جامعة أبو بكر بلقا يــد تلمسان

كلية الحقوق

الحماية الجنائية للتجارة الالكترونية

(دراسة مقارنة)

رسالة لنيل شهادة الدكتوراه في القانون الخاص

من إعداد الطالب :

صالح شنين

تحت إشراف :

أ. د محمد رايس

أعضاء لجنة المناقشة

أ. د – يوسف فتيحة أستاذ التعليم العالي جامعة تلمسان ..... رئيسا

أ.د – محمد رايس أستاذ التعليم العالي جامعة تلمسان .....مقررا ومشرفا

د – هامل هواري أستاذ محاضر (أ) جامعة سعيدة .....مناقشا

د – بوسماحة الشيخ أستاذ محاضر (أ) جامعة تيارت .....مناقشا

د – نقادي عبد الحفيظ أستاذ التعليم العالي جامعة سعيدة.....مناقشا

السنة الجامعية : 2013/2012

بسم الله الرحمان الرحيم

قال الله تعالى:

(قالوا سبحانك لاعلـم لنا إلا ماعلمتنا أنك أنت العليم الحكيم)

الآيـة 32 من سورة البقرة

التشكـر

فبعد شكرنا لله عز وجل خير المتوكل عليه، لا يسعنا في هذا المقام إلا توجيه أسمى عبارات الشكر والتقدير والامتنان إلى الأستاذ الدكتور محمد رايس لتفضله بالإشراف على هذه المذكرة، ولما قدمه لنا من ملاحظات مفيدة وتوجيهات قيمة ساهمت في تذليل المصاعب التي واجهتنا في الإعداد والكتابة نسأل الله له التوفيق والعطاء و .

كما نتقدم بوافر الشكر والامتنان للأساتذة الأفاضل رئيس وأعضاء لجنة المناقشة لتفضلهم بقبول مناقشة هذه الرسالة، داعين لهم بالتوفيق في خدمة العلم وكل من ساهم معي من قريب أو بعيد في انجاز هذه الرسالة.

الإهـداء

اهدي هذا العمل المتواضع إلى والدتي رحمها الله ، ووالدي الغالي شفاه الله

عماد الدين عياض ، وكل من ساهم من قريب أو بعيد في انجاز هذه الرسالة .

قائمة المختصرات

أولا: باللغة العربية

ص : صفحة

ج. ر : الجريدة الرسمية.

ق.ع.ج : قانون العقوبات الجزائري.

ق.ا.ج.ج : قانون الإجراءات الجنائية الجزائري

ق. م .ج : القانون المدني الجزائري

ق . ع . م : قانون العقوبات المصري

ق.ع.ف : قانون العقوبات الفرنسي.

ط : الطبعة.

ج : الجزء.

د.ت.ن : دون تاريخ نشر.

د.ج : دينار جزائري.

و.م.أ : الولايات المتحدة الأمريكية.

ثانيا: باللغة الأجنبية

Art : Article.
N° : Numéro.
P.L : Public Law.
Sec : section.
P : page.
éd : édition.
Op. Cit . : Ouvrage précité.
Rev. : Revue.
R.S.C. : Revue du Science Criminelle
R.I.D.P. :Revue International du Droit Pénale

مقدمـة

مقدمة

يعيش العالم اليوم ثورة معلومات واتصالات أحدثت تغيرات جذرية في المفاهيم المختلفة ومن أكثر المجالات التي تأثرت بهذا التطور التجارة والمعاملات التجارية، إذ ظهرت فكرة التجارة الالكترونية (le commerce électronique) والتي يقصد بها المعاملات التجارية التي تتم باستخدام تكنولوجيا المعلومات وشبكات الاتصال.

كما عرفتها على المستوى الدولي منظمة التعاون الاقتصادي والتنمية (OECED) بأنها جميع المعاملات التجارية التي تتم بين الشركات أو الأفراد، وتقوم على أساس التبادل الالكتروني للبيانات ، وكذلك عرفتها منظمة التجارة العالمية بأنها مجموعة عمليات عقد الصفقات وتأسيس الروابط التجارية وتوزيع وتسويق وبيع المنتجات عبر وسائل الكترونية [1].

أماعلى المستوى الوطني فان أغلب التشريعات الأجنبية لم تتضمن تعريفا للتجارة الالكترونية وكذلك التشريعات العربية باستثناء البعض كالتشريع التونسي الذي عرفها في الفصل 02 من قانون المبادلات والتجارة الالكترونية التونسي الصادر في 11 أوت 2000 ، بأنها العمليات التجارية التي تتم عبر المبادلات الالكترونية[2].

---

[1] – أماعلى المستوى الفقهي فقد تعددت التعريفات ، إذ عرفتها الجمعية الفرنسية للتلاماتيك والملتيميديا (AFTEL) تعريفا ضيقا بأنها مجموعة المعاملات التجارية التي يتم الشراء فيها عن طريق وسائل الاتصال ، كما عرفتها الجمعية الأمريكية للتجارة الالكترونية تعريفا واسعا بأنها مجموعة الاستعمالات لوسائل الاتصال ، للتفصيل راجع أحمد عبد الخالق، التجارة الالكترونية والعولمة، منشورات المنظمة العربية للتنمية الإدارية، مصر 2006، ص34 . أنظر أيضا هدى حامد قشقوش ، الحماية الجنائية للتجارة الالكترونية عبر الانترنت ، دار النهضة العربية القاهرة مصر ، 2000 ص 6. وانظر أبضا :

Mohamed bedhri. le commerce électronique: quellles perspectives au Maroc. Eljoussour. 2001. P64

[2] – كما جاء قانون المعاملات والتجارة الالكتروني لإمارة دبي رقم 2 لسنة 2002 بتعريف مشابه للتجارة الالكترونية في المادة الثانية منه مفاده أنها المعاملات التجارية التي تتم بواسطة المراسلات الالكترونية. كماعرفها جانب من الفقه المصري بأنها جميع المعاملات التي تتم عبر الانترنت ، لكنه وسع في هذه المعاملات ، كما أنه قصرها على الانترنت

وتكسب التجارة الالكترونية سواء بين المؤسسات[1]، أو بين المؤسسات والمستهلكين [2] أو بين الحكومة والمستهلكين [3]، أو بين المؤسسات والحكومة [4]، أهمية كبيرة يوما بعد الآخر وذلك من خلال التوجه المتزايد لكثير من دول العالم نحو الاعتماد عليها في ممارسة نشاطاتها و أعمالها التجارية ، سواء كانت على مستوى الأفراد أو الشركات أو الدول ، حيث بلغت إرادات اقتصاد الانترنت عالميا إلى 800 مليار دولار بنهاية عام 2001 لتطلق بذلك اقتصادا يعرف بالاقتصاد الرقمي[5].

تتميز التجارة الإلكترونية بالعديد من المزايا التي تجعل الإقبال عليها يتزايد وينمو يوما بعد يوم ، من أهمها أنها توفر تسويق أكثر فعالية وتحقيق أرباح أكثر، و تساعد كذلك على تخفيض مصاريف الشركات، وتؤدي إلي ، والقدرة أيضا على تحليل الأسواق والاستجابة لتغير متطلبات السوق ، تساعد على تقديم الخدمات للعملاء على مدار 24 ساعة، وكذلك خلق العديد من فرص العمل الحر

---

[1] – وتكون العلاقة في هذا الشكل بين منشئات الأعمال ، إذ يتم التعامل والاتفاق والتنفيذ عبر الاتصال الالكتروني للتفصيل أنظر أحمد عبد الخالق، مرجع سابق، ص40

[2] – تكون العلاقة فيها بين منشآت الأعمال والمستهلك ، بهدف تلبية طلبات ورغبات المستهلك ، إذ يتم بيع السلع والخدمات إلى المستهلك باستخدام تكنولوجيا المعلومات وشبكات الاتصال، وتتم إجراءات البيع والشراء عبر الانترنت وعادة

أخرى مثل الشيكات الالكترونية أو عن طريق التحويل من حساب المشتري البنكي إلى حساب البائع البنكي ، وكذلك يمكن أن يك .

[3] – وتوجد أيضا التجارة الالكترونية بين الحكومة والمستهلكين(G2C) والتي تكون العلاقة ما بين تقوم الحكومة بتقديم الانترنت، وقد تطور هذا

الشكل إلى مايعرف بالحكومة الالكترونية. للتفصيل أنظر أحمد عبد الخالق، مرجع سابق ، ص42 .

[4] –وتكون العلاقة بين الوزارات والمؤسسات الحكومية وبين منشئات الأعمال ، وهو ما يعرف بالشراء الحكومي الالكتروني ، حيث تقوم الحكومة بإتمام إجراءات ا .

[5] – وليد الزبيري ، التجارة الالكترونية عبر الانترنت ، دار المناهج الأردن ، 2004 ، ص17 .

تتسم التجارة الإلكترونية عبر الإنترنت بخصائص عديدة منها على سبيل المثال أنها تعتمد على الوثائق الإلكترونية وأنها ترتبط بالأنشطة التجارية ذات المفهوم الواسع الذي لا يقصرها على المعاملات التجارية فحسب بل تشمل جميع الأنشطة الاقتصادية كالاستثمارات وعمليات البنوك بالإضافة إلي أنها ذات طبيعة دولية دائما نظرا لعالمية شبكة الإنترنت، كذلك هي تتميز بالنمو حيث تشير بعض التقديرات الصادرة عن منظمة التعاون الاقتصادي والتنمية إلي أن قيمة مبادلات التجارة الإلكترونية في العالم قد تجاوزت 300 مليار دولار عام 2000م و هو يعادل 10 أضعاف مقارنة بعام 1998م وقفزت هذه القيمة لتصل عام 2003 إلي 1300مليار دولار، أما في الشرق الأقصى فقد بلغت قيمة المبادلات 400مليون دولار عام 2000م لتقفز إلي 3 مليار دولار عام 2003

إن ما بلغته التجارة الالكترونية من مكانة معتبرة يعود إلى تنوع وتوسع نطاق الأسواق المجال لدخول الأسواق الدولية والعالمية ، مما يتيح لأطراف العملية التجارية التعامل بينهم بسهولة ، بغض النظر عن اختلاف مواقعهم وبعد المسافات فيما بينهم [1].

كما تمتاز بسهولة انجاز العملية التجارية في وقت قصير وبأقل جهد و ادني تكاليف إذ وفرت التقنيات الحديثة كالمتاجر الافتراضية والبنوك الالكترونية وغيرها من التقنيات المالية ميزة السرعة في التعاقد و التنفيذ وخفض تكاليف الاتصالات وخفض كلفة الأيدي العاملة بتقليل حجمها والاستعانة عنها بالوسائل الالكترونية كالعاملة بالتسويق والمبيعات وخدمة الزبائن وخفض تكلفة الدعاية والإعلان ووسائل النفاذ إلى الأسواق [2].

وتوفر أيضا معلومات متكاملة عن الأسواق في كافة أنحاء العالم ، مما يتيح إمكانية مقارنة أسعار السلع والخدمات في الداخل والخارج، وبالتالي زيادة المنافسة مابين منتجي السلع ومقدمي الخدمات مما يؤدي إلى خفض الأسعار، كما تمتاز باستخدامها لأساليب تقنية تسهل

---

[1] – وليد الزبيري ، مرجع سابق ، ص17 وما بعدها. أكرم عبد الوهاب، التجارة الالكترونية، مكتبة ابن سينا القاهرة مصر، 2004 ، ص48.

[2] – أكرم عبد الوهاب، مرجع سابق، ص.48-49.

عمليات الوفاء بسرعة فائقة مثل النقل الالكتروني للأموال، وبطاقات الذكية وغيرها من الوسائل المصرفية ، وتسهل أيضا التواصل الفعال ما بين أطراف العملية التجارية [1] ، كذلك تتيح التجارة الالكترونية الفرصة للمؤسسات التجارية الصغيرة الدخول في منافسة المنشئات التجارية الكبيرة المحلية والعالمية، وتخلق أساليب جديدة في العمل،
يتناسب وأساليب الاتصالات وتكنولوجيا المعلومات [2].

لكن إذا كانت التجارة الالكترونية وسيلة هامة للوصول إلى أسواق العالم في أسرع وقت ممكن وبأقل مجهود وادني تكلفة ، فان أمام هذه التجارة الالكترونية تحديات ومعوقات ، إذ ترتب عن الأهمية المتزايدة لها ظهور مشاكل عملية وقانونية تتعلق بفروع القانون المختلفة كالقانون المدني والقانون التجاري والقانون الدولي الخاص ، بصفة خاصة في القانون الجنائي إذ أصبحت التجارة الالكترونية عرضة لاعتداءات إجرامية متزايدة على نحو يهدد التنمية الاقتصادية ، مما أدى إلى ضرورة إقرار الحماية الجنائية للتجارة الالكترونية للتصدي للجريمة المعلوماتية التي تهدد النشاط التجاري الذي يتم عبر وسائل الاتصال وخصوصا الانترنت .

يعد موضوع الحماية الجنائية للتجارة الالكترونية من الموضوعات الهامة من الناحية النظرية والعملية على حد سواء ، فمن الناحية النظرية يعالج كيفية مواجهة تشريعات الدول لجرائم الاعتداء على التجارة الالكترونية سواء في إطار القواعد العامة أو في النصوص الخاصة ، كما يتطرق للجوانب الإجرائية لحماية التجارة الالكترونية ، ويبحث أيضا مدى كفاية وفعالية الحماية الجنائية للتجارة الالكترونية .

أما من الناحية العملية والتطبيقية فالواقع يؤكد حركة تزايد حركة التجارة الالكترونية ، مما يتطلب حمايتها جنائيا من الجرائم ، حيث أدى انتشار الجرة الالكترونية عبر الانترنت خاصة إلى أن الكثير من الشركات خسرت أموال كبيرة بسبب التعاملات التجارية الالكترونية ، الأمر الذي يقتضي تدخلا من المشرع لحمايتهم من الجريمة المعلوماتية ، كما يقتضي الأمر حماية

[1] – أحمد عبد الخالق، مرجع سابق، ص.45 .

[2] – المرجع نفسه ، ص .46.

المستهلك الذي أصبح يعتمد في الحصول على كثير من السلع والخدمات عن طرق التعاملات الالكترونية .

نظرا لأهمية الحماية الجنائية للتجارة الالكترونية وضعت لجنة الأمم المتحدة للقانون التجاري الدولي قوانين نموذجية لمتطلبات التجارة الالكترونية ، كالقانون النموذجي للتجارة الالكترونية لعام 1996، والقانون النموذجي للتوقيعات الالكترونية لعام 2001 ، كما اهتم أصدر الاتحاد الأوربي مجموعة من التوجيهات كالتوجيه الأوربي رقم 200-31 المتعلق بالتجارة الالكترونية والتوجبه رقم 97- 07 المتعلق بحماية المستهلك في العقود عن بعد والتوجيه الأوربي رقم 97-489 بشان الدفع الالكتروني ، والتوجيه رقم 99-93 بشأن التوقيع الالكتروني .

كما اهتمت بعض الدول بحماية التجارة الالكترونية كفرنسا التي أصدرت قانون رقم 91-1382 المتعلق بأمن الشيكات وبطاقات الوفاء ، كما أصدرت بعض الدول العربية قوانين للتجارة الالكترونية كقانون المبادلات والتجارة الالكترونية التونسي لعام 2000، وقانون رقم 15-2004 لعام 2004 بشأن التوقيع الالكتروني بخلاف المشرع الجزائري الذي لم يهتم بموضوع الحماية الجنائية للتجارة الالكترونية بسبب عدم انتشار التجارة الالكترونية .

بناء على ذلك جاءت دراستي المقارنة لموضوع الحماية الجنائية للتجارة الالكترونية من الناحية الموضوعية والإجرائية، رغم حداثتة نسبيا ، ودقة البحث فيه و صعوبته لأنه لا يقتصر على مسائل قانونية ، بل يمزج بين القواعد القانونية والقواعد الالكترونية.

فنظرا لحداثة التجربة في الدول العربية وجدت من الملائم أن أتعرض لنظام الجارة الالكترونية من الناحية الجنائية من خلال دراسة مقارنة بين بعض التشريعات العربية والأجنبية بهدف البحث عن النظام القانوني الأفضل لحماية التجارة الالكترونية جنائيا في ظل الخوصصة التي تعيشها المنطقة العربية ثم إن أغلب الدول العربية تفتقر لقانون بشأن التجارة الالكترونية يحمي التجارة الالكترونية

كما أن القوانين النموذجية الدولية والأوربية المنظمة للتجارة الالكترونية لاتتضمن نصوصا عقابية ، وحتى الدراسات المتعلقة لهذه القوانين تركز بشكل أكبر على الجانب المدني والتجاري

وعليه فان البحث عن الحماية الجنائية للتجارة الالكترونية يرتكز بشكل أساسي على الرجوع للتشريعات الجنائية الوطنية ، بهدف الوصول الى الآليات الموضوعية والإجرائية للحماية الجنائية للتجارة الالكترونية ، ومدى كفاية وفعالية الحماية الجنائية للتجارة الالكترونية وهل تعبد ثقة المستهلك في التجارة الالكترونية .

نظرا لحداثة الموضوع وعدم وجود قواعد ونصوص خاصة بالتجارة الالكترونية في أغلب التشريعات ، فقد اعتمدت في دراسة الموضوع على المنهج التأصيلي ، والتحليلي ، والمنهج المقارن ، حيث استخدمت المنهج التأصيلي من اجل رد الفروع والجزئيات إلى أصولها العامة الواردة في القانون الجنائي .

وكذلك استعملت المنهج التحليلي من خلال تحليل وشرح الجوانب الموضوعية والإجرائية الالكترونية بجوانبها الموضوعية والإجرائية في بعض التشريعات العربية كالتشريع الجزائري والمصري ، والتونسي ، وفي أبرز التشريعات الأجنبية كالتشريع الفرنسي والتشريع الانجليزي والأمريكي .

كما اعتمدت المنهج المقارن من خلال مقارنة الحماية الجنائية للتجارة الالكترونية في بعض القوانين العربية كالتشريع الجزائري والمصري والتونسي، وفي بعض التشريعات الأجنبية وبصفة خاصة في القانون الفرنسي، وفي الولايات المتحدة الأمريكية ، وفي التشريع الانجليزي

تثير التجارة الالكترونية مشكلات عملية وقانونية في القانون الجنائي تتعلق بتحديد ما إذا كانت القوانين الجنائية القائمة سواء نصوص جرائم الأموال ، أو نصوص جرائم التزوير تواجه الأفعال غير المشروعة على التجارة الالكترونية ، وهل تحتاج إلى تدخل خاص يناسب طبيعة هذه التعاملات التجارية الالكترونية ، وتثير مشاكل أيضا تتعلق بمدى تطبيق النصوص الإجرائية التقليدية على جرائم التجارة الالكترونية ، وهل تحتاج إلى نصوص خاصة لمواجهتها.

