلية جديدة تسمى بقضاة الاتصال وهي تقنية تسمح لكل دولة عضو بتعيين هيئة قضاة وطنية يتكون اختصاصها الإشراف عن عملية المساعدة القضائية الدولية والتنسيق المباشر والفوري مع نظريتها الأجنبية في هذا المجال [3].

وقد ذهبت فرنسا إلى أبعد ن ذلك إذ قامت بتعيين قضاة اتصال تعمل مع دول ليست أعضاء في الاتحاد تساهم في تطوير وتيسير المساعدات القضائية بين الدول الأعضاء من خلال تقصير الوقت واختصار الإجراءات عن طريق التواصل المباشر فيما بين الدول بوسائل سريعة وميسرة كما تقوم هيئة قضاة الاتصال بمساعدة السلطات القضائية والأمنية في بلدها الأصلي على فهم التشريعات الوطنية للدول الأخرى [4].

وفيما يتعلق بتبادل الإنابة القضائية كصورة من صور المساعدة القضائية هدفها تسهيل الإجراءات بين الدول بما يكفل إجراءات التحقيقات اللازمة لمحاكمة المتهمين فقد أصبحت المعاهدات والاتفاقيات

---

[1]– وهذا ما أكدته الفقرة 3 من المادة 25 من الاتفاقيات الأوروبية للإجرام المعلوماتي حيث نصت على أنه "يمكن لكل طرف في الحالات الطارئة أن يوجد طلب للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل الاتصال السريعة مثل الفاكس أو البريد الالكتروني على أن تستوفي هذه الوسائل الشروط الكافية المتعلقة بالأمن وصحتها ويدخل ضمن ذلك الكتابة السرية إذ لزم الأمر وتقوم الدولة بالموافقة على هذا الطلب والرد على هذا الطلب عن طريق إحدى وسائل الاتصال السريعة "

[2]– المادة 25 من الاتفاقية الأوروبية بشأن الإجرام المعلوماتي.

[3]– تم الاعتماد على هذه الآلية بشكل تجريبي، بموجب المادة الأولى من ورقة العمل المشترك المصادق عليها من طرف المجلس الأوروبي في 196/04/22 طبقا للمادة 3 من اتفاقية الاتحاد الأوروبي / انظر الجريدة الرسمية للاتحاد الأوروبي، عدد 105 الصادر في 1996/04/27.

[4]– Vuelta Simon. Les nouveaux acteurs de la coopération pénale européenne LPA N=1 .2005. P4.

الدولية الخاصة بتبادل هذه المساعدة تشترط على الدول الأطراف إرسال الطلبات مباشرة لاختصار الوقت وتسريع الإجراءات بدلا من الولوج إلى الطرق الدبلوماسية التي تأخذ وقتا طويلا نظرا لما تتسم به من التعقيد والبطء [1].

وفيما يتعلق بمواجهة التحديات التي تواجه نظام تسليم المجرمين كشكل من أشكال التعاون القضائي الدولي لمكافحة الجريمة الذي فرضته التطورات الحاصلة في كافة المجالات ومنها تكنولوجيات الإعلام والاتصال سارعت معظم الدول في عقد اتفاقيات دولية وإقليمية لتبادل تسليم المجرمين، وقد كانت الدول الأوروبية سباقة في هذا المجال منذ إبرامها في 13 ديسمبر 1957 كأول اتفاقية في مجال تسليم المجرمين حيث نظمت أحكامه وشروطه وإجراءاته وقد تم تثبيت هذه الأحكام في المادة 24 من الاتفاقية الأوروبية حول الجرائم الالكترونية لعام 2001 من خلال إدراج الجرائم الالكترونية ضمن الجرائم التي يجوز فيها تسليم المجرمين، وكذا اقتراح بعض الحلول للمشاكل التي تثيرها عملية التسليم [2].

ولأجل تحقيق ذلك اعترف المشرع الجزائري بمبدأ تسليم المجرمين وجعل منه مبدأ دستوري وهذا من خلال المادة 82 من القانون رقم 01/16 المتضمن التعديل الدستوري بنصها على مبدأ جواز تسليم شخص بناء على قانون تسليم المجرمين وتطبيقا له، وتناولت المواد 694 وما يليها من قانون الإجراءات الجنائية الأحكام الإجرائية والموضوعية للتسليم.

ثانيا: التدريب كآلية لمواجهة تحديات التعاون الدولي في مكافحة جريمة التزوير الالكتروني

إن التقدم المتواصل في تكنولوجيا الحاسب الآلي يفرض على جهات إنقاذ القانون أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات، والإلمام بها حتى يتمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا ومواجهتها هذا من ناحية، ومن ناحية أخرى فإن أعمال القانون في مواجهة الجرائم الإلكترونية يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة في

---

[1]– نصت على ذلك المادة 27 فقرة 2 من الاتفاقية الأوروبية حول الجرائم الالكترونية لعام 2001 بقولها "... 2–أ يجب على كل طرف أن يعين هيئة مركزية أو هيئات تكون مسؤولة عن إرسال أو الرد على طلبات المساعدة المتبادلة أو إرسالها إلى السلطات المختصة.

ب يجب على الهيئات المركزية أن تتصل ببعضها البعض بشكل مباشر "

[2]– تنص المادة 24 على أنه " تطبق هذه المادة على تسليم فيما يبين الأطراف بالنسبة للجرائم المنصوص عليها في المواد من (2–11) من هذه الاتفاقية .....

تعبر الجرائم الجنائية الواردة في الفقرة 1 من هذه المادة مدرجة يجب فيها التسليم في أي اتفاقية بشأن تسليم المجرمين قائمة بين الأطراف ويتعهد الأطراف بإدراج هذه الجرائم على أنها يتم التسليم في أي اتفاقية بشأن تسليم المجرمين يتم إبرامها مما فيه ".

المدونة العقابية التقليدية لما تتسم هذه الجرائم من حداثة في الأسلوب وسرعة في التنفيذ وسهولة في إخفائها والقدرة على محو آثارها.[1]

وبالتالي فإن ظهور هذه الأنماط الجديدة من الجرائم أصبح يشكل عبئا ثقيلا على عاتق جميع أجهزة العدالة الجنائية، لأجل ذلك كان لابد أن تكون هذه الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والقدرة والمعرفة على كشف غموض تلك الجرائم والتعرف على مرتكبيها بسرعة وبدقة، وهذا لن يتحقق إلا بالتدريب ومن هذا المنطلق كانت الدعوى إلى وجوب تأهيل القائمين على هذه الأجهزة كما أنه لا يمكن لدولة بمفردها النجاح في مواجهة هذا النوع المستحدث من الإجرام دون تعاون وتنسيق مع غيرها من الدول وهنا كانت الحاجة إلى ضرورة وجود تعاون دولي في مجال التدريب وهذا ما سنوضحه فيما يلي:

أ – أهمية التدريب في مجال مكافحة جريمة التزوير الالكتروني:

يعد التدريب[2] جزء من عملية التنمية الإدارية وهو يهتم بالدرجة الأولى بالكفاءة والفعالية في انجاز العمل، من هنا حرصت الكثير من المنظمات العامة والخاصة على العناية به، باعتباره أحد الأدوات الأساسية لرفع مستوى الأداء وزيادة الكفاءة الإنتاجية للعاملين للقيام بواجبات أعمالهم والمهام الموكلة إليه على خير وجه، إضافة إلى تهيئتكم لتحمل المزيد من المسؤوليات من خلال زيادة قدراتهم على مواجهة المهام المعقدة في الحاضر والمستقبل [3].

ويعد التدريب الوسيلة الفعلية والتطبيقية الناجحة والمؤثرة التي تكفل الاستفادة من مهارات وتجارب الآخرين من خلال أشخاص مؤهلين على ذلك، والمقصود بالتدريب هنا التدريب الفني وغير التقليدي الذي يكسب الأفراد خبرة فنية عالية في مجال الجريمة الالكترونية، وهذه الخبرة الفنية لا تأتي دون تدريب وتخصصي يراعي فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية لتلقي التدريب، وهنا يكون من السهل تدريب متخصص في تكنولوجيا المعلومات وشبكات الاتصال بدلا

---

[1]– السيد عبد الحميد أحمد، المرجع السابق، ص 136.

[2]– يعرف التدريب بأنه : " نشاط مستمر ومخطط يهدف إلى سد الفجوة بين الأداء الحالي و الأداء المتوقع لشاغل الوظيفة فهو يقوم على أساس تحديد المهارات والقدرات الواجب توفيرها في شاغل الوظيفة، ومن ثم إحداث التغيرات في سلوك وقدرات الفرد أو الجماعة المسؤولة عن أداء هذه الوظيفة " أنظر: صالح محمد النويجم، تقوم كفاءة العملية التدريبية في معاهد التدريب الأمنية بمدينة الرياض من وجهة نظر العاملين فيها، رسالة ماجستير في العلوم الإدارية، جامعة العلوم الأمنية، الرياض، 2005، ص 9.

[3]– يوسف حسن يوسف، المرجع السابق، ص 176.

من تدريب القائمين على تنفيذ القانون كرجال الشرطة، ويذهب بعض الخبراء إلى أنه يجب أن تتوافر لدى المتدرب خبرة لا تقل عن خمس سنوات في المجالات التي لها علاقة بتكنولوجيا المعلومات كالبرمجة وتصميم النظم وتحليلها وإدارة الشبكات وعمليات الحاسب الآلي.[1]

ويجب أن يشمل المنهج التدريبي على بيان المخاطر والتهديدات ونقاط الضعف وأماكن الاختراقات لشبكة المعلومات وأجهزة الحاسب وأيضا ذكر مفاهيم وتعريفات للصفات التي يتميز بها المجرم المعلوماتي والدوافع وراء ارتكاب الجريمة الالكترونية[2].