كما تثير أيضا مشكلات تتعلق بوسائل وصور حماية المستهلك سواء تعلق الأمر بحماية بياناته الخاصة والتي ترتبط بحياته الخاصة ، أو تلك المتعلقة بتعاملاته البنكية أو أرقام بطاقة الائتمان .

أثارت الجرائم الإلكترونية لاسيما جرائم التجارة الالكترونية بعض المشكلات فيما يتعلق بالقانون الجنائي الموضوعي بحثا عن إمكانية تطبيق نصوصه التقليدية على الجرائم الالكترونية، و كذلك أثارت العديد من الإشكالات في نطاق القواعد الإجرائية التقليدية تعرقل عمل أجهزة العدالة في مواجهتها ، ءات المحاكمة من اختصاص جنائي ومدى سلطة المحكمة في قبول تقدير الدليل لالكتروني .

إذ يواجه أجهزة الضبط القضائي صعوبات ومشاكل عملية في مواجهة هذه الجرائم الالكترونية ترجع إلى ن ضعف خبرتهم في هذا المجال، وهذا ما جعل أغلب الدول الأجنبية ، وبعض الدول العربية تنشئ ضبطية قضائية متخصصة في الجرائم المعلوماتية بما فيها جرائم التجارة الالكترونية وتخويلها اختصاصات وسلطات معينة عادية واستثنائية ، كما تم إنشاء على المستوى الدولي والأوربي بالانتربول الاوربول على التوالي .

كما تثير جرائم التجارة الالكترونية إشكاليات قانونية في مرحلة التحقيق الابتدائي متعلقة بمدى قابلية نظم الحاسوب والانترنت للتفتيش والضبط ، كما أن إجراءات جمع الأدلة تتم في كثير من الدول في إطار النصوص التقليدية ، مما بترتب عليه الكثير من المشكلات بالنسبة لضبط أدلة هذه الجرائم ، والتي قد تتعدد أماكن ارتكابها داخل الدولة الواحدة، أو يمتد نطاقها لشمل الكثير من الدول فيتعذر بذلك اتخاذ إجراءات جمع الدليل بشأنها.

تخطى مدى الجريمة المعلوماتية لاسيما جرائم التجارة الالكترونية حدود الدول بل والقارات ولم يعد خطرها أو آثارها محصورة في النطاق الإقليمي لدولة بعينها ، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام أجهزة العدالة الجنائية المعنية بمكافحة الجريمة .

أبرزها مسألة تحديد المحكمة الجنائية المختصة في مجال جرائم التجارة الالكترونية، لأنه يترتب على ذلك تحديد القانون الواجب التطبيق في حالة تنازع القوانين ، ذلك أن ملاحقة الجناة

وكشف جرائمهم عبر الحدود يقتضي من الناحية العملية أن يتم في نطاق إقليم دولة أخرى ، وهو فضي إلى

تنازع الاختصاص القضائي بسبب صعوبة تحديد مكان وقوع الجريمة المعلوماتية عبر الوطنية .

كما تثير هذه الجرائم ومسألة سلطة المحكمة الجنائية في قبول و تقدير الأدلة الرقمية والالكترونية ، فلقد تركت ثورة تقنية المعلومات انعكاسات واضحة على إثبات الجريمة المعلوماتية عبر الوطنية بخلاف الجرائم التقليدية ، بالنظر إلى طبيعة هذا النوع من الجرائم

بمكافحتها والتصدي لها ، وتكمن المشكلات المتعلقة بالإثبات في أن هذه الجرائم باعتبارها تقع .

إلا إن الإشكالية الرئيسة التي يتمحور حولها البحث هل أوجدت التشريعات الجنائية المختلفة نظام متكامل لحماية التجارة الالكترونية جنائيا من الناحية الموضوعية والإجرائية يعيد ثقة المستهلك في التجارة الالكترونية ؟

ولمعالجة هذه الإشكالية قسمت البحث إلى بابين، حيث عالجت في الباب الأول الحماية الجنائية الموضوعية للتجارة الالكترونية بين النصوص التقليدية والنصوص المستحدثة، وقسمت هذا الباب إلى فصلين، تناولت في الفصل الأول الحماية الجنائية في إطار النصوص التقليدية من خلال نصوص جرائم الأموال في مبحث أول، ومن خلال نصوص جرائم التزوير في مبحث ثان، بينما تطرقت في الفصل الثاني للحماية الجنائية في إطار النصوص المستحدثة خلال الحماية الجنائية للتاجر في مبحث أول، ومن خلال الحماية الجنائية للمستهلك في مبحث ثان .

أما الباب الثاني فخصصته للحماية الإجرائية للتجارة الالكترونية، وقسمته إلى فصلين إذ تناولت في الفصل الأول الحماية الجنائية للتجارة الالكترونية قبل مرحلة المحاكمة من خلال مرحلة البحث والتحري في مبحث أول ، ومرحلة التحقيق الابتدائي في مبحث ثان أما الفصل

الثاني فتطرقت فيه للحماية الجنائية للتجارة الالكترونية في مرحلة المحاكمة من خلال تحديد المحكمة الجنائية المختصة بجرائم التجارة الالكترونية في مبحث أول ، وسلطة هذه المحكمة في قبول وتقدير الأدلة الجنائية الالكترونية في مبحث ثان.

وختمت الدراسة بخاتمة توصلت فيها للعديد من النتائج والاقتراحات.

الباب الأول

الحماية الجنائية الموضوعية للتجارة الالكترونية

الباب الأول

الحماية الجنائية الموضوعية للتجارة الالكترونية

لقد أدت الثورة المعلوماتية إلى ظهور التجارة الالكترونية التي انتشرت بسرعة هائلة وخاصة في الدول الغربية بفضل مزاياها العديدة والمتنوعة كسهولة انجاز العملية التجارية في أسرع وقت ممكن وبأقل مجهود وأدني تكلفة ، لكن واجهت التجارة الالكترونية تحديات ومعوقات أبرزها الجريمة المعلوماتية ، فبرزت الحاجة إلى توفير حماية جنائية لها .

ولما كان القاضي مقيد بمبدأ شرعية الجرائم والعقوبات فإنه لا يستطيع أن يجرم أفعال لم ينص عليها المشرع حتى ولو كانت هذه الأفعال خطيرة على الجانب الاقتصادي ، وكل ما يمكنه عمله هو محاولة تفسير النصوص القائمة .

بناءا على ذلك اتجه الفقه والقضاء في البداية لمحاولة تطبيق النصوص التقليدية المتعلقة بنصوص جرائم الأموال، ونصوص جرائم التزوير ، فأدى ذلك إلى جدل فقهي وقضائي كبير فتطلب الأمر تدخل تشريعي ، فتدخل المشرع في بعض الدول بتعديل النصوص القائمة لكي تتمشى مع الطبيعة الخاصة لجرائم التجارة الالكترونية ، بينما فضلت بعض التشريعات استحداث نصوص خاصة .

وعليه سنبحث في هذا الباب الحماية الجنائية الموضوعية للتجارة الالكترونية في إطار القواعد العامة لقانون العقوبات **(الفصل الأول)** ، ومن خلال نصوص جرائم الأموال **(المبحث الأول)** ، ثم من خلال نصوص جرائم التزوير **(المبحث الثاني)**، وفي إطار نصوص مستحدثة خاصة **(الفصل الأول)**، من خلال الحماية الجنائية للتاجر **(المبحث الأول)** ، والحماية الجنائية للمستهلك **(المبحث الثاني)**، على التفصيل الآتي :

الفصل الأول

الحماية الجنائية للتجارة الالكترونية في إطار النصوص العامة

واجهت التجارة الالكترونية تحديات أبرزها وأخطرها الجريمة المعلوماتية فتطلب الأمر حماية جنائية لها ، ولما كانت أغلب الدول وخاصة العربية تفتقر لقوانين تحمي التجارة الالكترونية فحاول الفقه والقضاء في البداية محاولة تفسير النصوص العامة المتعلقة بجرائم الأموال، ونصوص جرائم التزوير ، فلما كان القاضي مقيد بمبدأ شرعية الجرائم والعقوبات فإنه لا يستطيع أن يجرم أفعال لم ينص عليها المشرع حتى ولو كانت هذه الأفعال خطيرة ، بل يمكنه فقط محاولة تفسير تلك النصوص القائمة .

إذ حاول الفقه والقضاء تطبيق نصوص جرائم الأموال على أموال الجارة الالكترونية فتعرض لمدى صلاحية الأموال المعنوية كمحل لجرائم الأموال المتمثلة في جريمة السرقة والنصب وخيانة

الإجرامي في جرائم الأموال .

كما حاول الفقه والقضاء تطبيق نصوص جرائم التزوير على المستندات التجارية الالكترونية من حيث مدى اعتبارها محررات في مفهوم جريمة التزوير ، ومدى خضوعها للنشاط الإجرامي في جريمة التزوير .

وعليه سنبحث الحماية الجزائية في إطار القواعد العامة لقانون العقوبات من خلال نصوص جرائم الأموال(**المبحث الأول**)، ومن خلال نصوص جرائم التزوير(**المبحث الثاني**).

المبحث الأول

الحماية الجنائية للتجارة الالكترونية من خلال نصوص جرائم الأموال

لقد صاحب تنامي التجارة الالكترونية خطر الاعتداء على الأموال في نطاق التجارة الالكترونية مما سبب خسائر فادحة، فلزم الأمر توفير حماية جنائية لأموال الجارة الالكترونية في نطاق نصوص جرائم الأموال، في ظل غياب نصوص قانونية خاصة.

لذا سنبحث الحماية الجنائية للتجارة الالكترونية في إطار نصوص جرائم الأموال من خلال محل جرائم الأموال والتجارة الالكترونية (في المطلب الأول) والنشاط الإجرامي في جرائم الأموال والتجارة الالكترونية(في المطلب الثاني).

المطلب الأول: محل جرائم الأموال والتجارة الالكترونية

على الرغم من اختلاف جرائم ضد الأموال عن بعضها من حيث النشاط الإجرامي ، إلا أنها تشترك في أنها ترتكب على مال منقول مملوك للغير[1].

لقد كانت الأموال من وجهة النظر التقليدية تقتصر على الأموال المادية ، لهذا اقتصرت الحماية الجزائية على الأموال المادية، لكن مع التطور التكنولوجي ظهرت أموال معلوماتية معنوية ذات أهمية كبيرة كالبرامج والمعلومات، فاستدعى الأمر إعادة النظر في حصر الأموال في الأشياء المادية لوحدها [2] .

---

[1] - يختلف الفقه في اعتماد مصطلح المال أو الشيء للتعبير عن موضوع جرائم الأموال ، حيث اعتمد المشرع الفرنسي كلمة الشيء في المادة 311 من قانون العقوبات الفرنسي الجديد وما يليها ، وكذلك المشرع الجزائري في المواد 350 وما بعدها من قانون العقوبات الجزائري وهو الراجح ، على خلاف المشرع المصري الذي اعتمد لفظ المال في نصوص المواد311 وما يليها من ق ع المصري.

[2] – عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسوب ،الدار الجامعية الجديدة ، مصر ، 1999، ص81.

الفرع الأول: مدى صلاحية الأموال المعنوية كمحل لجريمة السرقة والنصب

سنبحث مدى صلاحية الأموال المعلوماتية المعنوية كمحل لجريمة السرقة أولا وثانيا مدى صلاحيتها كمحل لجريمة النصب على النحو الآتي :

أولا- مدى صلاحية الأموال المعنوية كمحل لجريمة السرقة:

تفترض جريمة السرقة وجود شرط مفترض يتمثل في محل جريمة السرقة المتمثل في المال ويشترط فيه أن يرد على شيء وأن يكون منقول ومملوك للغير[1] ، فما مدى انطباق هذه العناصر على الأموال المعلوماتية المعنوية.

1- مدى انطباق وصف المال على الأموال المعنوية:

لقد استقر الفقه على أن المال موضوع جريمة السرقة يجب أن يكون ماديا أي له كيان مادي ملموس ، وهذا ما تفرضه طبيعة الاختلاس في جريمة السرقة باعتباره الاستيلاء على الحيازة الكاملة ، وهو ما لا يتصور إلا بالنسبة للأشياء المادية [2]، والشيء المادي هو ما يشغل حيزا ملموسا في الفراغ الكوني ، أو هو كل ما له كيان ذاتي مستقل من العالم الخارجي أو هو كل ما له طول وعرض وسمك بصرف النظر عن حجمه أو وزنه[3].

ولذلك ظلت الأشياء والأموال المعنوية مستبعدة كمحل لجريمة السرقة إلا إذا اتخذت هذه الأموال مظهرا ماديا ، إلا أن التطور التكنولوجي خاصة في مجال الحاسبات أدى إلى إعادة النظر في إمكانية سرقة هذه الأشياء التي أصبحت تفوق في عددها وقيمتها الأشياء المادية [4].

---

[1] -Jean Larguier:droit Pénal spécial. Dalloz 1975. P.174.

[2] – هدى قشقوش ، شرح قانون العقوبات ، القسم الخاص ، دار النهضة العربية ، مصر ، 20007، ص30.

[3] - عبد القادر القهوجي وعبد الله فتوح الشاذلي، شرح قانون العقوبات، قسم الخاص مصر: دار المطبوعات الجامعي، 2003، 261.

[4] – عبد القادر القهوجي، مرجع سابق، ص86

إن عدم تحديد طبيعة الشيء محل السرقة أدى بالفقه والقضاء إلى أن يعيد حساباته في هذا الشأن حيث ذهب الفقه الحديث في مصر وفرنسا إلى أن نص المادة 311 من قانون العقوبات المصري والمادة 311 من قانون العقوبات الفرنسي الجديد لم تشترطا أن ينص فعل الاختلاس على محل مادي [1]، فقد ذكرت لفظ الشيء أو المال مطلقة دون قيد ، وهذا ما يعني أن المشرع المصري والفرنسي لم يقصد

المحل مطلق الأموال أو كل عناصر الذمة المالية وحتى ولو كانت هذه الأموال أو العناصر غير مادية أي معنوية طالما تقبل الأخذ أو الاختلاس[2].

كما أن المشرع الجزائري هو الأخر لم يجعل محل السرقة يقتصر على الأشياء المادية، فبالعودة إلى نص المادة 350 من قانون العقوبات الجزائري نجده لم يشترط أن يكون الشيء ماديا، إذا وردت كلمة الشيء مطلقة دون تخصيص[3].

وبالتالي فإن الأشياء المعنوية كبرامج الحاسوب والمعلومات تصلح كمحل لجريمة السرقة، إذ أن نصوص جريمة السرقة لا تحول من حيث المبدأ على إمكانية وقوع جريمة السرقة على شيء معنوي لكن ذهب فريق من الفقه الفرنسي يمثله الفقيه ميرل و الفقيه فيتي إلى أن كلمة الشيء الوارد ذكرها في المادة 311 /1 من قانون العقوبات الفرنسي الجديد ، ترتبط بذات كلمة مادية تشير إلى الأشياء المادية الملموسة [4].

---

[1] – هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن ، دار النهضة العربية 20007، القاهرة مصر ، 1992، ص66.

[2] – عبد القادر القهوجي، مرجع سابق، ص87.

[3] – راجع المادة 350 من الأمر رقم 156/66 المؤرخ في8 جوان1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم ، ج ر49 صادرة في 1966/6/11. والتي تنص :(كل من اختلس شيئا غير مملوك له يعد سارقا ويعاقب بالحبس من سنة (1) إلى خمس (5)سنوات وبغرامة من 100.00 د ج إلى 500.000 دج).

[4] - محمد الشوابكة ، جرائم الحاسب والانترنت ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع ، عمان الأردن 2004 ، ص149.

كما أن عدم تحديد طبيعة الشيء محل السرقة هو الذي دفع القضاء وأيده الفقه إلى القول بإمكانية اختلاس التيار الكهربائي على الرغم من أنه ليست له طبيعة مادية ، إذ أقرت محكمة النقض الفرنسية إمكانية سرقة التيار الكهربائي وخط الهاتف على أساس انتقال الطاقة في الحالتين [1]، كما أقرت محكمة النقض إمكانية سرقة التيار الكهربائي و خط الهاتف [2].

وعليه استقرت بعض التشريعات كالإنجليزي والألماني والإيطالي واللبناني وأيضا الفرنسي على العقاب على سرقة الطاقة [3] ، كما نص التشريع الجزائري في المادة 2/350 من قانون العقوبات الجزائري على تطبيق عقوبات السرقة على اختلاس الكهرباء [4].

ولقد قام فريق من الفقه وفقا لذلك بقياس سرقة البرامج والمعلومات على سرقة التيار الكهربائي إلا أن ذلك غير مستساغ ففي ذلك خروج على مبدأ شرعية الجرائم والعقوبات والذي يمنع التفسير بالقياس في مسائل التجريم بالإضافة إلى ذلك فالكهرباء تعتبر شيئا ماديا لا معنويا يخضع للسيطرة كغيره من الأشياء المادية ، فهي تعبأ وتنقل وتحاز وتقاس ويتحكم فيها سواء بالاستهلاك أو عدمه، وترد عليها الملكية ، وكل هذا يؤكد صلاحيتها للاختلاس [5].

وذهب فريق آخر من الفقه إلى أنه إذا كانت النصوص الجزائية تطبق على سرقة الطاقة ، فإن المعلومات وبرامج الحاسوب تعتبر طاقة ذهنية تقبل التملك والحيازة من خلال دعامتها [6]، كما أنها تقبل الانتقال بموافقة حائزها ، وهذه الموافقة يترجمها الرقم الكودي وكلمة السر اللذان يعدان بمثابة

---

[1] – هدى قشقوش ، شرح قانون العقوبات ،القسم الخاص ، مرجع سابق، ص30

[2] – أقرت محكمة النقض المصرية إمكانية سرقة خط الهاتف في حكمها الصادر في 17 نوفمبر 1980م ، والذي جاء فيه : «لما كان من المقرر أن السرقة هي اختلاس منقول مملوك للغير والمنقول في هذا المقام هو كل ما له قيمة مالية يمكن تملكه وحيازته ونقله ، وهذه الخصائص متوفرة في الكهرباء »

[3] - عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية ، الكتاب الثاني الحماية الجزائية لنظام التجارة الالكترونية، دار الفكر الجامعي الإسكندرية، 2002، ص188.

[4] – راجع المادة 350/ 2 من قانون العقوبات الجزائري.

[5] – نائلة عادل قورة ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي الحقوقية ، بيوت لبنان ، 2005، ص162.

[6] – المرجع نفسه ، ص162.

المفتاح ، و على الرغم من أنها شيء غير مادي تصلح لأن تكون محل لجريمة السرقة ،ولا يمثل هذا خروجا على مبدأ شرعية الجرائم والعقاب لأن نصوص السرقة تقبل هذا التفسير، وهي كما رأينا أنها لا تحدد صفة الشيء محل الجريمة إذ يستوي أن يكون هذا الشيء ماديا أو معنويا ، بل أن محكمة النقض الفرنسية قضت صراحة سرقة المحتوى ألمعلوماتي للشرائط خلال الوقت اللازم لنسخ هذه المعلومات[1].

إذن وفقا لنصوص جريمة السرقة تصلح برامج الحاسوب والمعلومات لأن تكون محلا للاختلاس والأخذ في جريمة السرقة باعتبار أنها أشياء معنوية يصدق عليها وصف المال لعمومية تلك النصوص الجنائية المنظمة لجريمة السرقة .

ومما لاشك فيه أن عدم انطباق وصف المال على البرامج والمعلومات يؤدي حتما إلى تجريده من الحماية القانونية الجنائية مما يفتح المجال واسعا أمام قراصنة البرامج والمعلومات ، إلا أنه يتعين عدم الاكتفاء بتطبيق تلك النصوص بعمومها ، بل يجب أن يتدخل المشرع بالنص على صلاحية هذه الأموال المعنوية لأن تكون محلا لجريمة السرقة ، أو إعطاء مفهوم واسع للمال كما فعلت بعض التشريعات التي عرفته على أنه كل شيء له قيمة مالية ، مما يدخل فيه الأشياء المعنوية [2].

2- مدى انطباق وصف المنقول المملوك للغير على الأموال المعنوية :

بالإضافة إلى وجوب أن يكون محل جريمة السرقة مالا، فيجب أن يكون هذا المال منقولا مملوكا للغير، فلا بد لقيام جريمة السرقة أن يكون محل السرقة مالا قابلا للانتقال مملوك لغير الجاني [3].

---

[1] – عبد القادر القهوجي، مرجع سابق، ص190.

[2]– كامل عفيفي عفيفي، جرائم الكمبيوتر ، دراسة مقارنة ، منشورات الحلبي الحقوقية بيروت لبنان، 2003، ص142.

[3] - ويلاحظ أن القانون الجنائي يعطي مفهوم واسع للمنقول، إذ يعد منقولا أي شيء يمكن نقله من مكان إلى آخر، فيدخل في هذا المجال علاوة على المنقولات بطبيعتها، العقارات بالتخصيص والعقارات بالاتصال. لتفصيل راجع هدى قشقوش ، شرح قانون العقوبات،القسم الخاص ، مرجع سابق ، ص27 وما بعدها.

وعن مدى انطباق وصف المنقول على الأموال المعلوماتية المعنوية، فإنه إذا كانت الأموال المعلوماتية المادية تعد من المنقولات وتصلح بالتالي لأن تكون محلا لجريمة السرقة ، فإنه بالنسبة للأموال المعنوية يتنازعها اتجاهان ، حيث يرى الرأي الأول عدم إمكانية انتقال المعلومات أو البرامج ، حيث أنها ذو طبيعة ذهنية بحثه ، إلا إذا انصب الانتقال على الهيكل أو الوسيط المسجل عليه هذه المعلومات[1]، إلا أن هذا الرأي انتقد من قبل جانب من الفقه على أساس أن القابلية للانتقال لا يشترط فيها انتقال الهيكل الخارجي ، بل يكفي فقط الانتقال الذهني[2].

أما الرأي الثاني فيرى أنه يمكن انتقال المعلومة والحصول على البرنامج أو المعلومة بتشغيل الجهاز ورؤية المعلومة على الشاشة ، في هذه الحالة تنتقل من الجهاز إلى ذهن المتلقي ، والحيازة للأشياء غير المادية تكون من نفس الطبيعة غير المادية لتلك الأشياء ، وبالتالي نصل إلى إمكانية حيازة المعلومات عن طريق البصر وهو المقصود من جانب الجاني [3].

إلا أن فعل الاختلاس للبرامج أو المعلومات عن طريق الالتقاط الذهني لا يقع تحت طائلة العقاب بوصفه مكون جريمة السرقة , إلا إذا تم بنشاط مادي بتشغيل البرنامج أو نقله على دعامة مادية[4].

وبالتالي لا يتحقق بالالتقاط الذهني اختلاس المعلومات أو البرامج ، إذ يجب أن يتم الاختلاس بنشاط مادي كوضع المعلومات أو البرامج موضع التنفيذ أو نقلها إلى الغير على دعامة مادية أو إذاعتها ، لأن هذا النشاط المادي هو الذي ينتج عنه انتقال المعلومات ويقوم به الاختلاس [5].

---

[111] – نائلة عادل قورة ، مرجع سابق ، ص159.

Michel VIVANT et autres, Droit de l'informatique et des réseaux, Lamy. 2001. P 1837

[2] – هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن ، مرجع سابق ، ص 53.

[3] – عبد القادر القهوجي، مرجع سابق، ص98.

[4] - شيماء عبد الغني عطاء الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة ، الإسكندرية مصر 2007، ص41

[5] – عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الأولى، دار النهضة العربية القاهرة مصر 2001، ص296-297. عبد القادر القهوجي، مرجع سابق ، ص98.

وعلى ذلك فإن المعلومات أو البرامج قابلة للانتقال لكن الانتقال الذي تتحقق به السرقة هو الذي يكون بنشاط مادي على النحو السابق ذكره .

ولا يكفي لقيام جريمة السرقة أن يكون المال منقولا بل لابد أن يكون مملوك للغير ، فالمشرع لما رصد العقوبة لج

تحظى الأموال المعنوية بالحماية الجنائية المقررة بنصوص جرائم الأموال، فيجب أن تكون مملوكة للغير[1].

ثانيا- مدى صلاحية الأموال المعنوية كمحل لجريمة النصب :

لا يوجد خلاف حول صلاحية المعلومات لأن تكون محلا لجريمة النصب في حال ما كانت موجودة في دعامة مادية ، باعتبار أن هذه الأخيرة هي التي تكون محلا لهذه الجريمة[2] ، ولكن الخلاف يدور حول صلاحيتها إذا كانت في صورة مستقلة عن الدعامة المادية ، كالتالي:

1- الاتجاه الأول:

يرى هذا الاتجاه عدم صلاحية برامج الحاسوب والمعلومات لأن تكون محلا لجريمة النصب ويستند أصحابه إلى عدم وجود نشاط مادي ملموس يحصل له التسليم والاستلام في جريمة النصب وحتى لو فرضنا حدوثه فإنه لا يترتب عليه حرمان المجني عليه من حيازة هذه البرامج والمعلومات حيث تبقى تحت سيطرته التامة ، وهذا ما لا يتناسب وطبيعة النشاط الإجرامي في هذه الجريمة [3] .

---

[1] -عبد القادر القهوجي وعبد الله فتوح الشاذلي ، مرجع سابق، ص290.

[2]- نائلة عادل قورة ، مرجع سابق ، ص173.

[3] - كامل عفيفي عفيفي، مرجع سابق، ص164.

2- الاتجاه الثاني:

يقول هذا الاتجاه بصلاحية البرامج والمعلومات كمحل لجريمة النصب ، على أساس أن نصوص جريمة النصب تعطي أمثلة على المحال ، دون اشتراط أن تكون هذه الأشياء مادية أم معنوية [1] . حيث نصت المادة336 من قانون العقوبات المصري على المنقول دون تحديد لطبيعته ماديا أم معنويا مما يؤدي إلى دخول برامج الحاسوب والمعلومات ضمن الأشياء التي تقع عليها جريمة النصب[2] .

كما توسع المشرع الفرنسي في مجال جريمة النصب حسب نص المادة 1/313 من قانون العقوبات الفرنسي التي نصت على أن محل النصب يشمل نقود أو قيم أو أموال أو تقديم خدمات والرضاء بعمل يفرض التزاما أو إعفاءا [3]. ويلاحظ انه تخلى عن لفظ الأشياء واستخدم بدلا منها المال ، مما يسمح بأن يكون محل النصب من الأموال المادية أم المعنوية [4].

وذكر المشرع الجزائري أيضا الأموال والمنقولات في المادة 372 من قانون العقوبات الجزائري دون تقييد لطبيعتها ، من شأنه أن يجعل الأموال المعنوية صالحة كي تكون محلا أو موضوعا لجريمة النصب ، وهو الرأي الراجح في نظرنا مادام النص قابل للتفسير وفقا لمبدأ الشرعية [5].

الفرع الثاني: مدى صلاحية الأموال المعنوية كمحل لجرائم خيانة الأمانة والإخفاء والإتلاف

سنتعرض لمدى صلاحية الأموال المعنوية كمحل لجريمة خيانة الأمانة أولا، ثم الإخفاء والإتلاف، ثانيا ، على التفصيل الآتي :

---

[1] – المرجع نفسه ، ص164.

[2] – عبد القادر القهوجي، مرجع سابق، ص 93.

[3] - عبد الحليم رمضان ، مرجع سابق ، ص144

[4] –عبد الفتاح حجازي ،النظام القانوني لحماية التجارة الالكترونية ،الحماية الجنائية للتجارة الالكترونية، مرجع سابق،ص 225

[5]– أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومة للطباعة والنشر ، الجزائر ، 2006، ص31 .

أولا- مدى صلاحية الأموال المعنوية كمحل لجريمة خيانة الأمانة:

عددت المادة 376 من قانون العقوبات الجزائري الأشياء التي تقع عليها جريمة خيانة الأمانة وتضمنت في الأخير عبارة (أية محررات أخرى)[1]، وكذلك المادة 341 من قانون العقوبات المصري التي ذكرت لفظ (غير ذلك)، وتضمنت المادة 1/314 من قانون العقوبات الفرنسي (مال أيا كان) مما يسمح بإمكانية وقوع هذه الجريمة على أشياء غير مادية مثل برامج الحاسوب والمعلومات[2].

لقد توسع القضاء الفرنسي في تعريف فكرة البضائع بحيث تشمل برامج الحاسوب والمعلومات حيث تعبر بضاعة حتى لو لم تحتوي على التزام أو تبرأ من دين أو التزام[3].

مع ذلك ذهب رأي في الفقه الفرنسي والمصري إلى القول بعد إمكانية وقوع هذه الجريمة على الأموال المعلوماتية المعنوية، نظرا للطابع غير المادي لهذه الأشياء والذي يحول دون قيام جريمة خيانة الأمانة عليها [4].

ثانيا- مدى صلاحية الأموال المعنوية كمحل لجريمة الإخفاء والإتلاف:

1- مدى صلاحيتها كمحل لجريمة الإخفاء :

تنص المادة 387 عقوبات جزائري على أنه «كل من أخفى عمدا أشياء مختلسة أو مبددة أو متحصله من جناية أو جنحة في مجوعها أو في جزء منها ... ». و تنص المادة 44 مكرر

---

[1] - راجع المادة 376 من قانون العقوبات الجزائري .

[2] - عبد القادر القهوجي، مرجع السابق، ص 92.

[3] - محمد أمين الشوابكة ، مرجع سابق ، ص 205.

[4] - عبد الحليم رمضان، مرجع سابق ، ص 146

-Pascal Vergucht. La répression des delits .Informatique dans une perspective international,these.montpelier. 1996. P.115

من قانون العقوبات المصري على أنه : «كل من أخفى أشياء مسروقة أو متحصلة من جناية أو جنحة مع علمه بذلك يعاقب ... ».

ويلاحظ أن لفظ الأشياء التي وردت في هذه النصوص جاء عاما دون تخصيص مما يسمح للبرامج والمعلومات تصلح محلا لجريمة الإخفاء، وهو ما يستفاد أيضا من المادة 1/321 من قانون العقوبات الفرنسي [1].

وبالتالي فإن الأموال المعنوية تصلح كمحل لجريمة الإخفاء، لكون تلك النصوص لم تقصر

والمعنوية [2].

ولقد طبق القضاء الفرنسي متمثلا في محكمة النقض الفرنسية نص المادة 1/321 على المعلومات بمفردها مستقلة عن دعامتها المادية ، وأيده في ذلك الفقه الفرنسي ، إذ قضت محكمة النقض الفرنسية بإدانة شخص عن جريمة إخفاء لأنه تلقى من أحد العمال معلومات تتعلق بسر التصنيع مع علمه بأنها متحصلة من جريمة كما قضت أيضا بإدانة شخص عن ذات الجريمة لأنه قام بنسخ صورة عن مستند مسروق بمعرفة شخص مجهول الهوية مع علمه بذلك [3].

2- مدى صلاحية الأموال المعنوية كمحل لجريمة الإتلاف :

لاصعوبة في تطبيق نصوص الإتلاف إذا كان محل الجريمة مكونات مادية ولكن تثار صعوبة في مدى تطبيق هذه النصوص على الأشياء المعنوية ، وقد انقسم الفقه إلى اتجاهين : حيث يرى الاتجاه الأول أنه إذا اقتصر الإتلاف على المعلومات فقط ، فلا تقوم الجريمة لانتفاء الصفة المادية[4] .

---

[1] - راجع المادة 1/321 من قانون العقوبات الفرنسي .

[2] – عبد القادر القهوجي، مرجع السابق، ص109.

[3] – عبد الله حسين علي محمود، مرجع سابق، ص299- 300 .

[4] – كامل عفيفي عفيفي ، مرجع سابق، ص205.

أما الاتجاه الثاني الراجح يرى أن البرامج والمعلومات تصلح محل لجريمة الإتلاف استنادا إلى أن المادة 361 من قانون العقوبات المصري ، والمادة 434 عقوبات فرنسي جاءت عامة دون أن تحدد طبيعة المال، مما يعني إمكانية تطبيق هذه النصوص على كافة الأموال مادية أو معنوية [1].

وهوما يستفاد أيضا من المادة 407 من قانون العقوبات الجزائري ، والتي جاءت هي الأخرى عامة دون أن تحدد طبيعة المال، مما يعني إمكانية تطبيق هذه النصوص على كافة الأموال [2].

المطلب الثاني: النشاط الإجرامي في جرائم الأموال والتجارة الالكترونية

توصلنا سابقا إلى أن الأموال المعلوماتية المعنوية وفقا للفقه الراجح ينطبق عليها وصف المال وقابلة للتملك، إلا أن هذا لا يعني تمتعها بالحماية الجزائية المقررة في نصوص جرائم الأموال بصورة تلقائية، نظرا لطبيعتها الخاصة التي تميزها عن الأموال المادية.

لذلك سنتناول مدى خضوع الأموال المعنوية للنشاط الإجرامي في جريمة السرقة والنصب (الفرع الأول)، ومدى خضوعها للنشاط الإجرامي في خيانة الأمانة، والإتلاف والإخفاء (الفرع الثاني).

الفرع الأول: مدى خضوع الأموال المعنوية للنشاط الإجرامي للسرقة والنصب

تتفق جريمة السرقة مع جريمة النصب في أن كلاهما ينطوي على اعتداء على ملكية الغير إلا أن النشاط في جريمة النصب يتمثل في فعل الاحتيال الذي يؤثر على إرادة المجني عليه فيدفعه إلى تسليم المال ، بينما في جريمة السرقة هو الاستيلاء على المنقول بدون رضاء المالك أوالحائز السابق.[3]

---

[1] – هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن ، مرجع سابق ، ص 56 وما بعدها.

[2] - تنص المادة 407 من قانون العقوبات الجزائري "كل من خرب أو اتلف عمدا أموال الغير المنصوص عليها في المادة 396 بأية وسيلة أخرى كليا أو جزئيا يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 500 إلى 5000 دج". لمزيد راجع أم

[3] - عبد القادر القهوجي وعبد الله فتوح الشاذلي، مرجع سابق، ص123.

أولا- مدى خضوع الأموال المعنوية للنشاط الإجرامي في جريمة السرقة

تعد جريمة السرقة من جرائم الأموال التي تهدف إلى انتزاع الملكية، ويطلق عليها جرائم الإثراء لما تحققه من ثراء لذمة الجاني على حساب المجني عليه [1].

نص المشرع الجزائري على جريمة السرقة في المواد 350 إلى 369 ق ع ج ، أما المشرع المصري فنظمها في المواد311 إلى 327 ق ع م المصري [2].

وقدّ عرفت المادة 311 من قانون العقوبات الفرنسي الجديد السرقة بأنها أخذ شيء منقول للغير دون رضاه، وعلى ذلك استقر الفقه والقضاء في مصر وفرنسا [3].

وجريمة السرقة تتكون من ركنين، ركن مادي يتمثل في اختلاس مال منقول مملوك للغير، وركن معنوي يتمثل في القصد الجنائي العام والخاص[4].

لاتقع جريمة السرقة إلا بتحقق النشاط الإجرامي بالاختلاس أو الأخذ ، ويقصد بالاختلاس الاستيلاء على الحيازة الكاملة للشيء ، بدون رضاء المالك أو الحائز السابق، ولقد نادى بذلك التعريف الفقيه إميل جارسون وفقا لنظرية الحيازة في القانون المدني [5]، وبالتالي يتحقق الاختلاس في جريمة السرقة بتوافر الاستيلاء على الحيازة الكاملة للمال، وعدم رضاء المالك أو الحائز [6].

---

[1]-laure Rasât (Mechel) , Droit pénal spécial , Dalloz , paris. 1997 , p 56[1]

[2] – والسرقة لغة تعني أخذ الشيء خفية ، أما قانونا فإنه يستفاد من المادة 350 من قانون العقوبات الجزائري والتي تقابلها المادة 311 من قانون العقوبات المصري أن السرقة هي اختلاس مال منقول مملوك للغير.

[3] – هدى قشقوش ، شرح قانون العقوبات، القسم الخاص ، مرجع سابق ، ص 23.

[4] - عبد القادر القهوجي وعبد الله فتوح الشاذلي، مرجع سابق، ص263.

[5] – فالاختلاس حسب الاتجاه القديم

رضاء أو علم المجني عليه ، وهو ما لا يتحقق إلا بنقل الشيء ونزعه من مالكه أو حائزه إلى حيازة وسلطة الجاني .

[6] – حسن صادق المرصفاوي ، قانون العقوبات ، دار المعارف ، القاهرة مصر ، 1962، ص264.

لقد ثار خلاف فقهي حول صلاحية البرامج والمعلومات للاختلاس ، نظرا لطبيعتها المعنوية مما أدى إلى انقسام الفقهاء إلى اتجاهين ، على النحو الآتي :

1- الاتجاه القائل بصلاحيتها للاختلاس أو الأخذ :

يرى أنصار هذا الاتجاه أنه يمكن تصور وقوع فعل الاختلاس على برامج الحاسوب والمعلومات بصفة عامة مستقلة عن الدعامة التي تحويها ، ويشترطون أن يتم ذلك الاختلاس بنشاط مادي هو عملية النسخ أو التصوير التي عن طريقها نقل البرامج والمعلومات[1].

بناءا على ذلك لايتحقق الاختلاس بالنسبة للمعلومات التي تم التقاطها ذهنيا ، إلا بنشاط مادي كما إذا وضعت موضع التنفيذ أو تم بيعها أو نقلها إلى الغير على دعامة مادية أو إذاعتها[2].