وفيما يتعلق بمنهج التحقيق فإنه لابد و أن يشتمل على إجراءات التحقيق والتخطيط للتحقيق وتجميع المعلومات وتحليلها، وكذا أساليب المواجهة والاستجواب، ومراجعة النظم الفنية للبيانات وأساليب العمل الجنائي [3].

بالإضافة إلى ذلك لابد وأن يشتمل على ما يتعلق بالتفتيش والضبط وكيفية استخدام الحاسب الآلي كأداة للمراجعة والحصول على أدلة الاتهام وما يخص الملاحقة الدولية والتعاون المشترك.[4]

ويتطلب أن يقوم بالتدريب جهة مختصة ولها الخبرة الكافية في اختيار المتدربين ذوو الخبرة العلمية والفنية والصفات الشخصية المميزة ولابد لعملية التدريب أن تكون مستمرة لأن الجرائم الالكترونية في تطور مستمر وسريع، ولابد أن تسعى الجهات الأمنية التي تكون مسؤولة عن التحقيق أن تستعين بالمختصين والفنين في مجال الحاسب الآلي.[5]

ليس هذا فحسب بل لابد وأن تسعى الأجهزة الأمنية المعنية بالتحقيق إلى استقطاب المتخصصين والكفاءات في المجال المعلوماتي وضمهم إليها ضمن كوادرها والاستفادة منهم كون أن غرس وتطوير الثقافة الحاسوبية وسط رجال القانون والشرطة، وربطها بالثقافة القانونية يكفل الأجهزة الأمنية والسلطات التحقيق النجاح الباهر في مواجهة الجرائم الالكترونية.

---

[1]– غانم مرضي الشمري، المرجع السابق، ص ص 116-117.

[2]– السيد عبد الحميد أحمد، المرجع السابق، ص 140.

[3]– هشام محمد فريد رستم، المرجع السابق، ص 497.

[4]– السيد عبد الحميد أحمد، المرجع السابق، ص 140.

[5]– غانم مرضي الشمري، المرجع السابق، ص 118.

ب مظاهر التعاون الدولي في مجال تدريب رجال العدالة الجنائية.

أجهزة العدالة في الكثير من الدول سيما الدول النامية ليست لديها تلك الجاهزية لمواجهة الجرائم الالكترونية وغيرها من الجرائم المستحدثة، وهذا لعدة أسباب منها الافتقار إلى الموارد الكافية مادية كانت أو بشرية، أو لأن سلطات التحقيق لديها محدودة أو لأنه لديها قوانين ونظم سبقها الزمن أو قد تفتقر لأي قوانين لتتصدى بها لهذه النوعية من الجرائم.

وعليه فلا يمكن لأي دولة النجاح بمفردها في مواجهة هذه الأنماط المستحدثة من الجرائم دون تعاون وتنسيق مع غيرها من الدول، وهنا كانت الدعوة إلى ضرورة وجود تعاون وتنسيق مع غيرها من الدول، وهنا كانت الدعوة إلى ضرورة وجود تعاون دولي ليس فقط في مجال المساعدات القضائية المتبادلة أو في مجال تسليم المجرمين فحسب، وإنما أيضا في مجال تدريب رجال العدالة [1] ،فتدريب الكوادر البشرية القائمة على إنقاذ القانون ليس بنفس المستوى في جميع الدول وإنما يختلف من دولة لأخرى بحسب تقدم الدولة ورقيها، ولو أمعنا النظر في بعض الصكوك الدولية والإقليمية لوجدنا أنها دعت وبصريح النص إلى ضرورة وجود تعاون بين الدول في مجال التدريب ونقل الخبرات فيما بينها، كما هو الحال في المادة 29 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000، والمادة 09 من مشروع الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود.

والتعاون الدولي في مجال تدريب رجال العدالة على مواجهة الجرائم الالكترونية قد يكون بين الدول وأجهزة العدالة لديها، فعلى الصعيد العربي نجد مثلا أن هناك اجتماعات تم عقدها في إطار التنسيق بين المعاهد القضائية العربية لتوفير التأهيل والتدريب المناسبين لأعضاء الهيئات القضائية العربية، وقد تمخضت الاجتماعات عن الاتفاق على إعداد مشروع اتفاقية للتعاون بين المعاهد القضائية العربية تسمى اتفاقية عمان للتعاون العلمي بين المعاهد القضائية العربية والتي وقعت في 9 أبريل 1977.

ففي مصر نجد النيابة العامة تعقد الكثير من الندوات والمؤتمرات وحلقات النقاش وتشارك فيها سواء عقد داخل مصر أو خارجها، بالإضافة إلى إرسال أعضاء النيابة العامة من مختلف الدرجات في

[1]– يقصد بتدريب رجال العدالة تلك العملية التي يخطط لها وتصمم لها البرامج ويبذل لها الجهد والمال وتغيير سلوك العاملين في أجهزة العدالة سواء كانوا من القضاة أو رجال التحقيق والنيابة العامة أو رجال الضبط القضائي، وهذا بهدف رفع مستوى كفاءاتهم ومهاراتهم، للمزيد أنظر: السيد هبد الحميد أحمد، المرجع السابق، ص 144.

مراجع خارجية وذلك بالتعاون مع أجهزة النيابة العامة في الدول الأخرى والهيئات الدولية يهدف الاطلاع على أحدث النظم المقارنة.[1]

والهدف من عقد هذه اللقاءات والندوات تبادل للآراء والخبرات بين المشاركين وتبادل الرأي وطرح الأفكار والتصورات وتشجيع التعاون بين الدول والأطراف أو المعاهدات من أجل مقاومة الجرائم الإلكترونية، كما أنها تفيد المتلقي التدريب عن طريق زيادة مهاراته وخبراته ومعلوماته، وقدراته على التعامل مع الأجهزة الدولية الأخرى، وهذا ما ينعكس على الجهة التي ينتمي إليها بالفائدة.

وتعد الولايات المتحدة الأمريكية من الدول المتقدمة تكنولوجيا والمتطورة تقنيا في مجال مكافحة الجرائم الالكترونية، وعلى الرغم من ذلك فهي تعي وتعلم أنه ما من دولة حتى وإن كانت متقدمة يمكنها التصدي لأخطار هذا النمط المستحدث من الجرائم.

ومن هذا المنطلق نجدها تحرص على توفير المساعدة التقنية والتدريب لرفع قدرات العدالة الجزائية لدى الحكومات الأخرى، ومساعدة ما لديها من أجهزة الشرطة والادعاء العام والقضاة ليصبحوا أكثر فعالية في مكافحة الجريمة، فهذه المساعدة لا تؤدي إلى تسيير بناء إطار للتعاون الدولي في مجال تطبيق القانون وحسب، ولكنها تعزز أيضا قدرة الحكومات الأجنبية المعنية على ضبط مشاكل الجريمة الإلكترونية لديها قبل أن يمتد ليتجاوز حدود بلدانها، فمكتب المساعدة والتدريب على تطوير أجهزة الإدعاء العام في الخارج، التابع لوزارة العدل الأمريكية المكلف تحديدا بتوفير المساعدة اللازمة لتحديد مؤسسات العدالة الجزائية في دول أخرى وتعزيز إدارة القضاء في الخارج [2].

وفي الوقت الحاضر، تقدم وزارة العدل الأمريكية مساعدة لتطوير القطاع القضائي في عدد من البلدان في إفريقيا، وآسيا، وأوروبا الشرقية والوسطى، وأمريكا اللاتينية، والشرق الأوسط مستعينا في ذلك بخبرة الوحدات المختصة، كما نجد أيضا أن أجهزة تطبيق القانون الأمريكية توفر أيضا تدريبا لنظيرتها من الأجهزة في البلدان الأخرى داخل الولايات المتحدة الأمريكية أو خارجها عن طريق إنشاء معاهدة خاصة بالتدريب كما هو الحال في المجر وكوستاريكا، وتايلند، وفي هذه المعاهدة يقوم خبراء أمريكيون في عمل أجهزة تطبيق القانون باطلاع المتدربين على أساليب وسبل مبتكرة للتحقيق، ويشجعون على تبادل الآراء على نظرائهم في مختلف أنحاء العالم.

[1]– غانم مرضي الشمري، المرجع السابق، ص 119.

[2]– المرجع نفسه، ص 120.

وخلاصة القول أنه ما من دولة يمكنها بنجاح مجابهة هذا التحدي في مواجهة هذه الأنماط المستحدثة من الجرائم ومنها الجرائم الإلكترونية بمفردها ولا مناص من مواصلة أجهزة تطبيق القانون في أنحاء العالم وتطوير القدرة على التعاون الدولي، ولا مفر للدول المتقدمة من مساعدة الدول النامية لتعزيز مؤسساتها المتخصصة بالتحري والتحقيق والمحاكمة.

خلاصة الباب الثاني:

لقد امتد تأثير التقنية المعلوماتية إلى الجانب الإجرائي بشكل أوسع مع مرور الوقت كون نصوص القوانين الإجرائية وضعت لتحكم الإجراءات المتعلقة بجرام تقليدية في عالم محسوس خلافا لجريمة التزوير الإلكتروني التي ترتكب في مسرح الكتروني افتراضي ما أثار التساؤل حول صلاحية تطبيق إجراءات التحقيق التقليدية في مكافحة هذه الجريمة.

ولتفادي القصور في النصوص الجزائية الإجرائية القائمة هي مكافحة هذه الجريمة من جهة ،وتفادي إفلات المجرم الإلكتروني من جهة أخرى،بادرت التشريعات في العديد من الدول إلى إعادة النظر في بعض القواعد الإجرائية لاسيما القواعد المتعلقة باستخلاص الدليل الالكتروني كالتفتيش والضبط في مجال البيئة الرقمية ،فضلا عن استحداث قواعد إجرائية حديثة تتلاءم والطبيعة الخاصة لهذه الجريمة،كالمراقبة الإلكترونية واعتراض المراسلات والتسرب الإلكتروني.