ويبررون اشتراط مادية النشاط الإجرامي الذي يتحقق به فعل الاختلاس على المعلومات بأنه أمر تفرضه طبيعة الأشياء ، ذلك أن التسامح بالنسبة لأحد العناصر المكونة للجريمة يجب أن يقابله تشدد بالنسبة للعناصر الأخرى لتجنب تشويه مفهوم تلك الجريمة [3].

يستند هذا الاتجاه فيما ذهب إليه إلى الأحكام الصادرة من القضاء الفرنسي كالحكم الصادر من محكمة النقض في قضية (**lOGABAX**) ، والذي تتلخص وقائعه في أن أحد مهندسي

---

[1] - عبد القادر القهوجي ، مرجع سابق ، ص98 وما بعدها ، هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن ، مرجع سابق ، ص 62.

[2] - فبالنسبة للالتقاط الذهني للبرامج فإن الفقه اختلف في هذا الشأن، لكن الفقه الراجح يرى عدم وقوع جريمة السرقة في حالة الالتقاط الذهني للبرامج أو المعلومات لعدم وجود نشاط مادي، فهو يشترط لقيام الجريمة أن يكون هناك نشاط مادي . للتفصيل راجع نافذ ياسين، النظام القانوني لحماية التجارة الالكترونية، رسالة لنيل درجة الدكتوراه في الحقوق كلية الحقوق بجامعة عين شمس 2007 ص 388. وعبد القدر القهوجي، مرجع سابق، ص98. وعبد الحليم رمضان ، الحماية الجنائية للتجارة الالكترونية(دراسة مقارنة) ، دار النهضة العربية ،القاهرة، مصر، 2001 ، ص147 .

[3] - فالموافقة على وقوع الاختلاس على شيء معنوي مقترن بضرورة تحققه بنشاط مادي ، وتتحقق مادية الاختلاس بالنسبة للمعلومات إذا ما تم نقلها على دعامة مادية أيا كانت مادتها أو هيئته . للتفصيل راجع كامل عفيفي عفيفي، مرجع سابق ، ص 146 -147

شركة فصل من عمله ، فرفع دعوى ضد رب العمل وقدم للمحكمة تأييدا لدعواه صورتين كان قد نسخهما لمستندين من مستندات الشركة أمكنه الحصول عليها قبل فصله من العمل ، فقدم للمحاكمة بتهمة سرقة هذه المستندات وبرأته محكمة أول درجة ، وتم تأييد حكم البراءة في الاستئناف على أساس انتفاء نية التملك ، ولكن محكمة النقض الفرنسية نقضت الحكم السابق لأن القانون لم يشترط انتزاع الشيء ، وأن الاختلاس يمكن أن يتحقق ولو كان الشيء بين يدي الجاني قبل الاستيلاء عليه على سبيل اليد العارضة ، ولأن الجاني استولى على مستندات الشركة لمصلحته الشخصية ودون علم ورضاء رب العمل المالك لها أثناء الوقت اللازم لتصويرها[1].

كما أصدر القضاء الفرنسي حكم آخر **باسم بوركاين** والذي تتلخص وقائعه من أن عاملين من عمال مطبعة بوركا ين قاما وبأدوات المطبعة بتصوير 47 شريطا عبارة عن قوائم بأسماء العملاء الأثرياء الذين يتعاملون مع المطبعة ثم أخذا بعد ذلك 70 شريطا أخرى، وقاما بتصويرها خارج المطبعة وعلى ماكيناتهم الخاصة وقدما للمحاكمة بتهمة جريمة السرقة وصدر الحكم بإدانتهما ورفضت محكمة النقض نقض هذا الحكم لتوافر جريمة السرقة ضدهما والتي تتمثل في سرقة بعض الأشرطة ، وسرقة محتوى بعض الأشرطة الأخرى [2].

وهكذا فإن هذا الاتجاه الفقهي يؤيد وقوع فعل الاختلاس على المعلومات مستقلة عن دعامتها المادية الأصلية إذا تم نسخها دون نقل لها من مكان تواجدها دون رضاء صاحبها، إلا أن قيمتها قد انقضت بفعل الاختلاس لأن صاحبها يكون قد فقد حقه في احتكار استغلالها [3].

---

[1] – محمد مرهج الهيتي ، التكنولوجيا الحديثة والقانون الجنائي ،الطبعة الأولى ، دار الثقافة للنشر والتوزيع ، عمان ، الأردن ، 2004.، ص208.

[2] – صدرت في هذا الشأن أحكام أخرى مثل الحكم المعروف باسم HERBERTEAU – وحكم آخر يعرف باسم Montbeliard ، تعتبر أن نسخ أو تصوير البرامج أو المعلومات بصفة عامة وبدون علم أو رضاء صاحبها لمصلحته الشخصية مكونا لجريمة السرقة .

[3]– ففعل الاختلاس وقع من خلال عملية نسخ المعلومات الموجودة في الدعامة ، وأدى إلى انتقالها من تلك الدعامة إلى الصورة أي من ذمة إلى ذمة ، بالرغم من أن المعلومات والبرامج مازالت بين يدي مالكها وتحت سيطرته إلا أن قيمتها قد انقضت بفعل الاختلاس لأن صاحبها يكون قد فقد حقه في احتكار استغلالها .

2-الاتجاه الرافض لصلاحيتها للاختلاس أو الأخذ :

رفض هذا الاتجاه إمكانية وقوع جريمة السرقة على المعلومات والبرامج مستقلة عن دعامتها المادية ، نظر للطبيعة غير المادية للبرامج والمعلومات، وكونها تبقى بين يدي صاحبها أي تظل تحت سيطرة مالكها أو حائزها بالرغم من نسخها بدون رضاء أو عدم علم المجني عليه [1].

إلا أن أنصار هذا الاتجاه لم يتفقوا واحد حول تفسير أحكام محكمة النقض ، كالآتي :

أ- الرأي الأول:

يرى هذا الرأي أن السرقة وقعت على الأصل أثناء المدة اللازمة لتصويره وأن الجاني هنا قد ارتكب جريمة استعمال لهذا الأصل حتى ولو لم يستمر الاستيلاء لفترة طويلة من الزمن ، ويستند أنصاره هذا إلى ما استقر عليه التطور القضائي بشأن سرقة الاستعمال وبصفة خاصة استعمال السيارات ، إذ أن محكمة النقض الفرنسية لم تشترط أن يكون الاستيلاء على السيارة تم على سبيل [2].

وهكذا فإن هذا الرأي يرى بوقوع سرقة الاستعمال على الدعامة التي تحتوي على المعلومات، حتى لو أن هذا الاستيلاء لم يستمر إلا الوقت اللازم للنسخ [3].

إلا أن جانب من الفقه المصري يرى عكس هذا الرأي ويعتبر أنها سرقة استعمال أو منفعة للبرامج في حق من يستولي على نسخة من المعلومات دون أصلها الذي يبقى في حوزة صاحبها[4].

---

[1] - إلا أن هناك اتجاه آخر يفرق بين حالتين ، فإذا كانت هذه المعلومات مجانية أي متاحة للجمهور للإطلاع عليها أو نسخها بدون مقابل فلا تقوم الجريمة في حالة نسخها أو الإطلاع عليها ، لكن إذا كانت هذه المعلومات متاحة للكافة مقابل مبلغ نقدي ، فإن الاعتداء عليها يشكل جريمة سرقة منفعة إذا وجد نص يعاقب على سرقة المنفعة .

[2] - يلاحظ أن المشرع الجزائري لم ينص على سرقة الاستعمال لا بنص عام ولا خاص على خلاف التشريعات الأخرى كالمصري والفرنسي الذين نصا عليها بنص خاص ، بالاستيلاء على السيارات بغير حق وبدون نية التملك.

[3] - عبد القادر القهوجي، مرجع سابق ، ص1003.

[4] - محمد مرهج الهيتي ، مرجع سابق ، ص232.

ب- الرأي الثاني:

يرى هذا الرأي أن السرقة وقعت على الآلة وليس أصل البرامج أو المعلومات أي الدعامة وأنها سرقة وقت الآلة ، أي أنه يعتبر أن فعل الأخذ أو الاختلاس وقع على الآلة ذاتها وأن هذا الفعل يتمثل في الاستيلاء على الوقت اللازم لنسخ صور هذه البرامج أو المعلومات الأصلية[1]، لكن هذين الرأيين يصطدمان بعقبة مؤداها أنه من الممكن الحصول على صورة للبرنامج أو نسخ صورة منه دون الاستيلاء على الأصل أو الماكينة وذلك إذا تم هذا النسخ من خلال طرفية تتصل بالحاسب المركزي سلكيا أو لاسلكيا بحيث يحرم صاحب البرنامج أو الآلة ولو لفترة قصيرة من استعمال أيهما [2]، ولتجاوز هذه العقبة ذهب رأي إلى تكييفها على أنها سرقة التيار الكهربائي اللازم لاستخراج الصورة لكن البعض الأخر استبعد جريمة سرقة التيار الكهربائي[3].

وبالتالي فإن أنصار هذا الرأي يرفضون صلاحية البرامج والمعلومات للاختلاس أو الأخذ لأنها تبقى تحت سيطرة صاحبها الأصلي ولا تخرج من حيازته على الرغم من نسخها وتصويرها[4].

إلا أننا نميل إلى الاتجاه المؤيد لوقوع جريمة السرقة على البرامج والمعلومات ، ويتحقق النشاط المادي للاختلاس بالنسخ أو الاستخدام للبرامج والمعلومات أو نقلها على دعامة ، لكنها تشكل سرقة استعمال ، والتي تقوم على الاستيلاء على المال بنية استعماله لا بنية تملكه فالاستيلاء هنا ينحصر في الحصول على منفعة الشيء دون أصله الذي يبقى في حيازة صاحبه[5] .

---

[1]- ويتفق هذا الرأي مع الرأي الأول في كون السرقة سرقة استعمال إلا أنهما يختلفان في محل الاختلاس فبينما يرى الأول أن السرقة سرقة استعمال للأصل يرى الثاني أن السرقة سرقة استعمال الآلة .

[2] - عبد القادر القهوجي، مرجع سابق، ص104.

[3] -عفيفي كامل عفيفي ، مرجع سابق، ص154.

[4] - عبد الحليم رمضان، مرجع سابق ، ص148.

[5] -عبد القادر القهوجي ، مرجع سابق ، ص104.

والواقع أن الاختلاف حول مدى صلاحية الأموال المعنوية للاختلاس مازال قائما بل إن الرأي الغالب مازال يتبنى الاتجاه المعارض، مما يعكس مدى الحاجة إلى تدخل تشريعي من شأنه أن يحسم هذا الجدل الفقهي [1].

ثانيا- مدى خضوع الأموال المعنوية للنشاط الإجرامي في جريمة النصب

نظم المشرع الجزائري جريمة النصب في المادتين372 و373 ق ع ج ، أما المشرع المصري فنظمها بالمادة 336 ق .ع .م ،المقابلة المادة 405 ق .ع .ف.

يقصد بجريمة النصب الاستيلاء على الحيازة الكاملة عمدا عن طريق الاحتيال على مال مملوك للغير[2]، ولقيامها لابد من توافر ركنين ، ركن مادي يتمثل في الاستيلاء على مال الغير بإحدى طرق الاحتيال المحددة قانونا ، وركن معنوي يتمثل في القصد الجنائي العام والخاص [3].

ويتمثل النشاط الإجرامي في جريمة النصب في الاحتيال [4]، والذي يتحقق إذا لجأ الجاني إلى استعمال إحدى الطرق الاحتيالية المحددة قانونا ، كأن يحمل المجني عليه على تسليمه دعامة مادية مثبت عليها أحد البرامج و المعلومات أو نسخة منها، فتقع جريمة النصب في هذه الحالة.

لكن الإشكال يطرح حول إمكانية ممارسة أفعال الاحتيال على النظام المعلوماتي بقصد الحصول على البرامج والمعلومات، وفي إطار التصدي لهذه الأشكال ، انقسم إلى اتجاهين:

---

[1] - ولقد تضمن مشروع قانون العقوبات الفرنسي الجديد على تجريم سرقة البرامج والمعلومات وذلك في نص المادة 307 ، لكن هذه الخطوة لم يكتب لهذه الخطوة النجاح . انظر هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن، مرجع سابق ، ص122 . راجع كامل عفيفي عفيفي ، مرجع سابق، ص154.

[2] - عبد القادر القهوجي وعبد الله فتوح الشاذلي، مرجع سابق، ص123.

[3] - هدى قشقوش ، شرح قانون العقوبات، القسم الخاص، مرجع سابق ، ص141 وما بعدها.

[4] – ويقصد بالاحتيال تغيير الحقيقة بالنسبة لواقعة ما تغييرا يؤدي بالمجني عليه إلى تسليم ماله إلى الجاني ، فجوهر الاحتيال الكذب الذي يلزم أن يتجسد في إحدى وسائل الاحتيال التي حددها المشرع على سبيل الحصر، أي أنه لقيام فعل الاحتيال يجب أن يتوافر الكذب أولا وأن يتخذ هذا الكذب صورة إحدى الوسائل الاحتيالية المحددة قانونا.

1-الاتجاه المعارض :

يرى هذا الاتجاه عدم إمكانية وقوع فعل الاحتيال على الحاسوب ، وبالتالي لا تتوافر جريمة النصب ، لأن جريمة النصب تستوجب أن يكون الجاني والمجني عليه أشخاص طبيعيين[1].

ولكي يطبق النص الجنائي لجريمة النصب يلزم أن يكون الجاني قد خدع شخص مثله، ومن ثم فإنه إذا تم خداع الشخص المكلف بمراقبة البيانات أو مراجعتها أو فحصها تقوم جريمة النصب إذا توافرت باقي عناصرها [2].

وحتى لو فرضنا إمكانية وقوع التسليم والاستلام في هذه الحالة من خلال الطرق الاحتيالية التي يلجا إليها والتي يترتب عليها وقوع المجني عليه في غلط يدفعه إلى نقل البرامج شفافيا أي عن طريق قول محتويات برنامجه الذي يلتقطه الجاني ويحفظه في ذاكرته ، فإنه لن ينتج عن ذلك حرمان المجني عليه من المعلومات التي نقلها بالقول بل تظل تحت سيطرة من نقلها وفي حوزته وهو أمر إن كان يتفق مع طبيعة المعلومات ،إلا أنه لا يتفق مع طبيعة النشاط الإجرامي في جريمة النصب[3].

2-الاتجاه المؤيد:

يرى هذا الاتجاه إمكانية وقوع الاحتيال على الحاسوب وتصور إيقاعه في غلط ويتمثل في الفقه الانجلوساكسوني ، وجانب من الفقه الفرنسي ، كالآتي :

---

[1] – كامل عفيفي عفيفي، مرجع سابق، ص169. عبد القادر القهوجي ، مرجع سابق ، ص106.

[2] – وأخذت بهذا الاتجاه العديد من التشريعات منها مصر وألمانيا والدا نمارك وفلندا واليابان والنرويج ولكسمبورغ وايطاليا وذلك لعدم وجود نشاط مادي يتحقق به التسليم والاستلام في جريمة النصب . راجع نافذ ياسين، مرجع سابق، ص 402.

[3] – محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة ، الإسكندرية، مصر 2004، ص125.

أ- الفقه الانجلوساكسوني :

يمكن تطبيق النصوص الخاصة بجريمة النصب على الاحتيال المعلوماتي في هذه التشريعات لأن النصوص وردت عامة بحيث يمكن تطبيق أحكامها على الاحتيال الواقع على الحاسوب [1].

ومن أمثلة تلك التشريعات ، التشريع العقابي الانجليزي لعام 1978 ، حيث نص في المادة 16 منه على معاقبة كل من حصل على نحو غير مشروع وبأي وسيلة خداع سواء لنفسه أو للغير على منفعة مادية ، لكن القضاء الانجليزي تردد في تطبيق هذا النص على بعض الوقائع فاضطر المشرع الانجليزي إلى تعديل قانون 1983 اعتبر فيه خداع الآلة من قبيل الاحتيال [2].

كما تبنى التشريع الكندي مفهوما موسعا للاحتيال ، بحيث تطبق المادتين 387 و388 من قانون العقوبات على النصب المعلوماتي ، كما تبنى التشريع الاسترالي مفهوما موسعا للنصب [3].

كما عاقبت بعض قوانين الولايات المتحدة الأمريكية على الاستعمال غير المشروع للحاسب الالكتروني بهدف ارتكاب أفعال الغش والاعتداء، أما على النطاق الفيدرالي فقد أصدر المشرع الأمريكي في أكتوبر 1984 عام 1996 [4].

ب-الفقه الفرنسي:

يرى جانب من الفقه الفرنسي إمكانية وقوع فعل الاحتيال على نظام الحاسوب بقصد الاستيلاء على الأموال ، واستندوا في ذلك إلى أن خداع الأنظمة المعلوماتية يدخل ضمن الطرق الاحتيالية

---

[1] – محمد علي العريان مرجع سابق، ص 126. نافذ ياسين، مرجع سابق، ص 408

[2] – عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية ، الكتاب الثاني :الحماية الجنائية للتجارة الالكترونية مرجع سابق ، ص 219.

[3] – أمين الشوابكة ، مرجع سابق ، ص 187-188. شيماء عبد الغني عطاء الله مرجع سابق، ص 362.

[4] – كما قام المشرع في الولايات المتحدة الأمريكية بإصدار تشريعات تعطي مفهوما واسعا للأموال بحيث تشمل كل شيء ينطوي على قيمة، ويدخل في نطاقها كافة الأموال سواء كانت مادية أو معنوية على نحو يشمل النصب على كل الأموال . للتفصيل انظر كامل عفيفي عفيفي، مرجع سابق، ص171-172. محمد علي العريان مرجع سابق، ص127.ذ

حيث تتوافر فيه بجانب الكذب واقعة خارجية هي إبراز أو تقديم المستندات أو المعلومات المدخلة إلى الحاسوب ، كما تتحقق هذه الطرق كذلك باستخدام المستندات غير الصحيحة التي يخرجها الحاسب بناءا على ما وقع في برامجه أو بياناته لكي يستولي على أموال الغير بدون وجه حق[1].

ويستند هذا الاتجاه إلى حكم محكمة النقض الفرنسية في حكمها في 4 ماي 1978 عندما طبقت عقوبة النصب على شخص دخل بسيارته إلى أماكن انتظار السيارات ، وبدلا من وضع النقود الأصلية المطلوبة في عداد الأماكن المعدة للانتظار نظير هذه الخدمة ، قام بوضع قطعة معدنية عديمة القيمة فيه ، وترتب على ذلك تشغيل الماكينة وتحريك عقاربها ، وكان سندها في ذلك الحكم أن وضع القطعة المعدنية عديمة القيمة في العداد يعد من قبيل الطرق الاحتيالية [2] .