وأدى القصور في التشريعات الوطنية وعجز الدول فرادى عن التصدي لجريمة التزوير الإلكتروني والجرائم الإلكترونية عموما إلى جعل المجتمع الدولي يقتنع بأن توحيد جهوده هو الحل الأمثل لمكافحة هدا النوع المستحدث من الإجرام.ومن هنا كان التعاون الدولي بين الدول من أنجع الحلول سواء من خلال إبرام العديد من الاتفاقيات الدولية المبرمة في هذا المجال أو من خلال التعاون الأمني والقضائي.

خاتمة

خاتمة:

تعد جريمة التزوير الالكتروني من الأنماط الإجرامية الجديدة التي فجرتها حديثا ثورة تقنية المعلومات والاتصالات، والتي تعد دراستها من الموضوعات الهامة التي باتت الحاجة إلى دراستها دراسة جيدة ومتأنية، وهذا نظرا لطبيعتها الخاصة والمختلفة تماما عن الجرائم التقليدية، وأنها من المستجدات التي لم تكن معروفة في القانون الجنائي بشقيه الموضوعي والإجرائي.

ولعل أهم ما يميز هذه الجريمة هو سرعة تناميها وتزايد درجة إتقانها، مستفيدة من التطورات المضطردة في مجال تقنيات المعلومات وعولمة المعرفة من خلال شبكة الانترنت التي يحصل من خلالها على معلومات كثيرة ومتجددة في جميع المجالات، وتميزها أيضا أنها جريمة معقدة يتطلب كشفها مجموعة من المهارات والمعارف، إضافة إلى الأجهزة الفنية المعقدة، كما يصعب إثباتها بالطرق الاعتيادية، إذ يتطلب ذلك وجود أجهزة وآلات ذات مواصفات فنية معينة، وبرمجيات خاصة، ومواد مخزنة على تلك الأجهزة لها دلالات محددة.

وترتكب هذه الجريمة عادة في بيئة المعالجة الآلية للبيانات ضد المحررات الالكترونية التي حلت محل المحررات الورقية في كافة مجالات الحياة المختلفة، وهو ما دفع بمجرمي المعلوماتية إلى العبث بمحتواه وتزويرها ما من شأنه إحداث ضرر للغير وتهديد الثقة في التعامل بتلك المحررات، ولهذا بادرت الدول والحكومات إلى أن لا تدخر جهدا في سبيل مكافحة هذه الجريمة وردع الجناة سواء كانت ذلك باستحداث القوانين والتشريعات الحديثة لتساير مثل هذه الجرائم المستجدة، وبتعاون الدول فيما بينها وتضافر الجهود من معلومات وتبادل للخبرات لمساعدة بعضها في مكافحة هذه الجرائم على جميع الأصعدة ومحاولة صياغة إستراتيجية دولية نموذجية لمواجهة هذا المد المتنامي من الإجرام وعلى رأسها جريمة التزوير الالكتروني.

وفي ضوء ما تقدم ثم التوصل إلى النتائج التالية، وتقرير بعض التوصيات تعرض في الآتي:

أولا: نتائج الدراسة

1-تتميز جريمة التزوير الالكتروني بطبيعة خاصة تميزها عن جريمة التزوير التقليدي لأنها تتطلب لارتكابها معرفة تامة بتقنية الحاسب الآلي.

2-يتزايد التزوير في مجال نظم المعالجة الآلية للبيانات بوصفه أحد أنواع الغش المعلوماتي تزايدا سريعا في الفترة الأخيرة في الوقت التي حلت فيه المحررات أو المستندات الالكترونية محل المحررات الورقية.

3-تمكن تصور تغيير الحقيقة في النظام الآلي للمعالجة الآلية بتغيير البيانات أو المعلومات أو حذفها أو إضافتها أو التلاعب فيها بأي صورة سواء كانت هذه البيانات مخزنة أم كانت تمثل جزءا من برامج التشغيل أو برامج التطبيق، ويجب في هذه الحالة أن تكون محلا للتجريم، ولكن ذلك لا ينطبق عليه التزوير المنصوص عليه وذلك لعدم انطباق وصف المحرر على البرنامج أو الأوعية المسجل عليها المعلومات أو العمليات.

4-نظرا لخطورة جريمة التزوير الالكتروني بادرت بعض التشريعات كفرنسا إلى تجريم التزوير في المستندات الالكترونية من خلال تعديل قانون العقوبات ليشمل التزوير كل تغيير في محرر كتابي أو أي دعامة أخرى ليدخل في طياته المحرر أو المستند الالكتروني.

5- ذهبت بعض التشريعات إلى تجريم التزوير الالكتروني باستحداث نصوص خاصة كقانون التوقيع الالكتروني المصري، وقانون المعاملات الالكترونية الإماراتي، أما المشرع الجزائري فإنه لم ينص على تجريم التزوير الالكتروني في قانون العقوبات على الرغم من اعترافه بحجية المحررات الالكترونية في الإثبات، كما لم يتطرق إلى تجريمه بمناسبة تعديل قانون العقوبات لعام 2004 عند نصه على الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، إلا أنه جرم التزوير الواقع على سواء السفر البيومتري، كما نص على تجريم تزوير بطاقات الشفاء الالكترونية، ناهيك عن تجريم التزوير الواقع على التوقيع الالكتروني بموجب قانون التوقيع والتصديق الالكترونيين.

6- إصدار القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتجريمه لأي جريمة ترتكب بواسطة المنظومة المعلوماتية، إلا أنه لم ينص على تجريم التزوير الالكتروني، إلا أنه استوعب أي جريمة الكترونية.

7-ضمانا لتفادي إفلات المجرم الالكتروني من العقاب والمتابعة الجزائية، بادر المشرع في الكثير من الدول إلى إعادة النظر في بعض القواعد الإجرائية المتعلقة باستخلاص الدليل كالتفتيش والضبط في البيئة الرقمية، فضلا عن استحداث قواعد اجرائية تتلاءم مع الطبيعة الخاصة لهذه الجرائم، كالمراقبة الالكترونية واعتراض المراسلات والتسرب الالكتروني، والتي جاء بها القانون (04/09) المتعلق بالقواعد

الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتعديل قانون الإجراءات الجزائية لسنة 2006.

8-إذا كانت أغلب التشريعات المعاصرة قد ركزت اهتمامها على الاعتراف للفرد بحقه في سرية المراسلات باعتباره حق دستوري، إلا أنه الإجراءات الجديدة لاستخلاص الدليل الالكتروني تشكل خطرا كبيرا يهدد الحق في الخصوصية، إلا أن المشرع حرص كل الحرص على حصر اللجوء إلى هذه الإجراءات في الحالات التي تستدعي ضرورة التحقيق، كما أحاطها بجملة من الضمانات القانونية التي يتعين على المحقق احترامها عند استعماله لهذه الإجراءات.

9-وقد أظهرت الدراسة أنه من بين المشكلات التي تواجه سلطات البحث والتحقيق ما يتعلق بالقيمة القانونية للدليل الالكتروني، ومدى قبول هذه الأدلة من طرف القاضي الجزائي، كون عملية استخلاص هذه الأدلة سواء بالطرق التقليدية أو المستحدثة تعترضها العديد من الصعوبات نظرا لطبيعة الدليل حد ذاته، أو لصعوبة التعامل معه.

10-يستدعي البعد الدولي لجريمة التزوير الالكتروني والجرائم الالكترونية عموما أن يتم تعزيز التعاون الدولي، فمكافحة هذا النوع من الإجرام يقتضي في غالب الأحيان التدخل السريع لمد الإجراءات إلى أنظمة معلوماتية خارج الدولة.

11-توصلنا إلى أن من بين الجهود الدولية لمواجهة الجريمة محل الدراسة مؤتمر هيئة الأمم المتحدة، واتفاقية بودابست لمكافحة إجرام الفضاء المعلوماتي، وعلى الصعيد العربي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

12-تعددت مظاهر وصور التعاون الدولي لمكافحة هذه الجريمة من تعاون أمني دولي عبر أجهزة متنوعة على الصعيدين الدولي المتمثلة في الانتربول، والإقليمي عن طريق جهاز الأوروبول، وإنشاء مجلس وزراء الداخلية العرب على الصعيد العربي، وتلعب هذه الأجهزة دورا فعالا في مكافحة هذه الجريمة وضبط الجناة، إضافة إلى التعاون القضائي الدولي المتمثل في المساعدة القضائية والتي تشمل تبادل المعلومات ونقل الإجراءات أو تبادل الإنابة القضائية وتسليم المحرمين.

13-بالموازاة مع ذلك اتضح أن هذه الجهود تتخللها عقبات كثيرة، يعود البعض منها إلى الطبيعة الخاصة لهذه الجرائم، فالطابع العابر للحدود التي تتسم به يثير العديد من المشاكل القانونية، لاسيما

مشكلة احترام سيادة الدولة التي تقف حاجزا أمام سلطات التحقيق، خاصة إذا اقترن ذلك بغياب آليات فعالة تضمن التعاون القضائي والأمني بين الدول في هذا المجال.

ثانيا:التوصيات

على ضوء النتائج المتوصل إليها، تمكننا أن نقدم جملة من الحلول التي نعتقد أنها فعالة وممكنة التجسيد، والتي أردنا أن تعرضها في شكل اقتراحات سواء على الصعيد الوطني أو الدولي:

1-يتعين على الدول التي لم تسن بعد قوانين جزائية موضوعية وإجرائية خاصة بالجرائم الالكترونية، الإسراع إلى تعديل وترشيد قوانينها القائمة، وذلك لتفادي القصور التشريعي وتخطي الثغرات القانونية الحاصلة في هذا المجال حتى لا يفلت المجرم الالكتروني من المتابعة الجزائية والعقاب.

2-يجب أن تبادر الدول إلى عقد الاتفاقيات الثنائية التي يكون من شأنها تنظيم مسألة التعاون القضائي بينها، فضلا عن عقد الاتفاقيات الجماعية سواء على المستوى العالمي أو الإقليمي أو العربي.

3-ضرورة تكثيف التعاون والتنسيق الدولي بين الدول من أجل تطوير وتوحيد التشريعات الجزائية الموضوعية والإجرائية التي تعنى بمكافحة الجرائم الالكترونية، وهذا من خلال تبني إجراءات التحقيق والمتابعة الجزائية السريعة والمناسبة، وخلق قنوات اتصال ثنائية أو متعددة الأطراف تسمح للسلطات القائمة بالتحقيق الاتصال بسهولة بنظريتها الأجنبية والتنسيق معها، أو التدخل السريع للتحقيق في إقليم دولة أجنبية دون أن يشكل ذلك مساسا بسيادة هذه الدولة.

4-إنشاء وحدة أمن وأجهزة قضائية متخصصة في مكافحة الجرائم الالكترونية، يكون لهم الإلمام الكافي بالجوانب التقنية والفنية لمتابعة هذه الجرائم، مع اخضاعهم لبرامج تدريبية خاصة، تساعدهم على تحديث معارفهم وإطلاعهم بآخر المستجدات الحاصلة في مجال المعلوماتية.

5-يستحب اتخاذ اتفاقية بودابست لسنة 2001 حول مكافحة الإجرام المعلوماتي أساسا لعقد الاتفاقيات الثنائية والجماعية بين الدول كونها تتضمن تنظيما ومعالجة جديدة لهذه الجرائم في جوانبها الموضوعية والإجرائية.

6-ضرورة أن يضمن المشرع الجزائري جريمة التزوير الالكتروني بما يتماشى مع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

7–ضرورة إضافة مادة إلى قانون العقوبات الجزائري بما يطابق نص المادة 1/441 من قانون العقوبات الفرنسي ليشمل إلى جانب تجريم تزوير المحررات الورقية تزوير المحررات الالكترونية أيضا.

8–ضرورة النص على جريمة التزوير الالكتروني في القانون 04/09 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حتى نضمن مواجهة جريمة التزوير بالقواعد الإجرائية المستحدثة والمنصوص عليها في هذا القانون.

9–ضرورة اهتمام الباحثين ورجال القانون الجزائريين بالدراسات القانونية التي تعنى بالجوانب الإجرائية للجرائم الالكترونية، والعمل على إثراء محتواها، لأنها لم تنل بعد حظها من البحث، ولا تزال لحد اليوم في منطقة الظل في بلادنا رغم ما يثيره الزحف الهائل للإجرام الالكتروني من مخاطر.

وفي الختام، فإنني لا أزعم من خلال بحثي هذا بلوغي جادة الصواب، ولكن أملي أن يحقق قدر من العزم منه، وما أنا إلا بشر اجتهد فأخطأ وأصاب، فإن أصبت فأجري على الله وإن أخطأت فأدعوه ألا يحرمني أجر المجتهدين ولله الأمر من قبل ومن بعد، والحمد لله رب العالمين.

قائمة المصادر والمراجع

قائمة المصادر والمراجع باللغة العربية

أولا :النصوص القانونية

أ الدساتير:

1- الدستور الجزائري الصادر بموجب المرسوم الرئاسي 96 /438 المؤرخ في 7 ديسمبر سنة 1996 المعدل بموجب المرسوم الرئاسي 20- 442 المؤرخ في30 ديسمبر 2020 المتضمن التعديل الدستوري، الجريدة الرسمية، العدد 82 المؤرخة في30 ديسمبر 2020.

ب- الاتفاقيات والمواثيق الدولية:

1- الاتفاقية العربية لمكافحة تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010
2- اتفاقية بودابست، المتعلقة بإجرام الفضاء الالكتروني الموقعة في 23 نوفمبر 2001.
3- الاتفاقية الأوروبية حول الجرائم المعلوماتية.
4- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية باليرمو عام 2000 .
5- القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها المعتمد من طرف مجلس وزراء العدل بتاريخ 08 أكتوبر 2003 ومجلس وزراء الداخلية العرب بتاريخ 21 أفريل 2004.

ج- القوانين العادية:

1- الأمر رقم 155/66 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بموجب الأمر 20- 04 المؤرخ في 30 غشت 2020، الجريدة الرسمية للجمهورية الجزائرية ، العدد 51، الصادرة بتاريخ 31 غشت 2020.

2- الأمر 156/66 المؤرخ 08 يونيو 1966 المتضمن قانون العقوبات، المعدل والمتمم بموجب الأمر 21- 08 المؤرخ في 08 يونيو 2021 ، الجريدة الرسمية للجمهورية الجزائرية، العدد 45، الصادرة بتاريخ 09 يونيو 2021.

3- الأمر 59/75 المؤرخ في 26 سبتمبر 1975 المتضمن القانون التجاري الجزائري، المعدل والمتمم.

4- القانون 03/2000 المؤرخ في 05 أوت 2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات، الجريدة الرسمية رقم 48 المؤرخة في 08أوت 2000.

5- القانون06 /01 المؤرخ في 20 فبراير 2006، المتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية العدد 14، الصادرة بتاريخ 08 مارس 2006.

6- القانون 06/06 المؤرخ في 2006/02/20، المتضمن تنظيم مهنة الموثق، الجريدة الرسمية الصادرة بتاريخ 2006/03/08 العدد 14 .

7- القانون 03/06 المؤرخ في 2006/02/20، المتضمن تنظيم مهنة المحضر القضائي الجريدة الرسمية المؤرخة في 08 مارس 2006، العدد 14.

8- الأمر 03/06 المؤرخ في 19 جمادى الثانية عام 1427، الموافق لـ15 يوليو 2006، الجريدة الرسمية عدد 496 الصادرة بتاريخ 20 جمادى الثانية 1427 الموافق لـ 16 يوليو2006المتضمن القانون الأساسي للوظيفة العامة .

9- القانون 01/08 المتمم للقانون 11/83 المؤرخ في 15 محرم 1429 الموافق ل 23 يناير 2008 المتمم للأمر 11/83 المؤرخ في 21 رمضان1403 الموافق ل 02 يوليو 1983 المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية الصادرة بتاريخ 19 محرم 1429 الموافق ل 27 يناير 2008.

10- القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية الجزائرية، العدد47، المؤرخة في 25 شعبان 1420الموافق ل 16 غشت 2009.

11- القانون 07/13 المؤرخ في 29 أكتوبر 2013 المتضمن تنظيم مهنة المحاماة، الجريدة الرسمية الصادرة بتاريخ 30 أكتوبر 2013، العدد 55.

12- القانون 03/14 المؤرخ في 24 ربيع الثاني 1435 الموافق لـ 24 فبراير 2014 المتعلق بسندات ووثائق السفر، الجديدة الرسمية، العدد 16، الصادر بتاريخ 21 جمادى الأولى 1435 الموافق لـ 23 مارس 2014.

13- القانون 15/ 12 المؤرخ في 15 يوليو 2015، المتعلق بحماية الطفل، الجريدة الرسمية رقم 39 المؤرخة في 19 جويلية 2015.

د- المراسيم

المراسيم الرئاسية:

1- المرسوم الرئاسي رقم 183/04 المؤرخ في 8 جمادى الأولى عام 1425 هـ الموافق لـ 26 جوان 2004 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام وتحديد قانونه الأساسي، الجريدة الرسمية للجمهورية الجزائرية، العدد 41 الصادرة في 27 جوان 2004.

2- المرسوم الرئاسي رقم 15- 261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 53 لسنة 2015.

المراسيم التنفيذية:

1- المرسوم رقم 14- 183 المؤرخ في 13 شعبان 1435 الموافق لـ 11 يونيو سنة 2014، المتضمن إنشاء مصلحة القضائي لمديرية الأمن الداخلي بدائرة الاستعلام والأمن ومهامها وتنظيمها، الجريدة الرسمية للجمهورية الجزائرية، العدد 32، الصادر في 12 يونيو 2014.

- 2- المرسوم التنفيذي 348/06 المؤرخ في 05 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ، الجريدة الرسمية للجمهورية الجزائرية المؤرخة في 08 أكتوبر 2006.

هـ- القوانين العربية:

1- القانون الاتحادي رقم 02 لسنة 2006 المعدل، بشأن مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة.

2- قانون التوقيع المصري وإنشاء هيئة صناعة تكنولوجيا المعلومات رقم لسنة 2004.

3- قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات لسنة 2006 .

4- قانون المبادلات والتجارة الالكترونية التونسي

5- قانون التوقيع الالكتروني وخدمات الشبكة في سوريا.

6- قانون العقوبات اللبناني.

ثانيا:الكتب :

1- إبراهيم حامد طنطاوي، المسؤولية الجنائية عن جرائم التزوير في المحررات- فقها وقضاء، الطبعة الأولى، المكتبة القاهرية، مصر، 1995.

2- إبراهيم طنطاوي، المسؤولية الجنائية عن جرائم التزوير في المحررات، الطبعة الأولى، المكتبة القانونية، ، مصر، 1995.

3- أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، مصر، 2006.

4- أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الطبعة الأولى، ديوان المطبوعات الجامعية، الجزائر، 1999.

5- أحمد فتحي سرور، الشرعية الدستورية وحقوق الإنسان في الإجراءات الجنائية، دون طبعة، دار النهضة العربية، مصر، 1995، .

6- أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، الجزء الأول، الطبعة الخامسة، ، دار النهضة العربية، مصر، 1981.

7- أحمد فتحي سرور، الوسيط في قانون العقوبات ، القسم الخاص، دون طبعة ، دار النهضة العربية، مصر، 2013.

8- أحمد محمود خليل، جرائم تزوير المحررات دون طبعة، المكتب الجامعي الحديث، مصر، 2008.

9- ادوارد غالي الذهبي، المسؤولية الجنائية للشخص المعنوي، الطبعة الأولى، دار النهضة العربية، مصر، 1978.