والواقع أن الاتجاه الثاني الذي قال بإمكانية وصلاحية البرامج والمعلومات للاحتيال هو الراجح ، فمن المتصور وقوع الاحتيال بالتلاعب في البرامج والمعلومات ، ومتى وقع التلاعب في هذه الأموال المعنوية بإحدى الوسائل الاحتيالية المحددة قانونا قامت جريمة النصب .

إلا أنه من الواجب المسارعة دون تباطأ نحو سن نصوص جزائية خاصة بتجريم هذا السلوك بصفة صريحة ، أو السعي نحو تعديل النصوص الحالية بحيث تستوعب في إطارها التجريمي الاحتيال على الأموال المعلوماتية المعنوية.

ولقد تنبهت بعض التشريعات لهذا الأمر وتفادت النقص التشريعي بسن نصوص تجرم الاحتيال المعلوماتي ، كالتشريع الانجليزي الذي أصدر نص خاص جرم فيه مسألة غش الكمبيوتر في قانون إساءة استخدام الكمبيوتر عام 1990 وأيضا جرم التشريع الفرنسي الغش المعلوماتي بالقانون رقم 19/88[3]، وكذا المشرع الجزائري بالقانون رقم 15/04[4] .

---

[1] – محمد علي العريان مرجع سابق، ص127.

[2] – محمد علي العريان مرجع سابق، ص126. محمد أمين الشوابكة ، مرجع سابق، ص 408.

[3] – شيماء عبد الغني عطاء الله ، مرجع سابق ص63.

[4] – القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004المعدل والمتمم للأمر رقم 66 /156 الموافق في 8 يونيو سنة 1966 المتضمن قانون العقوبات، ج . ر عدد71 مؤرخة في 2004.

الفرع الثاني: مدى خضوع الأموال المعنوية للنشاط الإجرامي لخيانة الأمانة والإتلاف والإخفاء

سنتعرض لمدى خضوع الأموال المعلوماتية المعنوية للنشاط الإجرامي في جريمة خيانة الأمانة أولا، ثم في جريمتي الإخفاء والإتلاف ثانيا، كالآتي:

أولا-مدى خضوع الأموال المعنوية للنشاط الإجرامي في جريمة خيانة الأمانة

نظم المشرع الجزائري أحكام جريمة خيانة الأمانة في المواد 376 إلى 382 من قانون العقوبات الجزائري، والتي تقابلها المواد 341 وما بعدها من قانون العقوبات المصري و314 وما بعدها من قانون العقوبات الفرنسي الجديد.

ويمكن تعريف جريمة خيانة الأمانة بأنها استيلاء الجاني على مال منقول مملوك لآخر يحوزه بناءا على عقد من عقود الأمانة[1].

يتمثل النشاط الإجرامي في جريمة خيانة الأمانة في الاستيلاء على الحيازة الكاملة للشيء المسلم إليه من قبل , ويتحقق هذا الاستيلاء طبقا للمادة 375 من قانون العقوبات الجزائري بالاختلاس [2]، أو التبديد [3]، وأضاف المشرع المصري الاستعمال في المادة341 ق ع م[4]، أما المشرع الفرنسي فقد قصر النشاط الإجرامي على الاختلاس في المادة 314 ق .ع .ف.

---

[1] – محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة ،1994، ص132.

[2] – ويقصد بالاختلاس في جريمة خيانة الأمانة كل فعل يكشف له الجاني عن تغيير نية من حائز حيازة ناقصة إلى حيازة كاملة لحسابه بأن يظهر بمظهر المالك.

[3] – يقصد التبديد تصرف الأمين في المال المؤتمن عليه تصرفا من شأنه أن يخرجه من حيازته مما يفصح أن اتجاه نيته إلى تملكه , ويستوي أن يكون التصرف قانونيا كالبيع أو ماديا كإتلاف أو استهلاك الشيء , وسواء كان التبديد كلي أمجزئي. للتفصيل راجع حسن صادق المرصفاوي ، مرجع سابق ، ص 544 .

[4] – ويعني الاستعمال استخدام الجاني المال المسلم إليه استخداما يستنفذ فيه قيمته كلها أو بعضها مع بقاء مادته على حالها، كقيام الناشر بطبع كمية من الكتب أكثر مما اتفق عليه ويستولي على القدر الزائد.

أو الاستعمال ، قامت جريمة خيانة الأمانة ، ولا يثار إشكال إذا كان محل الجريمة شيء مادي ، لكن الصعوبة إذا كان شيء معنوي فيطرح تساؤل حول مدى إمكانية صلاحيتها للاستيلاء [1] .

يتحقق الاختلاس في المجال المعلوماتي بكل فعل يفصح به الأمين على نيته في إضافة المال إلى ملكه ، كامتناع الأمين عن رد القرص المثبت عليه البرنامج أو المعلومات ، أو إذا تصرف فيه إلى شخص آخر، أو امتناع العميل عن رد بطاقة الائتمان إلى البنك بعد انتهاء صلاحيتها أو إلغائها [2].

كما تقع جريمة خيانة الأمانة بالاستعمال في الحالة التي يكون فيها الأمين نسخ البرامج والمعلومات لحسابه الخاص متجاوزا الاتفاق الذي يربطه بصاحبها ، ولاشك أن النسخ هنا يؤدي إلى استنزاف جزئي لقيمتها التجارية[3]، وتطبيقا لذلك قضت محكمة استئناف (Grenoble) سنة 1990 بوقوع جريمة خيانة الأمانة في حق مستخدم في إحدى الشركات قام بنسخ أشرطة العمل [4].

وقضت محكمة Créteil أيضا في حكم لها صادر في 15جانفي عام 1985، بأن حامل البطاقة الائتمانية التي طالب البنك بردها لاستخدامها بالمخالفة للشروط التعاقدية والذي يستمر في استخدامها يعد مرتكبا لجريمة خيانة الأمانة [5].

---

[1] – عبد الفتاح حجازي، النظام القانوني الحماية التجارة الالكترونية، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية مرجع سابق، ص240. شيماء عبد الغني عطاء الله، مرجع سابق، ص70.

[2] – عبد القادر القهوجي، مرجع سابق، ص106-107. كامل عفيفي عفيفي، مرجع سابق ، ص165

[3] – عبد القادر القهوجي، مرجع سابق، ص106-107.

[4] – كما قضت محكمة الاستئناف بهولندا بارتكاب جريمة خيانة الأمانة في حق محلل برامج بإحدى الشركات قام بنسخها على أقراص بغرض إنشاء مشروع خاص . للتفصيل راجع شيماء عبد الغني عطاء الله، مرجع سابق، ص73. وانظر أيضا:

-languier (J) ,Droit pénal spécial , Dalloz , 2eme édition , paris 1998 p25-252

[5] – لقد ثار خلاف فقهي حول تجريم من يتجاوز حامل البطاقة رصيده لكن الفقه الراجح ذهب إلى عدم تجريمه بل يرتب المسؤولية العقدية استنادا إلى محكمة النقض الفرنسية . للتفصيل انظر نائلة عادل قورة ، مرجع سابق ، ص579.

ويرى البعض أن جريمة خيانة الأمانة تقع على المعلومات في الحالة التي ينقل فيها الأمين شفويا المعلومات إلى شخص آخر يضعه موضع التنفيذ لحساب الأمين أو يبيعها إلى ذلك الشخص لكن في الحقيقة أن وضع المعلومات موضع التنفيذ ينطبق عليه وصف الاستعمال في جريمة خيانة الأمانة ،أما أذا تم بيع المعلومات بالنقل الشفوي فلا يتحقق النشاط الإجرامي لهذه الجريمة [1].

على الرغم من أن يحقق النشاط الإجرامي المتمثل في الاستيلاء على الحيازة الكاملة كالاختلاس أو التبديد أو الاستعمال شرط أساسي لقيام جريمة خيانة الأمانة للأموال المعنوية [2]، لكن لا يكفي ذلك بل لابد أن يتم ذلك الاستيلاء على البرامج والمعلومات المسلمة إليه بناء على عقد من عقود الأمانة المحددة قانونا في المادة 376 من قانون العقوبات الجزائري [3].

بالإضافة إلى عناصر الركن المادي السابقة ، فإنه يلزم أيضا لقيام جريمة خيانة الأمانة عنصر الضرر لاكتمال الركن المادي ، ويستوي أن يكون الضرر ماديا أو أدبيا ، أو حقيقيا ، أو احتماليا ولهذا فإنه لابد أن يترتب على الاستيلاء على المعلومات بإحدى الصور المحددة قانونا إلحاق الضرر بالمجني عليه ، و توافر الضرر من عدمه مسألة موضوعية تقدرها محكمة الموضوع في كل حالة [4].

---

[1] - عبد القادر القهوجي، مرجع سابق،107

[2] – وفي مجال البرامج والمعلومات فأن أكثر عقود الأمانة التي يشهد الواقع العملي كثرة وجودها على عقود العمل والوكالة وعارية الاستعمال ، فالعديد من أفعال التبديد والاختلاس والاستعمال التي يكون محلها البرامج ترتكب من قبل العاملين المعهود إليهم بما يكون أساسها عقد العمل ففي إطار عقد العمل قد يمنح للعاملين برامج تمكنهم من القيام بأعمال معينة يتطلبها العمل ، لكنهم يقومون باختلاسها أو تبديدها أو استعمالها . للتفصيل كامل عفيفي عفيفي، مرجع سابق، ص195.

[3] – يلاحظ أن المشرع الفرنسي لم يحدد عقود الأمانة في المادة 314 /1 ، لأن المسائل الاقتصادية في حالة تطور مستمر وهذا ما القي على القضاء الفرنسي عبء تحديد عقود الأمانة .

[4] –عبد الفتاح حجازي،النظام القانوني لحماية للتجارة الالكترونية،الحماية الجنائية للتجارة الالكترونية، مرجع سابق ، ص254.

ثانيا- مدى خضوع الأموال المعنوية للنشاط الإجرامي للإخفاء والإتلاف

سنبحث مدى خضوع الأموال المعنوية للإخفاء ، ثم مدى خضوعها للإتلاف ،على التفصيل الآتي:

1 -مدى خضوع الأموال المعنوية للنشاط الإجرامي في جريمة الإخفاء

عالج المشرع الجزائري جريمة إخفاء الأشياء المسروقة في المواد من387 الى389 من قانون العقوبات، أما المشرع المصري فتناولها في المادة 344 مكرر من قانون العقوبات، أما المشرع الفرنسي عالجها في المادة 221 /1 من قانون العقوبات .

يتمثل الركن المادي في جريمة الإخفاء في إخفاء أشياء أو أموال مسروقة، ويشكل الإخفاء النشاط الإجرامي [1]، بينما تعد الأشياء المسروقة محلا لجريمة الإخفاء [2].

ولما كان النشاط الإجرامي لجريمة الإخفاء لا يتحقق إلا إذا أتى الجاني نشاطا ماديا يدخل به الشيء في حيازته ، فإن الفقه التقليدي قال بعدم صلاحية البرامج والمعلومات للإخفاء ، نظرا لطبيعتها غير المادية من جهة ، ولكون فعل الاختلاس يرتكز على فعل ونشاط مادي للاستلام أو الاحتجاز ، فالإخفاء يجب أن يتم بنشاط مادي تطبيقا للمبدأ القائل (لا عقاب جنائي على سلوك ما بدون نشاط مادي) ولذلك لا يتصور وقوع الإخفاء على شيء معنوي كالبرامج والمعلومات [3].

---

[1] - إن الإخفاء هو كل اتصال فعلي بالمال المختلس أو المبدد أو المتحصل من جناية أو جنحة مهما كان سببه أو الغرض منه ، ومهما كانت ظروف زمانه أو مكانه أو سائر أحواله.

[2] - ولا يشترط في جريمة الإخفاء أن يقع الإخفاء على ذات الشيء المتحصل ، بل يمكن أن يقع على ما يقابله كثمن الشيء المسروق . راجع رمسيس بهنام ، النظرية العامة للقانون الجنائي ، الطبعة الثانية ، منشأة المعارف ، الإسكندرية مصر 1968 ، ص79. عبد القادر القهوجي وعبد الله فتوح الشاذلي، مرجع سابق، 309.

[3] - عبد القادر القهوجي، مرجع سابق ، ص108-109.

إلا أن الفقه الحديث قال بصلاحية المعلومات للإخفاء، واستند في ذلك إلى ما قضته محكمة النقض الفرنسية في قضية (Maillot) الذي تلقى من شخص أجير سر صناعي[1]، كما أدانت محكمة النقض الفرنسية بجريمة الإخفاء في قضية أخرى شخص أجير ألتقط صورة لوثيقة سرية تتعلق بالوظيفة، سبق أن تم سرقتها بواسطة شخص من الغير وظلت مجهولة [2]. وبذلك فإن هذين الحكمين ينطويان على إجازة إخفاء المعلومات والبرامج بغض النظر عن دعامتها المادية [3].

وبناءا على ما سبق يمكن القول أن الأموال المعنوية يمكنها أن تكون صالحة للإخفاء متى تم ذلك بنشاط مادي، لأن الإخفاء لا يمكن أن يكون إلا ماديا.

والحقيقة أن الاختلاف حول صلاحية البرامج والمعلومات الإخفاء يحتاج إلى تدخل تشريعي من شأنه أن يظل بحمايته هذه الأموال، لإزالة كل لبس أو غموض يمكن أن يحيط بشأن تطبيق نصوص جريمة الإخفاء على البرامج والمعلومات [4].

2- مدى خضوع الأموال المعنوية للنشاط الإجرامي في جريمة الإتلاف :

نص المشرع الجزائري على جريمة الإتلاف في المادة407 من قانون العقوبات، المقابلة للمادة 371 مكرر من قانون العقوبات المصري، والمادة 322 /1 من قانون العقوبات الفرنسي.

واختلف الفقه بين مؤيد ومعارض لوقوع جريمة الإتلاف على المعلومات، على التفصيل الآتي:

---

[1] – عبد الله حسين محمود، مرجع سابق، ص302. نائلة عادل قورة ، مرجع سابق ، ص184.

[2] - ونستخلص أن القضاء الفرنسي قد حاول تطبيق نصوص جريمة الإخفاء وتطويعها على إخفاء المعلومات ، فاعتبر أن التقاط صورة لوثيقة متحصله من سرقة في قضية(مايلو)، والحصول على سر صناعي وتطبيقه في قضية هو خير تعبير للنقل المادي المتعلق بحيازة المعلومة في القضية الثانية .

[3] – عبد الله حسين محمود، مرجع سابق، ص302.

[4] – نائلة عادل قورة ، مرجع سابق ، ص187.

ا-الرأي المؤيد:

يرى هذا الرأي إمكانية جريمة الإتلاف على المعلومات الالكترونية وذلك لان المواد السالفة الذكر جاءت عامة ولم تحدد طبيعة الأموال محل الجريمة ولم تقيد النشاط الإجرامي في جريمة الإتلاف بوسيلة معينة ، إذ هي من الجرائم ولهذا لا يوجد ما يحول دون وقوع جريمة الإتلاف على الأموال المعنوية خاصة وأن المشرع لم يحدد طريقة بعينها لوقوع الجريمة [1].

كما يلاحظ الفقه المصري أن المادة 371 مكرر من ق .ع . م ، نصت على أموال ثابتة أو منقولة ولم تحدد طبيعتها، مما يعني أنها تنطبق على كافة الأموال المادية والمعنوية [2].

كذلك اتجه التفسير القضائي في بعض الدول إلى وقوع جريمة الإتلاف على المعلومات كالمحكمة العليا بالنمسا قبل صدور القانون الخاص بالحاسوب سنة 1987 الذي تضمن جريمة العبث بالمعلومات المبرمجة[3]، كما اتجه القضاء الفرنسي إلى تطبيق نصوص الإتلاف على المكونات المعنوية ، حيث أدانت محكمة باريس عام 1999أحد الأشخاص بتهمة إتلاف المعلومات لقيامه بإدخال بيانات غير صحيحة إلى نظام الحاسوب، كما أدانت محكمة جنح ليموج بفرنسا عام 1994أحد الأشخاص بتهمة الإتلاف لقيامه بإدخال برنامج حصان طروادة إلى نظام الحاسوب [4].

---

[1]- لذلك فانه من المتصور أن يتجه الجاني بنشاطه الإجرامي إلى المعلومات والدعامة المسجل عليهما معا أو إلى المعلومات فقط، وقد تقع الجريمة عن طريق الاتصال المباشر بالجهاز أو الاتصال عن بعد . راجع عبد القادر القهوجي، مرجع سابق، ص112. راجع أيضا محمد عبيد الكعبي ، الحماية الجنائية للتجارة الالكترونية ، دار النهضة العربية ، القاهرة مصر، 2010 ص391. انظر أيضا كامل عفيفي عفيفي، مرجع سابق، ص206

[2] – كامل عفيفي عفيفي، مرجع سابق، ص 111.

[3] – شيماء عبد الغني عطاء الله، مرجع سابق ، 76.

[4]- انظر محمد عبيد الكعبي ، الحماية الجنائية للتجارة الالكترونية ، مرجع سابق ص390. كامل عفيفي مرجع سابق، ص2

وقد حسمت بعض التشريعات هذا الخلاف بإصدارها نص خاص بجريمة إتلاف البرامج والمعلومات، كقانون عقوبات ولاية واشنطن بالولايات المتحدة الأمريكية، وقانون العقوبات الفرنسي بالمادة 2/323 ، وقانون العقوبات الجزائري بالمادة 394 مكرر فقرة 2 التي تنص على أنه تضاعف العقوبة إذا ترتب على الدخول أو البقاء حذف أو تغيير لمعطيات المنظومة ، كما نصت المادة 394 مكرر 1 على معقبة كل من أزال معطيات النظام المعلوماتي[1] .

ب- الرأي المعارض:

عارض هذا الرأي وقوع جريمة الإتلاف على البرامج والمعلومات لطبيعتها غير المادية من جهة، ومن جهة أخرى أنها غير قابلة للتملك [2].

إلا أن الرأي الراجح في الفقه يتجه إلى وقوع جريمة الإتلاف على البرامج والمعلومات، رغم

هذه المعلومات تخضع لنصوص الإتلاف[3].

وعليه فان الأموال المادية لا تـ ا جرائم الأموال ، لكن الإشكال يطرح بالنسبة للأموال المعنوية كالبرنامج أو المعلومات
ولذلك عارض بعض الفقهاء اعتبارها محلا لجرائم الأموال، لعدم قاب ا انتقاله من حيازة المجني عليه إلى حيازة الجاني [4] .

---

[1] – راجع المدتين 394مكرر و394المادة مكرر 1 من قانون العقوبات الجزائري .

[2] – عبد القادر القهوجي ، مرجع سابق، ص111. جميل عبد الباقي الصغير ، القانون الجنائي والتكنولوجيا الحديثة ، الطبعة الأولى ، دار النهضة العربية، القاهرة مصر ، 1996، 156.