10- أسامة سمير حسين، الاحتيال الالكتروني الوجه القبيح للتكنولوجيا، الطبعة الأولى، دار الجنادرية للنشر والتوزيع، الأردن، 2011.

11- أمجد قطيفان الخربشة، جريمة غسيل الأموال، دراسة مقارنة، الطبعة الأولى، دار الثقافة ، لبنان، 2006.

12- أمين طغباش، الحماية الجنائية للمعاملات الالكترونية، الطبعة الأولى ، مكتبة الوفاء القانونية ، مصر، 2015.

13- إيهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، الطبعة الأولى، دار الجامعة الجديدة، مصر، 2008.

14- بكري يوسف، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، مصر، 2011.

15- جلال ثروت، تطور الإجراءات الجنائية، دون طبعة، دار الجامعة الجديدة، الإسكندرية مصر، 2003.

16- جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع ، الأردن، 2010.

17- جمال نجيمي، جرائم التزوير في قانون العقوبات الجزائري، دون طبعة، دار هومة، الجزائر، 2013.

18- جميل عبد الباقي الصغير، شرح قانون العقوبات – القسم العام – دون طبعة دار النهضة العربية، مصر، 2000.

19- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، الطبعة الأولى، دار النهضة العربية، مصر، 2002.

20- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة دراسة مقارنة ، دون طبعة، دار النهضة العربية، مصر، 2002.

21- حازم نعيم الصمادي، المسؤولية في العمليات المصرفية الالكترونية، الطبعة الأولى، دار وائل، الأردن، دون سنة نشر.

22- حسن بوسقيعة، الوجيز في القانون الجزائي الخاص – الجرائم ضد الأشخاص والجرائم ضد الأموال، الجزء الأول، الطبعة السابعة، دار هومة، الجزائر، 2007.

23- حسن صادق المرصفاوي، أصول الإجراءات الجنائية في القانون المقارن، دون طبعة، دار الفكر العربي، مصر، 2006.

24- حسن طاهر داود، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، 2000.

25- حسين المحمدي، الإرهاب الدولي تجريما ومكافحة ، الطبعة الأولى، دار المطبوعات الجامعية، مصر 2007، سليمان عبد المنعم، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين، دراسة مقارنة، دار الجامعة الجديدة للنشر، مصر، 2007.

26- حنان ريحان المضحكي، الجرائم المعلوماتية – دراسة مقارنة – الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2014.

27- خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009.

28- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، دار الفكر الجامعي، الجزائر 2009.

29- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دون طبعة، دار الهدى، الجزائر، 2010.

30- رشيدة بوكر، جرائم الاعتداء على نظام المعالجة الآلية للمعطيات، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012 .

31- رمزي رياض عوض، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى، دار النهضة العربية، مصر، 2010.

32- رمسيس بنهام، الجرائم المضرة بالمصلحة الجامعة دون طبعة، منشأة المعارف الإسكندرية، مصر، 1986.

33- زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي دون طبعة، دار الهدى، الجزائر 2011.

34- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم عبر شبكة الانترنت، الطبعة الأولى، دار النهضة العربية 1999، مصر.

35- سليمان احمد إبراهيم، القواعد الجنائية للجريمة المنظمة والتعاون الدولي في سبيل مكافحتها، دون طبعة، دار الكتاب الحديث، مصر، 2008.

36- سليمان أحمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام الشبكة المعلومات الدولية ، دار النهضة العربية، مصر، 2013.

37- السيد عبد الحميد أحمد ، جرائم الشبكة العنكبوتية وغسل الأموال في إطار الملاحقة الأمنية والقضائية الدولية، الطبعة الأولى، مكتب الوفاء القانونية، مصر 2018.

38- شريف الطباخ، التزوير والتزييف في ضوء الفقه والقضاء، الطبعة الثانية، المركز القومي للإصدارات القانونية، مصر، 2006.

39- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، الطبعة الأولى، دار الجامعة الجديدة، مصر، 2007.

40- ضياء علي أحمد النعمان، الغش المعلوماتي، الظاهرة والتطبيقات، الطبعة الأولى، المطبعة العربية، المملكة العربية، 2011 .

41- عامر محمود الكسواني، التزوير المعلوماتي للعلامة التجارية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2010.

42- عايد رجا الخلايلة، المسؤولية التقصيرية الإلكترونية- المسؤولية، الناشة عن إساءة اِستخدام أجهزة الحاسوب والانترنت- دراسة مقارنة ، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2009.

43- عباس العبودي، تحديات الإثبات بالمستندات الإلكترونية، الطبعة الأولى، منشورات الحلبي الحقوقية لبنان، 2011 .

44- عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الفكر القانونية، مصر، 2006.

45- عبد الرحمان خلفي، محاصرات في قانون الإجراءات الجزائية، الطبعة الأولى، دار الهدى، الجزائر، 2012.

46- عبد الرحمن عبد الله حميد آل علي، جرائم التزوير المعلوماتية، الطبعة الأولى، دون ذكر دار النشر، دون مكان، 2009.

47- عبد العزيز سعد، أصول الإجراءات أمام محكمة الجنايات، دون الطبعة، دار هومة للطباعة والنشر والتوزيع، الجزائر 2010.

48- عبد العزيز سعد، جرائم التزوير وخيانة الأمانة واستعمال المزور، الطبعة السادسة، دار هومة، الجزائر، 2013.

49- عبد الفتاح بيومي حجازي، الحكومة الالكترونية، الكتاب الثاني، الطبعة الأولى، دار الفكر الجامعي الإسكندرية، مصر، 2008 .

50- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم التزوير والانترنت، دون طبعة، دار الكتب القانونية، مصر، 2008 .

51- عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنت في التشريعات العربية، الطبعة الأولى، دار النهضة العربية، مصر، 2009.

52- عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنت في القانون العربي النموذجي، الطبعة الأولى، دار النهضة العربية، مصر 2009.

53- عبد الله بن عبد العزيز، التفتيش في الجرائم المعلوماتية في النظام السعودي، دراسة تطبيقية، دون طبعة، جامعة نايف العربية للعلوم الأمنية، السعودية، 2011.

54- عبد الله بن مسعود محمد السبراني، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الالكتروني، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011.

55- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت الجرائم الالكترونية، دون طبعة، منشورات الحلبي الحقوقية، لبنان، 2007.

56- عبد المالك، الموسوعة الجنائية، الجزء الثاني، الطبعة الأولى، لبنان، 2005/2004.

57- عدنان الخطيب، موجز القانون الجزائي، الكتاب الأول، المبادئ العامة في قانون العقوبات دون طبعة، مطبعة جامعة دمشق، سوريا، 1963.

58- علاء عبد الباسط خلاف، الحماية الجنائية للحاسب الالكتروني والانترنت، الطبعة الثانية، معهد الكويت للدراسات القضائية والقانونية، الكويت، 2008.

59- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دون طبعة، منشاة المعارف، مصر، 2011.

60- عمر بن يونس، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي، دون طبعة، دون دار نشر، 2006.

61- عوض محمد عوض، قانون الإجراء الجنائي، الجزء الأول، دون طبعة، مؤسسة الثقافة الجامعية، مصر، 2005.

62- غانم مرضى الشمري، الجرائم المعلوماتية، الطبعة الأولى، الدار العلمية للنشر والتوزيع، الأردن، 2016.

63- غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر والقانون، مصر 2013.

64- غنية باطلي، الجريمة الالكترونية، دون طبعة، الدار الجديدة، الجزائر، 2015.

65- فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية – دراسة مقارنة – دون طبعة، منشورات الحلبي الحقوقية، لبنان، 2003.

66- فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص وفقا لأحدث التعديلات، الطبعة الثالثة، دار النهضة العربية، مصر، 2012.

67- محمد إبراهيم سعد النادي، جرائم الانترنت بين الشريعة الإسلامية والقوانين الوضعية – دراسة مقارنة- الطبعة الأولى، مكتبة الوفاء، مصر، 2017.

68- محمد أبو العلا عقيدة، الاتجاهات الحديثة في قانون العقوبات الفرنسي الجديد، د.ط، دار النهضة العربية، مصر، 2004.

69- محمد أبو العلاء عقيدة، مراقبة المحادثات التلفونية، دراسة مقارنة، دون طبعة، دار النهضة العربية، 2008.

70- محمد أحمد وقيع الله، أساليب التزييف والتزوير وطرق كشفها، الطبعة الأولى، دار الأكاديميون للنشر والتوزيع، الأردن، 2014.

71- محمد الأمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى ، مركز البحوث والدراسات والبحوث ، السعودية2004.

72- محمد الأمين البشري، محسن أحمد، معايير الأمم المتحدة في مجال العدالة الجنائيين ومنع الجريمة، دون طبعة، أكاديمية نايف للعلوم الأمنية، السعودية، 1998.

73- محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2004.

74- محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دون طبعة، دار المطبوعات الجامعية مصر، 2004.

75- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة السادسة، دار هومة للطباعة والنشر والتوزيع، الجزائر 2011.

76- محمد زكي أبو عامر، شرح قانون العقوبات القسم الخاص، دون طبعة، دار الجامعة الجديدة، مصر، 2015.

77- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، مصر، 1998.

78- محمد علي العريان، الجرائم المعلوماتية، الطبعة الأولى، دار الجامعة الجديدة للنشر، مصر، 2004.

79- محمد عوض، الجرائم المضرة بالمصلحة العامة، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، مصر. 1984.

80- محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية، الطبعة الأولى، مكتبة الوفاء القانونية، مصر، 2014.

81- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة، الأردن، 2005.

82- محمود نجيب حسني، جرائم الاعتداء على الأموال، دون طبعة، دار النهضة العربية، مصر، 1992.

83- محمود نجيب حسني، شرح قانون الإجراءات الجزائية وفقا لأحدث التعديلات التشريعية، الجزء الثاني، دون طبعة، دار النهضة العربية، مصر، 2013.

84- محمود نجيب حسني، شرح قانون العقوبات وفقا لأحدث التعديلات التشريعية، الجزء الثاني، دون طبعة، دار النهضة العربية، مصر، 2013.

85- مفيد نايف الدليمي، غسيل الأموال في القانون الجزائي، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2006.

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

87- نادية دردار، الجهود الدولية لمكافحة الجريمة، الطبعة الأولى، المركز القومي للإصدار القانونية، مصر، 2017.

88- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفطر الجامعي، مصر، 2007.

89- نائلة قورة، جرائم الحاسب الآلي، الطبعة الأولى، دار النهضة العربية، مصر، 2004.

90- نبيل صقر، الوسيط في الجرائم المخلة بالثقة العامة، دون طبعة، دار الهدى، الجزائر، 2015.

91- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، الطبعة الأولى ، دار الفكر الجامعي، مصر ، 2007.

92- نزيه نعيم شلالا، دعاوى التزوير واستعمال المزور، دون طبعة، منشورات الحلبي الحقوقية، لبنان 2002.

93- نعيم مغبغب، مخاطر المعلوماتية والانترنت، منشورات الحلبي الحقوقية، دون طبعة، لبنان، 2008.

94- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، الأردن، 2010 .

95- هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، الطبعة الأولى، دار النهضة العربية، مصر، 2012.

96- هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، دون طبعة، مكتبة الآلات الحديثة، مصر، 1994

97- هلالي عبد الله أحمد، الجوانب الموضوعية لجرائم المعلوماتية على اتفاقية بودابست دون طبعة، دار النهضة العربية، القاهرة، 2006 .

98- هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، مصر، 1999 .

99- هلالي عبد الله أحمد، تفتيش نظم الحاسب ونظم الحاسب وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، مصر، 1997.

100- هلالي عبد الله أحمد، جرائم المعلوماتية عابرة الحدود، الطبعة الأولى، دار النهضة العربية، مصر، 2007.

101- هلالي عبد الله، شرح قانون العقوبات البحريني- القسم الخاص، الطبعة الأولى، منشورات جامعة البحرين، 2007 .

102- وسيم شفيق الحجاز، الإثبات الالكتروني، مكتبة صادر ناشرون، دون ذكر مكان ، 2002.

103- يوسف حسن يوسف، الجرائم الدولية للانترنت، المركز القومي للإصدارات القانونية، مصر، 2011.

ثالثا: الأطروحات والمذكرات:

1- ابراهيم الغماز، الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه (منشورة) عالم الكتب، القاهرة 1980.

2- ابراهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص قانون جامعة مولود معمري، تيزي وزو، الجزائر، 2018.

3- براهيمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة بسكرة، الجزائر 2015.

4- الهام بن خليفة، الحماية الجنائية للمحررات الالكترونية من التزوير، أطروحة دكتوراه علوم، جامعة الحاج لخضر، باتنة، الجزائر، 2016.

5- بن قارة مصطفى عائشة، الحماية الجنائية للحكومة الالكترونية، دراسة مقارنة، أطروحة دكتوراه، تخصص قانون عام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2017- 2018.

6- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة المقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2007.

7- حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه علوم جامعة الحاج لخضر، باتنة، الجزائر، 2016

8- السيد محمد سعيد عتيق، النظرية العامة للدليل العلمي في الإثبات الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 1993.

9- عبد الرحمان عبد الله حميد آل علي، جرائم التزوير المعلوماتية، رسالة مقدمة لنيل شهادة الماجستير، أكاديمية شرطة دبي، دون تاريخ.

10- عبد الرحمان محمد بحر، معوقات التحقيق في جرائم الانترنت – دراسة مسحية على ضباط الشرطة بمنطقة البحرين، رسالة ماجستير في العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض 1992.

11- عزة محمود، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب الآلي، أطروحة دكتوراه، كلية الحقوق، مصر 1994.

12- محمد كمال عبد السميع شاهين، الجوانب الإجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي – دراسة مقارنة، أطروحة دكتوراه، تخصص قانون جنائي، كلية الحقوق، جامعة حلوان، مصر، 2015.

13- نبيلة هبة هروال، جرائم الانترنت – دراسة مقارنة – أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2014.

14- ياسر محمد الكومي محمد أبو حطب، الحماية الجنائية والأمنية للتوقيع الالكتروني في التشريع المصري والتشريعات المقارنة، أطروحة دكتوراه كلية الحقوق، جامعة حلوان، مصر، 2013.

رابعا- المقالات والأبحاث:

1- أسامة بن غانم العبيدي، الجهود الدولية في مكافحة الجريمة المعلوماتية، مجلة الحقوق العدد4، الكويت 2015.

أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، مجلة البحوث الأمنية المجلد 29، جامعة نايف للعلوم الأمنية، السعودية، العدد 58، 2019

2- أشرف توفيق شمس الدين، حجية المحررات الالكترونية في الإثبات، ورقة عمل مقدمة في ندوة المعاملات القانونية الالكترونية وعقود التجارة الالكترونية، دبي، 2007.

3- إسماعيل عبد النبي شاهين، أمن المعلومات في الانترنت، بحث مقدم إلى المؤتمر القانون والكومبيوتر والانترنت، كلية الشريعة والقانون الإمارات العربية المتحدة، 2000.

4- بن حديد سامية، الحماية الجنائية لبطاقات الدفع من جرائم التزوير في القانون الجنائي الجزائر، مجلة دراسات، جامعة الأغواط، الجزائر، 2017، العدد57.

5- بوحنة محمد، التعاون العربي في مجال الإعلام الأمني، مجلة الشرطة الجزائرية العدد 100، 2011، ص ص 70، 71. للمزيد اطلع على الموقع الالكتروني للمديرية العامة للأمن الوطني المتاح على الرابط www.dagsm.dz تاريخ الاطلاع: 13/06/2018.

6- جون فرانسوا هركوت، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، بحث مقدم ضمن أعمال الندوة الإقليمية حول جرائم المتصلة بالكومبيوتر، الفترة ما بين 19- 20 يونيو 2007، الدار البيضاء المملكة المغربية، ص 101 منشور على الموقع الالكتروني http// undp- pogar- org/localuser/ progarp/ rule of / cybercrime - 09 pdf.

7- حسين بن سعيد الغافري للتحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، ص .19 مقال منشور على الموقع، www.eastlws.Com

8- حلاب منير، دور الدرك الوطني في ميدان محاربة الجرائم المعلوماتية، الملتقى الوطني حول الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها يومي 16- 17 نوفمبر 2015 كلية الحقوق، جامعة بسكرة، الجزائر.

9- دعاء هاني السيد، الإثبات الجنائي في الجرائم الالكتروني، بحث مقدم للمركز القومي للبحوث الاجتماعية والجنائية، البرنامج التدريبي للكشف عن الجريمة بالوسائل العلمية الحديثة الدورة 62، الفترة من 2010/04/18 إلى 2017/07/15.

10- راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، مجلة "كلية الحقوق للبحوث القانونية والاقتصادية، العدد الأول، دار الجامعة الجديدة، مصر ، 2008.

11- زكي زكي أمين حسونة، جرائم الكمبيوتر الجرائم الأخرى في مجال التكتيك المعلوماتي بحث مقدم للمؤتمر السادس للقانون الجنائي المنعقد بالقاهرة في الفترة من 25 إلى 28 أكتوبر 1993.

12- عبد الرحمان حملاوي، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، بحث مقدم إلى أعمال الملتقى الوطنية حول الجريمة المعلوماتية بين الوقاية والمكافحة، يوم 16- 17 نوفمبر 2015، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر.

13- عبد الرحمان خليفي، إسناد المسؤولية الجزائية للشخص المعنوي في جرائم الأموال، مراحله في إطار فعاليات الملتقى الوطني الأول حول جرائم المالية في ظل التحولات الاقتصادية والتعديلات التشريعية، وقسم العلوم القانونية والإدارية، جامعة 08 ماي 1945 ، قالمة، الجزائر، يومي 24، 25 أفريل، 2007.

14- عبد القادر الفتوح، المسرح الالكتروني، بحث منشور على شبكة الانترنت :

http://writers- abridh.com,sa/kpage.asp§art=7753

https://www.usdoj.gov/criminal/cybercrime/cyber.Htm

15- عبد الله حسين محمود، إجراءات جمع الأدلة في الجريمة المعلوماتية، مؤتمر حول الجوانب القانونية والأمنية للعمليات الالكترونية، دبي، 2003.

16- عبد المجيد جباري، عملية تعديل قانون الإجراءات الجزائية بين الإثراء التشريعي والتطبيق القانوني، مجلة المفكر البرلماني، العدد 21، 2008 .

17- عبد الناصر محمد محمود فرغلي، عبيد سيف سعيد، ورقة بحث مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الإثبات الجنائي بالأدلة الرقمية من الناحية القانونية والفنية، دراسة تطبيقية مقارنة، الرياض، الفترة من 12 إلى 14 /2007/11.

18- علي حسن أحمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، بحث منشور على الموقع الالكتروني لمركز الإعلام الأمني، أكاديمية الشرطة البحرينية، مملكة البحرين، أفريل 2011، ص 186، الرابط الالكتروني :

www.policemc.gov,bh/reports/2011arpril1-4- 2011/634372714052376622.pdf

19- علي حسن أحمد الطوالبة، مشروعية الدليل الالكتروني المستمد من التفتيش، بحث منشور على الموقع الالكتروني لمركز الإعلام الأمني، أكاديمية الشرطة البحرينية، مملكة البحرين، 2011 تاريخ الإطلاع 2017/12/17 موجود على الرابط

www.policemc.gov,bh/reports/2011/april/13.2011/634383168746341770.pdf

20- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية المجلة القانونية التونسية، مركز النشر الجامعي، تونس، 2009.