[3] –عبد الفتاح حجازي، النظام القانوني لحماية التجارة الالكترونية، الحماية الجنائية للتجارة الالكترونية، مرجع سابق ، ص261 .

[4] – على الرغم من الاستيلاء على المعلومات والبرامج ، ألا أن استيلاء الغير عليها لا يحرم صاحبها منها، و لا يحول بينه و بين استغلالها و لكنه ينقص من قيمتها الاقتصادية ، وبالتالـ

.

و ن أغلب

الأموال لم تشترط صراحة ضرورة أن يكون المال موضوع الجريمة

.

و يعة البرامج و

[1]، ذلك أن

استيلاء الغير عليه لا يحرم صاحبها منها، و لا يحول دون استغلالها و إن كان هذا الاستغلال

، وعليه لابد من تدخل تشريعي بتعديل

النصوص القائمة أو استحداث نصوص خاصة في هذا الإطار.

[1] – إلا أن جريمة الإتلاف تحقق حماية جنائية كاملة للأموال المعنوية عمن معلومات وبرامج ، على خلاف باقي جرائم الأموال التي توفر حماية نسبية .

المبحث الثاني

الحماية الجنائية للتجارة الإلكترونية في إطار نصوص جرائم التزوير

نص المشرع الجزائري على جرائم التزوير في المواد 197 إلى 231 من قانون العقوبات الجزائري، المقابلة للمواد 211 إلى 227 من قانون العقوبات المصري، و المادتين 144 و 451 من قانون العقوبات الفرنسي .

والتزوير هو تغيير الحقيقة بقصد الغش في سند أو وثيقة أو أي محرر أخر بإحدى الطرق المادية أو انه إحداث ضررا بالمصلحة العامة أو مصلحة شخص من الأشخاص [1].

ولقيام جريمة التزوير لابد من توافر ركنين: ركن معنوي، يتخذ صورة القصد الجنائي العام والخاص وركن مادي يتمثل في تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون ، على نحو يسبب ضرر للغير [2].

وبالتالي فإن جريمة التزوير لا تتوافر إلا إذا كان محل تغيير الحقيقة محررا ويقصد بالمحرر كل كتابة منسوب صدورها إلى شخص أو جهة معينة من شأنها أن تولد مركز قانوني معين أو ترتيب نتائج معينة، و يشترط في المحرر الكتابة، و أن تكون منسوب إلى شخص معين، و أن يحدث اثر قانوني معين [3].

---

[1] – محمد زكي أبو عامر وسليمان عبد المنعم، قانون العقوبات (القسم الخاص)، منشورات الحلبي الحقوقية، بيروت – لبنان 2006 ص 524 .

[2]- كما هو معلوم بأن التزوير شأنه شان بقية الجرائم يتكون من ركنين هما الركن المادي والركن المعنوي ولكنه يختلف عنهما من حيث انه يشترط لتحققه أن يتوفر ركن ثالث خاص هو الضرر حتى يتم معاقبة فاعله . للتفصيل راجع محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، الجرائم المخلة بالمصلحة العامة، 1972، ص 280 وما بعدها.

[3]– عوض محمد، الجرائم المضرة بالمصلحة العامة، دار المطبوعات الجامعية، الإسكندرية، 1985، ص 174.

ويراد بالمحرر أيضا كل مسطور أو وثيقة تحتوي على علامات أو عبارات ينتقل بها معنى معين من شخص إلى آخر، عند النظر إليه رأي يمكن الاطلاع على محتواه بمجرد المشاهدة[1].

ومع التطور التقني في وسائل الاتصال الحديثة و تقنيات المعلومات، ظهر نوع جديد من المحررات هي المحررات الإلكترونية التي توسيع استخدامها في كثير من المجالات و ما زاد في استخدامها اتجاه كثر من الدول لتطبيق الحكومة الإلكترونية و التوسع في التجارة الإلكترونية، و احتجابها إلى تنفيذ العقود الإلكترونية كوسيلة عاقد بين الأفراد و الهيئات و الدول عبر الانترنت.

وفي ظل الانتشار الهائل للمحررات الإلكترونية عبر شبكات الاتصال، كانت هناك ضرورة ملحة لحمايتها جنائيا لاسيما التزوير كأخطر جريمة.

تعد جريمة التزوير في المجال المعلوماتي من اخطر صور الغش المعلوماتي نظرا للدور الهام والخطير الذي أصبح يقوم به الحاسب الآلي الآن والذي اقتحم كافة المجالات [2]، وأصبحت تجري من خلال كم هائل من العمليات ذات الآثار القانونية الهامة والخطيرة والتي لا يصدق عليها وصف " المكتوب" في القانونين المدني والجنائي ، وقد أثار هذا الوضع الشك حول دلالتها في الإثبات وحول إمكانية وقوع جريمة التزوير العادية ولهذا كان التدخل التشريعي ذو أهمية بالغة.

وعليه سنبحث مفهوم المحررات الإلكترونية (المطلب الأول)، ثم مدى إمكانية تطبيق نصوص التزوير على المحررات الإلكترونية (المطلب الثاني).

---

[1] – فوزية عبد الستار، مرجع سابق، ص 255.

[2] – التزوير المعلوماتي هو تغيير للحقيقة يرد على مخرجات الحاسب الآلي ويستوي في المحرر المعلوماتي أن باللغة العربية محفوظة على دعامة لبرنامج منسوخ على اسطوانة وشرط أن يكون المحرر المعلوماتي ذا أثر أثبات حق واثر قانوني . وقد عرف المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات البرازيلي لعام 1994 في مقرراته وتوصياته بشأن جرائم الكومبيوتر والتزوير المعلوماتي بأنه المجرى الطبيعي لمعالجة البيانات ترتكب باستخدام الكومبيوتر وتعد فيما لو أرتكبت بغير هذه الطرق من قبيل أفعال التزوير المنصوص عليها في القانون الوطني.

المطلب الأول: ماهية المحررات الإلكترونية

تنطوي جريمة التزوير على تغيير الحقيقة في محررات، وبظهور انتشار تكنولوجيا المعلومات و الاتصال ، ظهرت المحررات الالكترونية، ولفهم الطبيعة الخاصة للمحررات الإلكترونية نلقي الضوء على مفهومها (الفرع الأول)، ثم شروطها (الفرع الثاني)، كالآتي:

الفرع الأول: مفهوم المحررات الإلكترونية

لتحديد مفهوم المحررات الإلكترونية لابد من الوقوف على تعريفها، و المقارنة بين المحررات الإلكترونية، و بين غيرها من المحررات التقليدية.

أولا- تعريف المحررات الإلكترونية:

تعرضت بعض التشريعات لتعريف المحررات الالكترونية، بينما لم تعرفها بعض التشريعات الأخرى تاركة تعريفها للفقه الذي أورد عدة تعريفات لها ، على النحو الآتي :

1-التعريف التشريعي:

عرفت بعض التشريعات الحديثة المحررات الإلكترونية من زوايا مختلفة ، إذ عرفها المشرع الانجليزي في المادة 1/8 من قانون التزوير والتزييف لسنة 1981 بأنها تشمل كل شريك ممغنط أو صوتي أو كل وسيلة توجد بها بيانات مسجلة بطريقة ميكانيكية أو أخرى[1].

---

[1]- يتسع مفهوم المحرر في القانون الانجليزي ليشمل : أي وثيقة محسوسة أوغير محسوسة ، أي شريط ممغنط أو كاسيت أو أي أداة أخرى سجلت فيها بيانات بوسيلة ميكانيكية أو الكترونية أو أي وسيلة أخرى ، وبالتالي فإن القانون الإنجليزي

للتفصيل راجع: - Michel VIVANT et autres, op. cit, P 1833.

Pascal Vergucht. La répression des delits informatique dans une perspective international, .Montpelier. 1996. P.96-thèse

كما عرفها القانون الكندي لسنة 1985 بأنها كل ورقة أو أي مادة أخرى سجلت عليها كلمات يمكن للشخص أو لجهاز الكمبيوتر أو أي وسيلة أخرى قراءتها و فهمها [1].

وعرف أيضا قانون التجارة الأمريكي المستند الالكتروني في المادة7/2على أنه سجل يتم إنشاؤه أو .[2]

وعرفتها أيضا بعض التشريعات العربية، كالتشريع الجزائري في المادة 323 مكرر من قانون القانون المدني رقم 10/05[3] ، على أنها كتابة تتكون من تسلسل حروف أو أوصاف أو أرقام أو أي علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها ، وكذا طرق إرسالها[4].

وهكذا يتضح مما سبق بأن المشرع الجزائري اعتمد المفهوم الواسع للكتابة سواء الكتابة على الورق أو على دعائم غير مادية، فالمهم أن تكون الكتابة واضحة ومفهومة.

كما عرفها التشريع المصري في المادة الأولى من قانون التوقيع الإلكتروني رقم 15 لسنة 2004أنه رسالة تنشأ أو تدرج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة إلكترونية، أو رقمية، أو ضوئية أو بأي وسيلة أخرى مشابهة [5].

وعرف أيضا التشريع الإماراتي المحرر الإلكتروني في قانون التجارة الإلكترونية لإمارة دبي رقم 2 لسنة 2002 بأنه سجل أو مستند إلكتروني يتم إنشاؤه أو تخزينه أو استخدامه أو نسخه أو

---

[1]- شيماء عبد الغني عطاء الله، مرجع سابق، ص 84.

[2]-Benjamin Wright et Jane K .Winn, the law of electronic commerce, third edition a division of aspen publishing , Ink New York2000,p12-14.

[3]- القانون05-10المؤرخ في 20جوان 2005المعدل والمتمم للأمر 75-58 المتضمن القانون المدني الجريدة الرسمية عدد 44، الصادرة في 12جوان2005.

[4] – ويلاحظ أن المشرع الجزائري استعمل مصطلح الوسيلة ، والأصح الدعامة (supports) حسب القانون المدني الفرنسي.

[5]- إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الحديثة للنشر، الإسكندرية، مصر ،2008، ص 14.

إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط ملموس أو على أي وسيط إلكتروني آخر، ويكون قابلا للاسترجاع بشكل يمكن فهمه[1].

كما عرف المشرع الأردني المحرر الإلكتروني في المادة 02 من قانون المعاملات الإلكترونية رقم 85 لسنة 2001، بأنه رسالة معلومات يتم إنشاؤها أو إرسالها تسليمها أو تخزينها بالوسائل الإلكترونية أو بوسائل مشابهة بما في ذلك تبادل البيانات الإلكترونية أو البريد الإلكتروني أو أو الفاكس أو النسخ الرقمي[2].

2-التعريف الفقهي:

عرف الفقه المحرر الإلكتروني بأنه كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعلومات أو يكون مشتقا من هذا النوع، أي كل دعامة مادية مهيأة لاستقبال المعلومات التي يتم تسجيل المعطيات عليها من خلال تطبيق إجراءات المعالجة المعلوماتية، [3].

ويختلف المستند المعالج آليا عن المستند غير المعالج آليا وتعتبر مستندات معلوماتية الأوراق المعدة لتسطير المعلومات عليها والأقراص الممغنطة التي لم يسجل عليها أي شيء بعد والملاحظات التي تكون على شكل كتب أو نشرة متعلقة بطريقة استخدام البرامج [4].

كما ذهب البعض إلى تعريفه، بأنه جسم منفصل أو يمكن فصله عن نظام المعالجة ، وقد سجلت عليه معلومات معينة، سواء كانت للاستخدام أو بواسطة نظام المعالجة أو يكون مشتقا [5].

---

[1] – راجع المادة 02 من قانون المعاملات الالكترونية لإمارة دبي .

[2]– لورنس محمد عبيدات ، إثبات المحرر الالكتروني ن دار الثقافة للنشر والتوزيع ' عمان الأردن، 2005 ص 77.

[3] – علي عبد القادر القهوجي، مرجع سابق، ص 150.

[4] – وكذلك تعتبر البطاقات البنكية التي لم تدخل الخدمة بعد وهذه إن كان مسجلا عليها معلومات مكتوبة بخط اليد أو مطبوعة أو محفورة إلا أنه لم يتم معالجتها بعد، إذ أنها مازالت في مرحلة الإعداد فقط. للتفصيل راجع أمال قارة، مرجع سابق، ص 135.

[5] – إيهاب فوزي السقا، مرجع سابق، ص 16.

كذلك يقصد بالمستند المعالج آليا كل دعامة مادية يمكن أن يدون عليها شيء معنوي، ويقصد بالمستند في مجال المعلوماتية كل شيء مادي متميز (قرص ،أو شريط ممغنط أو خلافه) يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات المعالجة ، ويستوي بعد ذلك أن يكون هذا الشيء قد خرج من الآلة و ثم تصنيفه أو تخزينه أو أنه مازال بداخلها انتظارا لاستخراجه أو تعديله [1].

ثانيا- المقارنة بين المحرر الإلكتروني و المحرر الورقي:

1-أوجه الاتفاق:

أ-يتفق المحرر الإلكتروني مع المحرر الورقي في أن كلاهما يحتوي على مجموعة من الرموز التي تعبر عن مجموعة مترابطة من الأفكار و المعاني الإنسانية، مما يعني أن المحرر أداة للتفاهم و تبادل الأفكار بين الأفراد[2].

وعليه حرصت بعض التشريعات كالتشريع الانجليزي والفرنسي على إدخال بيانات الحاسوب ضمن طائفة المحررات في مفهوم جريمة التزوير ، بغض النظر عن المادة التي سجلت عليها .

ب- للمحررات الإلكترونية ذات الحجية المقررة للمحررات الورقية في نطاق المعاملات المدنية و التجارية وفقا لمعظم التشريعات الحديثة ، إذ نص المشرع الفرنسي في المادة 1/1316 من القانون المدني على أن للمحرر الإلكتروني قوة في الإثبات مثل المحرر الورقي بشرط تحديد هوية الشخص محدد مصدر هذا المحرر، وأن يتم تدوينه والاحتفاظ به في ظروف تسمح بضمان سلامته[3].

---

[1] – وبالتالي فإن المحرر الإلكتروني هو محرر يتضمن بيانات معالجة إلكترونية، ومكتوب وموقع عليها بطريقة إلكترونية، وموضوع على دعامة مادية، مع إمكانية تحويله لمحرر ورقي عن طريق إخراجه من الكمبيوتر. للتفصيل راجع :علي عبد القادر القهوجي، مرجع سابق، ص 151.

[2] – إيهاب فوزي السقا، مرجع سابق، ص 18.

[3]-"l'écrits sous forme électronique est admis en preuve au même titre que l'écrit sur support papier sous réserve que puisse être dument. identifiée la personne dont il émane et qu' il soit établie et conserve dans des conditions de nature a en garantir intégrité".

وبالتالي ساوى المشرع الفرنسي في الحجية بين المحررات التقليدية الالكترونية والمحررات الورقية بشرط تمييز مصدره وتحديد هويته ، وكان انشاؤه وحفظه قد تم في ظروف تسمح بضمان سلامته [1].

كما ساوى المشرع الجزائري بموجب المادة 323 مكرر 1 بين الكتابة الإلكترونية والكتابة العادية من حيث حجية الإثبات، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها، ووضعها في ظروف تضمن سلامتها[2].

كما أضفى المشرع المصري الحجية الكاملة على المحررات الإلكترونية و إعطائها ذات الحجة المقررة للكتابة و المحررات الورقية الرسمية أو العرفية، هي أحكام قانون الإثبات في المواد المدنية و التجارية، حتى استوفت الشروط المنصوص عليها في القانون وفقا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون حسب المادة 15 منن قانون التوقيع الإلكتروني[3].

ج- تحظى المحررات الإلكترونية كالمحررات الورقية من حماية جنائية لاسيما من جريمة التزوير في معظم التشريعات الحديثة، سواء في إطار قانون العقوبات، كما هو الحال بالنسبة للتشريع الفرنسي في المادة 1/441 من قانون العقوبات الفرنسي، والتشريع الكندي في الفصل 321 من قانون العقوبات الكندي، أو في إطار نصوص خاص كما هو الحال بالنسبة للتشريع البريطاني والتشريع الأمريكي. وكذلك التشريع المصري بمقتضى المادة 23 من قانون التوقيع الإلكتروني[4].

---

[1] - ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة الإسكندرية مصر ، 2007، ص 173.

[2] - راجع المادة 323 مكرر من القانون المدني الجزائري .

[3] - إيهاب فوزي السقا، مرجع سابق، ص 18.

[4] - تنص المادة 23 من قانون التوقيع الإلكتروني: مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو أي قانون آخر، يعاقب بالحبس أو بغرامة لا تقل عن 10 آلاف جنيه و لا تجاوز 100 ألف جنيه كل من أتلف أو عيب توقيعا أو وسيطا أو محررا إلكترونيا، أو زور شيئا من ذلك الاصطناع أو التعديل أو التحويل أو بأي طريق آخر، و في الفقرة ج من ذات المادة يعاقب كل من استعمل محررا إلكترونيا معيبا أو مزورا مع علمه بذلك.

وهذا بخلاف التشريع الجزائري الذي لم يساير التشريعات الحديثة في هذا الإطار في انتظار تعديل نصوص جريمة التزوير لكي تسع التزوير المعلوماتي أو إصدار نص خاص بالتزوير المعلوماتي .

2-أوجه الاختلاف:

رغم التشابه بين المحرر الورقي والمحرر الالكتروني ، في احتوائهما على معان وأفكار انساسية محددة ، وأن المساس بكليهما يحدث ضررا يبرر تجريم المساس بهما ، لكنهما يختلفان من النواحي الآتية :

أ-المحررات الورقية تعكس شخصية كاتبها، لذا يمكن إحالتها إلى خبير لمعرفة مدى صحة نسبتها إليه، أما المحررات الإلكترونية فتكتب بواسطة الحاسوب[1]. وبالتالي بما أن المحرر الالكتروني يتم كتابته بالحاسوب فلا يمكن تحديد من قام بكتابته، على خلاف المحررات الورقية .

ب- المحررات الورقية معانيها وأفكارها مكتوبة على مادة ورقية، حتى وان تم إرسالها عبر أجهزة الكترونية كالفاكس ،والبريد الالكتروني بعد إجراء عملية المسح الضوئي ، بينما المحررات الإلكترونية مخزنة على دعامات إلكترونية أو مغناطيسية[2].

وعليه فالعمر الافتراض للمحرر الورقي قصير مقارنة بالمحررات الالكترونية ، فهذه الاخيرة تعمر طويلا لكونها مسجلة ومحفوظة في وسائط الكترونية .

ج- المحررات الورقية يمكن الاطلاع على محتواها لمجرد النظر إليها، بينما المحرر الإلكتروني لايتم الاطلاع عليه بمجرد الرؤية ، بل يلزم وضعه في وسيط إلكتروني قابل لقراء ته[3].