21- علي كحلون، الجريمة المعلوماتية، وتوجهات محكمة التعقيب، مجلة الأخبار القانونية، تونس، السنة السابقة عدد 127/126، جانفي 2012.

22- علي محمود علي محمود، الأدلة المحصلة من الوسائل الالكترونية في إطار نظريات الجنائي بحث مقدم إلى المؤتمر العلمي حول الجوانب القانونية للمعلومات الالكترونية، الإمارات العربية المتحدة، 2003.

23- عماد بوخرص وحسني غديرة، جرائم الإعلامية في القانون المقارن، الملتقى الجهوي لجرائم الإعلامية، المعهد الأعلى للقضاة، تونس، 2001.

24- فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجنائية، مجلة العلوم الإنسانية جامعة منتوري، قسنطينة، الجزائر، العدد 33، جوان 2010.

25- محمد أمين البشري : التحقيق في جرائم الحاسب الآلي والانترنت، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، العدد 30، جامعة نايف العربية للعلوم الأمنية، الرياض 1431 هـ.

26- محمد أمين البشري، التحقيق في الجرائم المستحدثة، المجلة العربية للدراسات الأمنية والتدريب، العدد ثلاثون، السعودية، 2000.

27- محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، الطبعة الثالثة، كلية الشريعة والقانون، الإمارات العربية المتحدة الفترة من 1 إلى 3 ماي 2004.

28- محمد عوض محمد، مشكلات السياسة الجنائية المعاصرة من جرائم نظر المعلومات، بحث مقدم إلى مؤتمر القانون الكومبيوتر والانترنت، الفترة من 1- 3 مايو 2000، كلية الشريعة والقانون، الإمارات العربية المتحدة.

29- محمد محدة، المسؤولية الجنائية للشخص المعنوي، مجلة المفكر جامعة محمد خيضر، العدد الأول، بسكرة، الجزائر، 2000.

30- محمد محدة، السلطة التقديرية للقاضي الجنائي، مجلة البحوث، المركز الجامعي الوادي، الجزائر، العدد الأول، 2004.

31- محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، المؤتمر السادس للجمعية المصرية للقانون الجنائي حول مشكلات السياسة الجنائية في مجال الجرائم الواقعة على البيئة والجرائم الواقعة في مجال تكنولوجيا المعلومات، المنعقد في الفترة ما بين 25- 28 أكتوبر 1998، مصر، دار النهضة العربية، مصر، 1993.

32- محمد مزوالي، المسؤولية الجنائية للأشخاص المعنوية عن الجرائم الالكترونية في القانون الجزائري، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، الجزائر، العدد الأول، 2009.

33- محمود عبد الحميد عبد المطلب، بحث بعنوان جرائم استخدام شبكة المعلومات العالمي (الجريمة عبر الانترنت)، بحث مقدم إلى مؤتمر القانون والكمبيوتر، المنعقد في الفترة بين 1 و3 ماي 2000، الطبعة الثالثة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004.

34- نبيل إسماعيل عمر، قاعدة عدم قضاء القاضي بعلمه الشخصي، المجلة العربية للدراسات الأمنية المجلد الأول، العدد الأول، 1989، الرياض، السعودية.

35- نزيه عبد اللطيف، التزوير المعلوماتي htpp:/Nazih abdelatif.blogspo.com.

36- هدى حامد قشقوش، الحماية الجنائية للتوقيع الالكتروني بحث مقدم لمؤتمر الأبحاث المصرفية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 12/10 ماي 2003.

37- يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، الإمارات العربية المتحدة، فبراير 2002 منشور على الموقع الالكتروني : http://www.arablaw.org/download/cybercrimesworkpaper.doc

خامسا- المعاجم والقواميس:

1- إسماعيل بن حماد الجوهري، تاج اللغة وإصحاح اللغة العربية، الطبعة الرابعة، دار العلم للملايين، بيروت، لبنان، 1987

2- جمال الدين أبو الفضل محمد بن مكرم بن منظور الأنصاري الإفريقي المصري، لسان العرب، المجلد الرابع، دار الكتب العلمية، لبنان، 2002.

قائمة المصادر والمراجع باللغة الفرنسية والانجليزية:

1/المصادر الأجنبية:

1- Loi N 2001 .1062.15 nov- 2001 relative a la sécurité quotidienne. JORF 16nov - 2001 .

2- Loi N= 2003- 239 18 marc 2003 pour la sécurité intérieure , JORF 19 mars 2003.

3- Loi N= 2004- 204.9 mars 2004. Pourtant adaptation de la justice aux évolution de la criminalité ,JORF 19 mars , 2004..

4- Loi N=2004- 575.21 juin 2004 pour la confiance a de l'économie numérique ,JORF 22 JUIN 2004,[1]- Loi N= 2004- 669 du 9 juillet 2004 relative aux communications électroniques et aux service de communication ,JORF du 10 juillet 2004. P 12483.

5- Loi n°2000t - 230 du 13- 03- 2000 portant adaptation du droit de la preuve aux technologie de l'information et relative à la signature électronique **,JORF** n°62 du 14/03/2000.

Code de procédure pénale français ,JORF du 16 novembre2016

2/المراجع بالفرنسية:

1- Ann Jacobs, la loi du 6 janvier 2003 concernons le méthodes particulière de recherche et quelque autres méthodes d'enquêtes, revue de la faculté de droit de l'université de liège, Canada, 2004.

2- Bident Michel , le droit du traitement de l'information, Nathan, paris 2000

3- CéliNE Renard, castétes , cours de droit de l'internet, Paris, France 2010.

4- CHOPIN- Férédirique. Les politiques publiques de lutte contre la cybercriminalité, Aj pénal Paris, France.

5- Christiane Féral- Schul, cyber droit, le droit à l'épreuve de l'internet, Quatrième édition, Dalloz, paris, France, 20060

6- Cour de cassation, chambre criminelle ; 22 octobre2003-

7- Francis Barbant, les perquisitions informatiques , Revue de barreau, tome 62 Automne, 2002, canada..

8- Frédérique Chopin, la cybercriminalité, Exposé publié sur L'en encyclopédie électronique : le répertoire de droit pénale, 2013.

9- Gassin, R, le droit pénal de l'informatique, les systémes de traitements automatique des données, commentaire de la loi 88/18 du 18/01/1988 relative à la fraude informatique, J.C.P, dalloz, France.

10- Jean- Christophe, saint peau, la présomption d'imputation d une infraction aux organes ou repesant d 'une personne morale ,recueil , Dalloz,2007.

11- Jean- Christophe, saint peau, la présomption d'imputation d une infraction aux organes ou repesant d 'une personne morale ,recueil , Dalloz,2007.

12- Louis Gorron, L'incrimmation du faux et du mensonge en droit pénal, 2011.

13- Marie- Christine Piatti, les libertés individuelles à l'épreuve des nouvelles technologies de l'information, presses universitaire de Lyon, 10ème Edition, 2001.

14- Michael Moran. Interpol et la lutte contre la cybercriminalité ;actes du séminaire internationales sur la lute cotre la cybercriminalité. Organise par la centre de recherche juridique et juridiciare a Alger le 5- 6 mai 201 ; 1ére édition. 2011.

15- Mohamed buzahar, la criminalité informatique sur l'internet, journal de loi , N°1 juriclasseur communication , 2002

16- Norman (Adrian R.b), computer and the law criminal law journal, vol 15 , 1991

17- Philipe Bluteau, la faux en écriture publiques, courrier des Maires, N°= 249, France,2011.

18- Philipe pierre, l'indemnisation du préjudice moral en droit française s.d(www.fondation l,org/préjudice- moral étude- fr).

19- Quemener- Myriam, la coopération entre les organes de lute contre la cybercriminalité pour une stratégie globale de cyber sécurité française, Revue LAMY droit des affaires, numéro 87 , novembre 2013 , wolter kluwer, France,.

20- spirituels jean P, les crimes informatique et d'autre crime dans le domaine de la technologie informatique en Belgique, Revue international de droit pénale, Paris, France, 1993 .

21- Sylviane Métille Mesuré de surveillance sécrètes, le rôle de l'information dans la protection des droits de l'individu, revue de plaidoyer, paris, France 2001 .

22- Thiery legalboudec, LOLCTIC et la lutte contre la cybercriminalité, actes du séminaire internationales, sur la lutte contre la cybercriminalité, organisé par le centre de recherche juridique et judiciaire à Alger le 5,6 mai 2010, 1ère 2dition, 2011.

23- Thompson david, computer crime the improvement of investigative skills part two, www.acpr.gov.au/pdf/ACPR 101.

24- Vuelta Simon. Les nouveaux acteurs de la coopération pénale européenne LPA N=1 .2005.

25- Vuelta Simon. Les nouveaux acteurs de la coopération pénale européenne LPA N=1 .2005.

26- Yves Mayaud, code pénal, 108e edition, Dalloz, Paris, 2001.

3/المراجع بالانجليزية:

1- Eoghan Casey, Digital evidence and computer crime forensic science, computer and the internet, second edition, academic press an imprint of Elsevier, London, 2004.

http://www.IOCE.org/index.phpid=15.

2- Bainbridge David, Hacking the unauthorized access of computer system, the legal implications. MI, Rev, March1989.

3- Kertez (j) and pussztal (L),computer crimes and other crimes against information technlogee in Hungary.

فهرس الموضوعات

فهرس الموضوعات:

المحتويات	الصفحة
شكر وعرفان	
إهداء	
مقدمة.....	01
الباب الأول: الآليات الموضوعية لمكافحة جريمة التزوير الالكتروني	
الفصل الأول: المفاهيم العامة لجريمة التزوير الإلكتروني	
المبحث الأول: مفهوم التزوير التقليدي.....	13
المطلب الأول: تعريف التزوير التقليدي.....	13
الفرع الأول: التعريف اللغوي للتزوير.....	14
الفرع الثاني: التعريف الفقهي للتزوير.....	15
الفرع الثالث: تعريف التزوير في إطار نصوص قانون لعقوبات.....	16
المطلب الثاني: التفرقة بين التزوير وجرائم أخرى مشابهة.....	19
الفرع الأول: الفرق بين التزوير والتقليد.....	19
الفرع الثاني: الفرق بين التزوير والاستعمال المزور.....	23
الفرع الثالث: الفرق بين التزوير والنصب.....	27
المبحث الثاني: مفهوم جريمة التزوير الالكتروني.....	30
المطلب الأول: تعريف التزوير الالكتروني.....	30
الفرع الأول: التعريف الفقهي للتزوير الالكتروني.....	31
الفرع الثاني: التعريف التشريعي للتزوير الالكتروني.....	34
المطلب الثاني: خصائص جريمة التزوير الالكتروني.....	36

فهرس الموضوعات:

الفرع الأول: صعوبة الكشف عن جريمة التزوير الإلكتروني.....	**37**
الفرع الثاني: جريمة التزوير الالكتروني عابرة للحدود.....	**39**
الفرع الثالث: تفرد شخصية المجرم.....	**40**
المطلب الثالث: الفرق بين جريمة التزوير الالكتروني وجرائم أخرى مشابهة.....	**42**
الفرع الأول: الفرق بين جريمة التزوير الالكتروني والتزوير التقليدي.....	**43**
الفرع الثاني: الفرق بين جريمة التزوير الالكتروني وجريمة الإتلاف المعلوماتي.....	**45**
الفرع الثالث: الفرق بين جريمة التزوير الالكتروني وجريمة الاحتيال المعلوماتي.....	**48**
الفرع الرابع: الفرق بين جريمة التزوير الالكتروني وجريمة التلاعب في بيانات نظام معالجة البيانات.....	**51**
الفصل الثاني: القواعد الموضوعية لمكافحة جريمة التزوير الإلكتروني	
المبحث الأول: القواعد الموضوعية لجريمة التزوير الالكتروني على مستوى التجريم.	**58**
المطلب الأول: أركان جريمة التزوير الالكتروني.....	**59**
الفرع الأول: الركن المادي.....	**59**
الفرع الثاني: الركن المعنوي.....	**80**
الفرع الثالث: الركن الشرعي.....	**84**
المطلب الثاني: أنواع جرائم التزوير الالكتروني.....	**95**
الفرع الأول: التزوير في المحررات الالكترونية الرسمية أو العمومية.....	**96**
الفرع الثاني: جرائم التزوير في المحررات الأخرى.....	**104**
المبحث الثاني: القواعد الموضوعية لجريمة التزوير الالكتروني على مستوى العقاب.	**116**
المطلب الأول: العقوبات المقررة لجريمة التزوير الالكتروني في التشريع الجزائري...	**117**
الفرع الأول: العقوبات المقررة للشخص الطبيعي.....	**117**
الفرع الثاني: العقوبات المقررة للشخص المعنوي.....	**124**

فهرس الموضوعات:

المطلب الثاني: العقوبات المقررة لجريمة التزوير الالكتروني في التشريعات المقارنة.	**130**
الفرع الأول: العقوبات المقررة لجريمة التزوير الالكتروني في القانون الفرنسي.....	**130**
الفرع الثاني: العقوبات المقررة لجريمة التزوير الالكتروني في نصوص خاصة.....	**135**
خلاصة الباب الأول.....	**142**
الباب الثاني: الآليات الإجرائية لمكافحة جريمة التزوير الإلكتروني	
الفصل الأول: القواعد الإجرائية لمكافحة جريمة التزوير الإلكتروني على المستوى الداخلي	
المبحث الأول: قواعد الاختصاص القضائي المتعلقة بجريمة التزوير الالكتروني....	**147**
المطلب الأول: قواعد الاختصاص الجنائي الدولي.....	**148**
الفرع الأول: تطبيق مبدأ الإقليمية على جريمة التزوير الالكتروني.....	**148**
الفرع الثاني: تطبيق مبدأ الشخصية على جريمة التزوير الالكتروني.....	**152**
الفرع الثالث: تطبيق مبدأ عينية على جريمة التزوير الالكتروني.....	**154**
الفرع الرابع: أثر خصوصية جريمة التزوير الالكتروني على مسألة الاختصاص القضائي	**158**
المطلب الثاني: قواعد الاختصاص الجنائي الداخلي.....	**161**
الفرع الأول: الاختصاص الشخصي.....	**161**
الفرع الثاني: الاختصاص النوعي.....	**162**
الفرع الثالث: الاختصاص المكاني.....	**164**
المبحث الثاني: القواعد الإجرائية للتحقيق وجمع الأدلة في جريمة التزوير الالكتروني.....	**171**
المطلب الأول: الأجهزة المختصة بالتحقيق في جريمة التزوير الالكتروني.....	**172**
الفرع الأول: الأجهزة المختصة بالتحقيق عن جريمة التزوير الالكتروني في التشريع	

الجزائري.....	172
الفرع الثاني: الأجهزة المختصة بالتحقيق عن جريمة التزوير الالكتروني في التشريع الفرنسي.....	184
المطلب الثاني: القواعد الإجرائية لجمع الأدلة في جريمة التزوير الالكتروني.....	190
الفرع الأول: مفهوم الدليل الالكتروني.....	191
الفرع الثاني: حجية الدليل الالكتروني في نطاق الإثبات الجنائي.....	198
الفرع الثالث: القواعد الإجرائية لاستخلاص الدليل الالكتروني.....	205
الفصل الثاني: الجهود الدولية لمكافحة جريمة التزوير الإلكتروني	
المبحث الأول: الجهود الدولية لمكافحة جريمة التزوير الإلكتروني في إطار الأجهزة الدولية.....	248
المطلب الأول: التعاون الأمني والدولي لمكافحة جريمة التزوير الالكتروني.....	249
الفرع الأول: التعاون الأمني في إطار الأجهزة العالمية.....	250
الفرع الثاني: التعاون الأمني على المستوى الأوروبي.....	253
الفرع الثالث: التعاون الأمني على المستوى العربي.....	257
المطلب الثاني: جهود هيئة الأمم المتحدة والاتفاقيات والمعاهدات والجهود الدولية الأخرى في مكافحة جريمة التزوير الالكتروني.....	260
الفرع الأول: جهود هيئة الأمم المتحدة.....	260
الفرع الثاني: الاتفاقيات والمعاهدات الدولية في مجال مكافحة جريمة التزوير الالكتروني.....	264
المطلب الثالث: الجهود الدولية لمكافحة جريمة التزوير الالكتروني في إطار التعاون القضائي.....	269
الفرع الأول: المساعدة القضائية الدولية.....	270

فهرس الموضوعات:

الفرع الثاني: نظام تسليم المجرمين.....	**275**
المبحث الثاني: التحديات التي تواجه التعاون الدولي في مجال مكافحة جريمة التزوير الالكتروني.....	**284**
المطلب الأول: الصعوبات التي تواجه التعاون الدولي في مجال مكافحة جريمة التزوير الالكتروني.....	**284**
الفرع الأول: الصعوبات الناتجة عن الطبيعة الخاصة لجريمة التزوير الالكتروني...	**285**
الفرع الثاني: الصعوبات الناتجة عن ضعف قوانين مكافحة الجرائم الالكترونية.....	**289**
الفرع الثالث: الصعوبات الناتجة عن عدم فعالية التعاون الدولي.....	**292**
المطلب الثاني: الحلول القانونية لمواجهة التحديات الخاصة لمكافحة جريمة التزوير الالكتروني.....	**297**
الفرع الأول: الحلول القانونية لتدارك تحديات مكافحة جريمة التزوير الالكتروني على مستوى التشريعات الوطنية.....	**297**
الفرع الثاني: الحلول القانونية لتدارك تحديات مكافحة جريمة التزوير الالكتروني على مستوى التشريعات الدولية.....	**304**
ملخص الباب الثاني.....	**313**
خاتمة.....	**315**
قائمة المصادر والمراجع.....	**321**
فهرس الموضوعات.	

ملخص:

تعد جريمة التزوير الالكتروني من الأنماط الإجرامية الحديثة التي أفرزها التطور التكنولوجي، وهي تختلف تماما عن جريمة التزوير التقليدي سواء في ذاتية أركانها وأساليب ارتكابها، والبيئة الافتراضية واللامادية التي تقع فيها، وكذا خصوصية مرتكبيها.

ومع تزايد معدلات هذا النوع المستحدث، اضطرت الدول إلى ترشيد نصوصها العقابية التقليدية لتصبح نافذة في مواجهة ومواكبة التطورات التي تصاحبها.

ومن هنا جاءت هذه الدراسة كمحاولة للإحاطة بهذا النوع المستحدث من الإجرام على الصعيد الوطني،أو على الصعيد الدولي، وذلك من خلال الإجابة على الإشكالية الآتية:

ما مدى فعالية الآليات الموضوعية والإجرائية التي وضعتها التشريعات الجنائية في مواجهة جريمة التزوير الالكتروني ؟ وهل تطبيق هذه الإجراءات كافيا وفعالا لاحتواء متغيرات هدا النوع المستحدث من الإجرام؟.

Abstract :

The crime of electronic counterfeiting is one of the modern criminal produced by electronic developement ,it is completely different from the traditional counterfeiting crime ,both in the subjectivity of its element,the modalities of its commission ,the virtual and intangible environment in which it occurs,as well as the specificity of its outhors.

With the increase in rates of this new kind ,countries have been forced to update their traditional procedural texts to become effective and executive in dealing with and keeping pace with evolutions that accompany them.

Thus,this study attempted to copture this new type of crime at the national ,regional or international levels ,by respoding to the following problem :

How effective are the formal and procedural mechanisms established by criminals law in combating the crime of electronic counterfeiting ?

Is the application of these procedures suufficient and efficient to contain the variables of this new type of crime ?.