---

[1]- شيماء عبد الغني عطاء الله ، مرجع سابق، ص 81.

[2]- محمد رايس ، الحماية الجنائية للسند الالكتروني ، مجلة الدراسات القانونية صادرة عن كلية الحقوق جامعة بيروت ،العدد الأول 2006-2007، ص82. إيهاب فوزي السقا، المرجع السابق، ص 20

[3]- شيماء عبد الغني، مرجع سابق، ص 81.عمر الفاروق الحسيني ، تأملات في بعض صور الحماية القانونية لنظم الحاسب الآلي ، بحث مقدم لمؤتمر الحاسب الالكتروني ، القاهرة ، ماي 1991، ص26.

د- المحررات الورقية تعتبر من الأشياء المادية، بينما المحررات الإلكترونية ذات طابع معنوي ما لم يتم إخراجها من أجهزة الحاسوب[1].

الفرع الثاني: شروط المحررات الإلكترونية

يشترط الفقه في المحررات الإلكترونيات حتى تكون حجة في الإثبات، شرط الكتابة الإلكترونية، و التوقيع الإلكتروني، كالآتي:

أولا-الكتابة الإلكترونية:

تعتبر الكتابة من أهم طرق الإثبات المختلفة لمزاياها وضماناتها الهامة ، لهذا أضفت عليها التشريعات الحديثة حجية مطلقة ما دام الخصم لم ينكرها أو يدع تزويرها، ولذلك هي ملزمة للقاضي و لا تخضع لتقديره[2].

وقد عرف المشرع الفرنسي الكتابة في المادة 1316 من التقنين المدني الفرنسي على أنها كل تدوين للحروف أو العلامات أو الأرقام أو أي رمز أو أي إشارة أخرى ذات دلالة تعبيرية واضحة و مفهومة أيا كانت الدعامة التي تستخدم في إنشائها، أو الوسيط الذي تنتقل عبره [3].

وقد اعترف المشرع الفرنسي بالكتابة الإلكترونية بموجب المادة 1316 من قانون التوقيع الإلكتروني رقم 230/2000 في إطار تعديل القانون المدني، حيث نصت هذه المادة على أنه تتمتع الكتابة الإلكترونية بنفس الحجية المعترف بها للمحررات الكتابية في الإثبات، شريطة تحديد شخص مصدرها على وجه الدقة، وأن يكون تدوينها وحفظها قد تم في ظروف تدعو إلى الثقة[4]. وعليه فإن المشرع الفرنسي أعطى للكتابة الإلكترونية ذات قوة الكتابة الورقية في الإثبات شرط

---

[1]-إيهاب فوزي السقا، مرجع سابق، ص 20.

[2]- ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة الإسكندرية مصر ، 2007، ص 178.

[3]- وبالتالي تبنى المشرع الفرنسي تعريفا واسعا للكتابة ليشمل كال كل أنواع الكتابة سواء الكتابة الورقية ، أو الكتابة الالكترونية . للتفصيل راجع لزهر بن سعيد النظام القانون لعقود التجارة لالكترونية ، دار الفكر الجمعي ، مصر ، 2010، 126. راجع أيضا نبيل إبراهيم سعد، الإثبات في المواد المدنية و التجارية في ضوء الفقه و القضاء، منشأة المعارف، الإسكندرية مصر، 2000، ص 89

[4]- Eric. A.Caprioli, le juge et la preuve électronique,contribution au colloque destrasbourg. Sur le commerce electroni. 8-9octobre 1999. P. 128.

تحديد مصدرها على وجه الدقة أي تعيين الشخص الذي ينسب إليه المحرر الإلكتروني و الذي يتحمل الالتزامات الناشئة عنه، غير أن هذا الشرط يمكن الاستغناء عنه باعتباره أحد وظائف التوقيع[1].

و يشترط في الكتابة أيضا تدوينها و حفظها في ظروف تدعو إلى الثقة لكونها معرضة للتحريف و التعديل، و هذا يتطلب إنشاء خدمة تشبه الأرشيف تتولى القيام بهذه المهمة[2].

كما عرف المشرع الجزائري أيضا الكتابة الالكترونية بموجب المادة 323 مكرر من قانون 10/05، بأنها سلسلة حروف أو علامات أو أرقام أو أي علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة ، أو طرق إرسالها ، وأضفى عليها الحجية بالمادة 323 مكرر 1 [3]، إذا توافرت شروطها المتمثلة إمكانية تحديد مصدرها ، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها.

كما عرف المشرع المصري أيضا الكتابة الإلكترونية بمقتضى المادة الأولى من قانون رقم 15 لسنة 2004 المتعلق بالتوقيع الإلكتروني، بأنها كل حروف أو أرقام أو رموز أو أي علامات أخرى تثبت عل دعامة إلكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة و تعطى دلالة قابلة للإدراك، بمعنى أنها عبارة عن بيانات و معلومات محفوظة و مثبتة في دعامة إلكترونية أو أي وسيلة مشابهة كشريط ممغنط(F.D) أو قرص مدجج (C.D) [4].

---

[1]- ثروت عبد الحميد، مرجع سابق، ص 180.

[2]– إذا كان تعريف الكتابة في المادة 1316 لم يهتم بطريقة التعبير عن البيانات و المعلومات التي تضمنها المحرر إلا أنه اشترط أن تكون الرموز و الإشارات المستخدمة في الكتابة ذات دلالة تعبيرية واضحة و مفهومة.

[3] – ويلاحظ أن نص المادتين 323 مكرر 323 مكرر1 مأخوذ من المادتين 1316و1316–1 مدني فرنسي. كما يلاحظ أن المشرع تبنى مفهوما موسعا للكتابة واعترفت بالكتابة ، وهذا من شأنه أن يضع حدا للغموض ويواكب التطور التقني في مجال التجارة لالكترونية ويوفر الثقة والأمان للمتعاقدين متى توافرت شروط الكتابة .

[4]– عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية مصر ، 2006، ص 76.

كما أضفى المشرع المصري على الكتابة الإلكترونية ذات الحجية المقررة للكتابة الورقية بموجب المادة 15 من قانون التوقيع الإلكتروني، متى استوفت الشرط المنصوص عليها في هذا القانون وفقا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون[1].

ثانيا-التوقيع الإلكتروني:

بالإضافة إلى شرط الكتابة في المحررات، يجب أن يكون المحرر منسوبا لشخص ما عن طريق التوقيع عليه، حتى يكون دليلا كاملا في الإثبات.

وقد تباينت التعريفات التي أعطيت للتوقيع الإلكتروني بحسب الزاوية التي ينظر منها إلى التعريف، فقد عرفه قانون الأونسترال النموذجي للتوقيع الالكتروني في المادة 2 بأنه بيانات في شكل إلكتروني مدرجة في سلسلة بيانات أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتقييم هوية الموقع بالنسبة إلى رسالة البيانات و لبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات، كما عرفه التوجيه الأوربي رقم 1999/93 الصادر عن المجلس في 1999/12/13 في المادة (1/2) بأنه عبارة عن معلومات أو معطيات في شكل إلكترونين ترتبط أو تتصل منطقيا بمعطيات إلكترونية أخرى، وتتخذ كوسيلة لإقرارها[2].

وعرفه أيضا التشريع الأمريكي الصادر في2000/06/30 المتعلق بالتجارة الإلكترونية بأنه شهادة رقمية تصدر عن إحدى الجهات المختصة وتميز كل مستخدم و يمكن أن يستخدمها في إرسال أي وثيقة أو عقد تجاري أو تعهد أو إقرار[3].

---

[1] - إيهاب فوزي السقا , مرجع سابق ، ص29. شيماء عبد الغني عطاء الله، مرجع سابق ، ص81.

[2]- ط لحجيته وفقا للمادة 4/1316 من القانون المدني الفرنسي ، بأن يدل على شخصية صاحبه و يضمن علاقته بالواقعة التي أجرها و تؤكد شخصية صاحبه وصحة الواقعة المنسوبة إليه إلى أن يثبت عكس ذلك .

[3]- عبد الحميد ثروت، مرجع سابق، ص 48-49

وعرف المشرع المصري أيضا التوقيع الإلكتروني في المادة 01 من قانون التوقيع الإلكتروني بأنه ما يوضع على المحرر الإلكتروني، و يتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها و يكون له طابع منفرد يسمح بتحديد شخص الموقع و يميزه عن غيره [1].

كما اعتد المشرع المصري كغيره من التشريعات الحديثة بالقوة الثبوتية للتوقيع الإلكتروني في المادة 14 من قانون التوقيع الإلكتروني [2].

على غرار المشرع الفرنسي لم يعرف المشرع الجزائري التوقيع الالكتروني ، لكنه اعترف به بمقتضى المادة2/327 من قانون رقم 10/05المؤرخ في 20 جوان 2005 [3]، والتي نصت على أنه يعتد بالتوقيع الالكتروني وفق الشروط المذكورة في المادة 323 مكرر 1 ، والمتمثلة في إمكانية التأكد من هوية الشخص التي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها ، إلا أنه لم يعرف التوقيع الالكتروني.

وفي مجال الفقه تعددت التعريفات ، أفضلها الذي يعرف التوقيع الالكتروني على أنه مجموعة من الإجراءات التقنية تمكن من تحديد شخصية من يصدر عنه هذه الإجراءات [4]، وقبوله بمضمون التصرف الذي يصدر التوقيع بشأنه[5].

فهذا التعريف يركز ضرورة قيام التوقيع الالكتروني بالوظائف التقليدية له ، وهي تمييز هوية الشخص والتعبير عن رضائه الارتباط بالتصرف القانوني ، لكنه لايغفل إصدار التوقيع الالكتروني وتوثيقه ، والتي غالبا ما يتولاها شخص مرخص له من الجهات المختصة بذلك ، وهذه الإجراءات

---

[1]– إيهاب فوزي السقا، مرجع سابق ، ص 30. عبد الحميد ثروت ، مرجع سابق ، ص 47.

[2] – راجع المادة 14 من قانون التوقيع الالكتروني المصري .

[3] – يلاحظ أن التشريع الجزائري أخذ نص المادة 327 من المادة 4/1316 قانون مدني فرنسي

[4] – وهذه الإجراءات التقنية تكون مجموعة من البيانات تعطي في النهاية مفتاحا سريا خاصا بشخص معين ،ويكوناها طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره .

[5]– محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر 2003، ص 179-
Davio E. internet face au droit . cahiers du; c. R .I .D.n.12; story scientica. 1997. P.80.

تضمن أن يخص التوقيع صاحبه وحده دون غيره ، كما تسمح عند الضرورة بالتعرف على صاحبه كذلك تضمن عدم السطو عليه ، وأيضا تضمن عدم تعديل أو المساس بالبيانات الموقع ليها [1].

وتجدر الإشارة إلى أن وجوب توفر التوقيع الالكتروني في المحرر الالكتروني ليس حتميا ، وذلك لأنه يمكن تصور وجود سند الكتروني دون توقيع الكتروني ، إذ يكون السند على شكل بيانات أو قوائم ، كالقوائم الانتخابية للحالة المدنية ، وقوائم المنتخبين ، فهي عبارة عن بيانات لاتذيل بتوقيع [2].

المطلب الثاني: مدى تطبيق نصوص التزوير على المستندات الالكترونية

لجريمة التزوير ركنان، ركن مادي يتمثل في تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون، على نحو يسبب ضرر للغير، وركن معنوي يتخذ صورة القصد الجنائي العام والخاص[3].

ونظرا لأن الركن المعنوي لايثير صعوبة في تحققه في التزوير المعلوماتي على خلاف الركن المادي ، سنقتصر على الركن المادي من خلال التطرق إلى مدى انطباق وصف المحرر على المستندات الالكترونية (الفرع الأول)، ومدى خضوعها لفعل تغيير الحقيقة (الفرع الثاني)، كالآتي:

---

[1] – عبد الحميد ثروت ، مرجع سابق ، ص.50-51.

[2] – محمد رايس ، الحماية الجنائية للسند الالكتروني مرجع سابق ، ص84

[3]- يتمثل الركن المعنوي في القصد الجنائي بنوعيه قصد جنائي عام يتحقق بانصراف إرادة الجاني إلى تغيير الحقيقة في المحرر، وقصد جنائي خاص يتحقق باتجاه نية الجاني إلى استعمال المحرر في ما زور من أجله . للتفصيل راجع محمود مصطفى، شرح قانون العقوبات، القسم الخاص، مطبعة جامعة القاهرة مصر، 1984، ص 136.

الفرع الأول: مدى انطباق وصف المحرر على المستندات الالكترونية

إن محل جريمة التزوير هو المحرر، ويقصد به كتابة مركبة من حروف أو علامات تدل على معنى أو فكرة معينة، ويمكن قرآه محتواها بصريا[1]، كما عرفه البعض على أنه عبارات خطية مدونة بلغة يمكن فهمها الناس [2]، ويشترط في المحرر الكتابة بأن
محلية أو أجنبية ولا عبرة بالمادة التي سطرت عليها الكتابة ، كما يشترط أن تكون الكتابة منسوبة لشخص معين، وأن يحدث أثارا قانونية[3].

وعليه فهل تعد المستندات الالكترونية من قبيل المحررات التي يسري عليها نصوص جريمة التزوير

للإجابة على هذا التساؤل لقد انقسم الفقه والقضاء بين معارض ومؤيد، كالآتي:

أولا-الرأي المؤيد:

يرى هذا الاتجاه أنه يمكن اعتبار المستندات الالكترونية محرر تطبق عليه جريمة التزوير، لأن المشرع لم يحدد نوعية المحرر[4].

حيث يرى بعض الفقه الفرنسي إمكانية تغليب روح النصوص واعتبار ما يظهر على شاشة الحاسب شكلا مستحدثا للمحرر[5].

---

[1] -هشام محمد فريد ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة مصر ، 1992، ص326. محمود نجيب حسني ، مرجع سابق ، ص357.

[2] – رمسيس بهنام ، الجرائم المضرة بالمصلحة العامة ، منشأة المعارف ، الإسكندرية مصر، 1986، ص174

[3] – محمود نجيب حسني ، مرجع سابق ، ص357. كامل عفيفي عفيفي، مرجع سابق ، ص242-243.

[4] – أمال قارة ، مرجع سابق ، ص137.

[5] -Devezeles(Jean) qualification pénales applicables aus fraudes informatique acte du viii eme congres del AFDp. Grenoble 2. 29novembre. 1985.p.191

إلا أن الفقه البلجيكي يرى أن نصوص التزوير في المحررات لايمكن أن تنطبق إلا في حالة ظهور المعلومات التي تم تزويرها في المستخرجات الورقية [1].

وقد اتجه القضاء الفرنسي أيضا إلى التفسير الموسع للمحررات في نطاق المعاملات التجارية، حيث قضت محكمة النقض الفرنسية (الدائرة التجارية) بجواز التمسك بالنسخة المرسلة عبر الفاكس وبالتالي أقرت حجيتها في الإثبات [2]، كما أصبحت تعاقب على أي تزوير في أي محررات لها قيمة في الإثبات قبل تدخل المشرع بنص صريح[3].

وتبنت أيضا هذا التفسير سويسرا ، حيث قضت المحكمة الفيدرالية السويسرية تطبيق القواعد العامة للتزوير على الكتابة الالكترونية ، وكذا القضاء الياباني[4].

كما قضت المحكمة العليا في اليونان سنة 1983 وأيضا المحكمة العليا في هولندا سنة 1991 بسريان وصف التزوير على المستندات الالكترونية[5].

ثانيا- الرأي المعارض:

يعارض هذا الاتجاه اعتبار المستندات الالكترونية محرر تطبق عليه جريمة التزوير، حيث أنه عارض بعض الفقه الفرنسي قبل صدور قانون 1988 قيام جريمة التزوير اذا كان تغيير الحقيقة

---

[1] -بينما يرى جانب من الفقه السوري تطبيق نصوص التزوير عندما تكون البيانات قد سجلت على أسطوانة أو شريط ممغنط لأنه يعتبر هذه الوسائط الالكترونية محررا، وتغيير الحقيقة فيه يعد تزويرا وذلك بسبب انتقال المعلومات و المعطيات المخزنة إلى جسم مادي له سمات المحرر المكتوب و الذي يمكن قراءته بالعين باستخدام الحاسب للكشف على . للتفصيل راجع كامل عفيفي عفيفي، مرجع سابق ، ص245.

[2] – شيماء عبد الغني عطاء الله ، مرجع سابق ، ص82.

[3] – أسامة المناعسة ، مرجع سابق ، ص159.

[4]- Michel vivant et autres .op cit. p.1853.

[5] -Pascalvergucht.op. cit,p.96.

الذي يكون محله الأشرطة الممغنطة، وذلك لعدم وجود عنصر الكتابة ،فجريمة التزوير تشترط الكتابة ، ولكونها لاتصلح كوسيلة إثبات[1].

كما ذهب الفقه في مصر استنادا إلى المادة 211 ، وايطاليا وفقا للمادة 485 وبلجيكا وفقا للمادة 190، وفنلندا وسويسرا إلى عدم دخول المحرر الالكتروني[2]،لان نصوص التزوير تخص المحرر بمفهومه التقليدي وهو المحرر الورقي الذي يقتضي أن يكون وجوده ماديا وملموسا يمكن رؤيته بالعين المجردة أي يجب أن يكون محتوى الوثيقة أو الوعاء قابلا للمشاهدة البصرية بغير الوسائل الفنية على خلاف المحررات الالكترونية[3].

أما بالنسبة للفقه والقضاء في الجزائر ، فلم يتخذ موقفا من هذه المسألة ، لكن بالنظر لعمومية نصوص التزوير فيمكن اعتبار المستندات الالكترونية محررات تطبق عليها جريمة التزوير [4]، بالنظر إلى الغاية والهدف من تجريم التزوير ،لأن الهدف من تجريم أفعال التزوير هو حماية الثقة العامة بالمحررات بغض النظر عن طبيعتها.

لمعالجة القصور في النصوص التقليدية عمدت بعض التشريعات الحديثة لمواجهة القصور في النصوص التقليدية ، إلى استحداث نصوص تجريمية جديدة أو إدخال تعديلات على التشريعات التقليدية، من أجل المعاقبة على جريمة التزوير الواقعة على المستندات المعلوماتية، حفاظا على الثقة الواجب توافرها في المستندات المعلوماتية [5].

---

[1]– عفيفي كامل عفيفي ، مرجع سابق، ص 243–244. أحمد حسام طه تمام، الجرائم الناشئة عند استخدام الحاسب الآلي (ودراسة مقارنة)، دار النهضة العربية، القاهرة مصر 2000، ص391.

[2] – نائلة عادل قورة ، مرجع سابق، ص 584–585

[3] – إيهاب فوزي السقا، مرجع سابق، ص55. نائلة عادل قورة ، مرجع سابق، ص584–585.

[4] – فالمواد 214 إلى 229 من قانون العقوبات ، تشترط المحرر بصفة عامة لقيام جريمة التزوير، فمثلا المادة 214 تعاقب السجن المؤبد كل قاض أو موظف أو قائم بوظيفة عمومية ارتكب تزويرا في المحررات العمومية أو الرسمية أثناء تأدية وظيفته وبالتالي ذكرت المحررات العمومية والرسمية بصفة عامة سواء كانت ورقية أو الكترونية .

[5] – كامل عفيفي عفيفي ، مرجع سابق ، ص246.

ومن أمثلة هذه التشريعات التشريع الفرنسي الذي استحدث المادتين 5/462 6/462 بموجب قانون سنة1988، غير أنه وبموجب قانون 1994 ألغاهما وأخضعهما للمادة 441 من قانون العقوبات[1] والتي أصبحت تشمل كل صور التزوير كما أن ووضع نص خاص بالتزوير المعلوماتي يحقق حماية للنظام المعلوماتي فقط دون الحفاظ على الثقة العامة، مما ينقص من ثقة المتعاملين بها،[2].

ويلاحظ أن القانون الفرنسي في المادة 441 من قانون العقوبات لم يقصر التزوير على المحررات الورقية ، بل يشمل جميع المحررات حتى الالكترونية ، وبأي وسيلة مادية أو معنوية [3].

وبالتالي أصبح يشمل إلى جانب المحرر التقليدي كل وسيط لأخر للتعبير عن فكرة ولكن يشترط أن يكون يشترط أن يكون من الممكن استخدام المحرر أو الوسيط الذي تم تزويره لممارسة حق أو تصرف وأن يصلح لإثبات حق أو تصرف له آثار قانونية [4] .

وكذلك تبنى المشرع المصري فكرة المحرر الالكتروني وأضفى عليه الحجية الكاملة في المادة 15 من قانون التوقيع الالكتروني[5]، كما أورد نصا خاصا يعاقب على تزوير المحررات الالكترونية بمقتضى المادة 23 من القانون رقم 15لسنة2004 المتعلق بالتوقيع الالكتروني[6].

---

[1] – وكان السبب الذي أدى إلى إلغاء النص الخاص بالتزوير المعلوماتي هو أن إفراد نص خاص بالتزوير الالكتروني سوف يكون من غير جدوى مادام مفهوم التزوير غير واضح، وهو ما دفع بالمشرع الفرنسي إلى إدراج تعريف للتزوير في المادة 441 . للتفصيل راجع – آمال قارة، مرجع سابق ، ص134. وانظر أيضا نائلة عادل قورة ، مرجع سابق، ص588.

[2] – عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص134.

[3] – المرجع نفسه ، ص164.

[4] – ايهاب فوزي السقا ، مرجع سابق ، ص 56.

[5] – تنص المادة 15 على أنه :"للمحررات الالكترونية في نطاق المعاملات المدنية والتجارية والادارية، ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحام قانون الإثبات في المواد المدنية والتجارية ".

[6] – تنص المادة 23 من قانون التوقيع الالكتروني المصري على أنه:" يعاقب كل من زور توقيع أو محرر الكتروني بطريق للاصطناع أو التعديل أو التحوير أو بأي طريق آخر"

أما بالنسبة للتشريع الجزائري فانه أدرج النصوص الخاصة بتزوير المحررات في الأقسام الثالث والرابع و الخامس من الفصل السابع من الباب الأول من الكتاب الثالث من قانون العقوبات في المواد 214 إلى 229 التي تشترط المحرر لتطبيق جريمة التزوير ، إلا أنه لم يستحدث نصا خاصا بالتزوير المعلوماتي، و لم يعدل نصوص التزوير لتصبح تشمل كافة صور .

وكان من الأفضل لو أضاف المشرع الجزائري نصا يعرف فيه التزوير على أنه كل تغيير للحقيقة بطريق الغش في مكتوب أو في أي دعامة أخرى تحتوي تعبيرا عن الفكر ، حيث يمكن أن

جزائية فعالة لكافة المستندات[1].

وبالتالي لم ينص المشرع الجزائري على جريمة التزوير المعلوماتي بصراحة كما فعل المشرع الفرنسي في المادة 441 من قانون العقوبات الفرنسي[2]، فهل يمكن تطبيق نصوص التزوير التقليدية على جريمة تزوير المحررات الالكترونية [3].

الفرع الثاني: مدى خضوع المحررات الالكترونية للنشاط الإجرامي للتزوير

يتمثل النشاط الإجرامي لجريمة التزوير في فعل تغيير الحقيقة و يعني استبدالها بما يخالفها بمعنى إدخال تغيير على المحرر على نحو يغير مضمونه أو شكله ، ولكن بشكل لا يعدمه أو يهدر قيمته ، ويستوي أن يكون تغيير الحقيقة كليا أو جزئيا، نتفى التزوير[4].

---

[1] – آمال قارة، مرجع سابق ، ص134

[2] – راجع المادة 441 من قانون العقوبات الفرنسي

[3] – راجع الفصل السابع من المواد197– 253 مكرر من قانون العقوبات الجزائري .

[4] – والمقصود هنا تغيير الحقيقة القانونية النسبية وليس تغيير الحقيقة الواقعية المطلقة، إذ يكفي لتغيير الحقيقة الذي تتطلبه جريمة التزوير أن يكون هناك مساس بحقوق الغير، أو مراكزهم القانونية الثابتة في تلك المحررات . للتفصيل راجع فوزية عبد الستار ، مرجع سابق ، ص245. محمود نجيب حسني ، مرجع سابق، ص218.

إن مجرد تغيير الحقيقة لايكفي لقيام جريمة التزوير ، وأن يتم بإحدى الأشكال التي حددها القانون سواء الطرق المادية أو المعنوية ، وأن يترتب عليه ضرر[1] .

ولقد حدد المشرع الجزائري أشكال تزوير المحررات في المواد 214-216 من قانون العقوبات[2] كما حدد المشرع المصري طرق التزوير على سبيل الحصر في المادتين 211، 213 من قانون العقوبات .

وعليه هل يمكن تغيير الحقيقة في المحررات الالكترونية بطرق التزوير المادي والمعنوي ؟

أولا- مدى إمكانية تغيير الحقيقة في المحررات الالكترونية بالتزوير المادي:

يقصد بالتزوير المادي هو تغيير الحقيقة بطريقة مادية تترك أثرا يدركه البصر ، وقد لا يتبين إلا بالاستعانة إلا بالخبير [3].

ولقد حدد المشرع الجزائري أشكال التزوير المادي في المادتين 214، و216 من قانون العقوبات بينما نص عليها المشرع المصري في المادة 211 من قانون العقوبات .

وعلى العموم تمثلت هذه الأشكال في التلاعب بالمحررات بالإدخال والتغيير و المحو ، والتقليد والاصطناع ، وانتحال شخصية الغير أو الحلول محلها [4].

---

[1] - يعرف الفقهاء الضر بأنه مساس بمصلحة يحميها القانون ، ولا يتطلب القانون وقوع الضرر فعلا ويكفي أن يكون الضرر محتملا، والضرر الفعلي هو الضرر المحقق أي الواقع فعلا ، أما الضرر المحتمل متى كان يمكن تحققه في المستقبل

[2] - حدد المشرع الجزائري عدة أشكال للتزوير في المحررات في المواد 214-229 ، ونص على أشكال التزوير المادي في المادتين 214، و216، بينما أشكال التزوير المعنوي نص عليها في المادة 215 من قانون العقوبات.

[3] - محمود محمود مصطفى، مرجع سابق ، ص141.

[4] - إذ تنص المادة 214 من قانون العقوبات على أنه يعاقب بالسجن المؤبد كل قاضي أو موظف ارتكب تزوير في المحررات العرفية أو الرسمية أثناء تأدية وظيفته : بوضع توقيعات مزورة ، أو بإحداث تغيير في المحررات أو الخطوط أو التوقيعات ، أو بانتحال شخصية الغير أو الحلول محلها ، أو بالكتابة في السجلات أو غيرها من المحررات العمومية أو بالتغيير فيها بعد إتمامها أو قفلها .

ويتصور وقوع فعل تغيير الحقيقة في المحررات الالكترونية من خلال طرق التزوير المادية ولكن بشرط أن يكون التزوير لاحقا على نشأة المستند الأصلي و الحقيقي المعالج آليا ، فلا تتحقق تلك الجريمة بتغيير الحقيقة أثناء نشأة المستند خلاف جريمة التزوير العادية[1].

وعليه يمكن تصور تغيير الحقيقة في نطاق المحررات الالكترونية بالطرق المحددة قانونا على وهي بصفة عامة التلاعب في المعطيات بالإضافة والحذف والتعديل ، والتقليد والاصطناع ، وانتحال شخصية الغير أو الحلول محلها.

ويتم التلاعب بالمحررات الالكترونية بالإدخال عن طريق إدخال بعض البيانات أو المعلومات إلى برنامج من خلال استغلال الأخطاء والعيوب ، أوعن طريق تزوير التوقيعات والأختام والبصمات بإدخالها بواسطة جهاز الماسح الضوئي المرتبط بالحاسوب ، ويضاف التوقيع أو الختم أو البصمة للورقة التي احتوت على البيان المزور ومن ثمة إضفاء الرسمية على هذه المحررات [2]، كما يمكن أيضا تزوير الصور الشخصية بإدخالها لجهاز الحاسوب عن طريق جهاز الماسح الضوئي ثم التلاعب بها ووضعا في محررات [3].

كما يتم التلاعب بالمحررات الالكترونية أيضا بمحو بعض أو كل البيانات من خلال الحذف أو الشطب ، مما يجعلها غير صالحة للاحتجاج بها أو الانتفاع منها كما هو الحال بالنسبة للشخص الذي دخل على برنامج سجلات الشرطة وقام بحذف بعض أسماء المجرمين المطلوبين للعدالة وذلك في عام 1979 ، ويتحقق تغير الحقيقة أيضا بإتلاف كل أو بعض البيانات ولكن لا يعد الإتلاف على البرنامج الذي تحويه تلك البيانات أو المعلومات لأننا هنا لا نكون بصدد جريمة التزوير المعلوماتي نكون أمام جريمة أخرى هي جريمة إتلاف المعلومات[4].

---

[1] – عبد القادر القهوجي، مرجع سابق، ص155.

[2] – إيهاب فوزي السقا، مرجع سابق، ص64. و عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، مرجع سابق ص190.

[3] – إيهاب فوزي السقا، مرجع سابق، ص68.

[4] – عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، مرجع سابق، ص191.

كذلك يتم التلاعب بتعديل المعلومات والبيانات الالكترونية ، وهي طريقة تجمع بين الحذف والإضافة كاستبدال كلمة بكلمة أو رقم برقم [1]، مثل لطبع فواتير مصطنعة أو فواتير ذات قيمة كبيرة ويقوم العملاء بتسديدها منخدعين في الثقة التامة التي يتوسمونها في تلك الحاسبات، ومثال ذلك قيام العاملين في شركة تأمين بولاية لوس أنجلوس الأمريكية باختلاق بفعل حاسبها الآلي 64 ألف ، وقد تقاضت تلك الشركة
من اتحاد الشركات التأمين في الولايات المتحدة عمولة نظيرا إجمالي لتلك الوثائق في حين اقتصر دورها فقط على إدارة الحسابات، ولغرض إعطاء العقود الوهمية مظهرا
الشركة المذكورة بتفعيل الملفات المختلفة عن طريق تغيير الوظيفة وبعض البيانات الوهمية [2].

ويتصور أيضا وقوع التزوير للمحررات الالكترونية بواسطة التقليد الذي هو المحاكاة، أي إنشاء محرر مشابه محرر آخر، كنسخ البرامج دون ترخيص ، أو تقليد العلامات أو الدفاتر التجارية [3].

وكذلك يمكن تصور التزوير المعلوماتي بالاصطناع الذي هو إنشاء محرر بأكمله ونسبته إلى غير مصدره ، كتزوير النقود الورقية بواسطة الحاسوب أو كإنشاء مواقع وهمية على شبكة الانترنت ونسبتها إلى شركة تجارية لها مواقع على الانترنت ، بهدف الاستيلاء على البيانات الخاصة بمستخدمي الموقع كرقم بطاقته الائتمانية [4].

---

[1] – فوزية عبد الستار، مرجع سابق ، ص261.

[2]– محمد عبد الله أبو بكر سلامة، جرائم الكومبيوتر والانترنت (موسوعة جرائم المعلوماتية)، دار المعارف، بالإسكندرية مصر، 2006، ص 7.

[3] _

إمضاءات مزورة للمحررات ، ففي هذه الحالة تحقق التقليد مع الاصطناع .ومع ذلك يرى جانب من الفقه أن التقليد قد يقع لوحده مثال ذلك تقليد خط الغير في محرر موقع على بياض.

[4] – إيهاب فوزي السقا، مرجع سابق، ص72.عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت ، مرجع سابق ، ص202

وأيضا يتم التزوير المادي بانتحال شخصية الغير أو الحلول محلها ، كمن يعثر على بطاقة ائتمان ن ثم يقوم باستخدامها في الشراء والدفع من خلال مواقع الانترنت والحصول على سلعة أو خدمة منتحلا اسم وصفة صاحب بطاقة الائتمان [1].

ثانيا – مدى إمكانية تغيير الحقيقة في المحررات الالكترونية بالتزوير المعنوي :

والتزوير المعنوي يتحقق بتغيير الحقيقة في محرر دون المساس بمادته أو شكله، لذلك فهو لا يترك أثرا يمكن إدراكه بالحواس ، لذلك هناك صعوبة في إثباته على عكس التزوير المادي ويقع التزوير المعنوي غالبا عند إنشاء المحرر[2].

ولقد نص المشرع الجزائري على التزوير المعنوي في الماد ة 215 من قانون العقوبات [3]، كما نص عيها المشرع المصري في المادة 213 من قانون العقوبات ، وتمثلت عموما بتغيير أو إسقاط الموظف لا قرارات أصحابها، أو بجعل واقعة مزورة في صورة واقعة صحيحة ، أو بجعل واقعة معترف بها في صورة واقعة غير معترف .

ويرى جانب من الفقه لا يتصور وقوع فعل تغيير الحقيقة من خلال طرق التزوير المعنوية و التي لا تتحقق إلا أثناء تكوين المستند[4] .

وفي المقابل يرى رأي أخر إمكانية حدوث التزوير المعنوي في المحررات الالكترونية عن طريق تزوير إقرارات صاحب الشأن، بقيام الموظف العام بتغيير الحقيقة في محرر الكتروني يدونه

---

[1] – انظر ايهاب فوزي السقا ، مرجع سابق ، ص 75.

[2] – محمود محمود مصطفي ، مرجع سابق ، ص141.

[3] – تنص المادة 215 من قانون العقوبات الجزائري على أنه : "يعاقب بالسجن المؤبد كل قاض أو موظف أو قائم بوظيفة عمومية قام أثناء تحرير محررات من أعمال وظيفته بتزييف جوهرها أو ظروفها بطريق الغش وذلك إما بكتابة اتفاقات خلاف التي دونت أو أمليت من طرف الإطراف أو بتقريره وقائع يعلم أنها كاذبة في صورة وقائع صحيحة أو بالشهادة كذبا بان وقائع قد اعترف بها أو وقعت في حضوره أو بإسقاطه أو بتغييره عمدا الإقرارات التي تلقاها ".

[4] – عبد القادر القهوجي، مرجع سابق، ص151.

كالمحررات الالكترونية البنكية، وفواتير الهاتف وحسابات المؤسسات والشركات المخزن داخل الحاسوب[1].

كما يمكن وقوع التزوير المعنوي المعلوماتي بواسطة جعل واقعة مزورة في صورة واقعة صحيحة بانتحال شخصية الغير كمن يعثر أو يسرق بطاقة ائتمان شخص ما ويقوم باستخدامها في الحصول على سلعة أو خدمة ، منتحلا اسم وصفة صاحب بطاقة الائتمان[2].

كما تتحقق هذه الصورة بالترك ، كأن يتعمد محاسب احدي الشركات عند إعداد رواتب العاملين والتي تكون غالبا ضمن برنامج على جهاز الحاسوب إسقاط دفعة الدين التي سددها الموظف من راتبه ضمن قرض حصل عليه أو يمتنع عن التأشير على مديونته للشركة [3].

ويقع أيضا التزوير المعنوي بجعل واقعة معترف بها ففي صورة واقعة غير معترف بها كأن يثبت موثق العقد في العقد الالكتروني أن البائع اقر أمامه بقبض الثمن مع أنه لم يقر بذلك.

والحقيقة أن التزوير المعنوي يمكن حدوثه في المحررات الالكترونية مع كثرة استعمال البيانات المعلوماتية في الحياة العملية سواء في المجالات الأمنية والقضائية والطبية وبصفة خاصة المعاملات التجارية الالكترونية [4] .

---

[1] – إيهاب فوزي السقا، مرجع سابق، ص74.

[2] – ايهاب فوزي السقا ، مرجع سابق ، ص75.

[3] – عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، مرجع سابق ص218.

[4] – كامل عفيفي عفيفي ، مرجع سابق ، ص255.

الفصل الثاني

الحماية الجنائية الموضوعية للتجارة الالكترونية في إطار نصوص خاصة

نظرا لقصور الحماية الجنائية للتجارة الالكترونية بواسطة النصوص العامة التقليدية وبصفة خاصة نصوص جرائم الأموال وجرائم التزوير، من حيث أنها وضعت للأموال المادية، ومن حيث عدم تناسب العقوبات مع جرائم التجارة الالكترونية ، وعليه برزت الحاجة إلى حماية جنائية خاصة للتجارة الالكترونية في إطار قانون العقوبات أو في قوانين مستقلة .

وبناءا على ذلك وضعت لجنة الأمم المتحدة للقانون التجاري الدولي قوانين نموذجية للتجارة الالكترونية ، كالقانون النموذجي للتجارة الالكترونية لعام 1996، والقانون النموذجي للتوقيعات الالكترونية لعام 2001 ، كما أصدر الاتحاد الأوربي مجموعة من التوجيهات كالتوجيه الأوربي رقم 200-31 المتعلق بالتجارة الالكترونية ، والتوجيه رقم 97- 07 المتعلق بحماية المستهلك في العقود عن بعد والتوجيه الأوربي رقم 97- 489 بشان الدفع الالكتروني ، والتوجيه رقم 99-93 بشأن التوقيع الالكتروني .

كما اهتمت بعض الدول بحماية التجارة الالكترونية كفرنسا التي أصدرت قانون رقم 91-1382 المتعلق بأمن الشيكات وبطاقات الوفاء ، كما أصدرت بعض الدول العربية قوانين للتجارة الالكترونية كقانون المبادلات والتجارة الالكترونية التونسي لعام 2000، وقانون التوقيع الالكتروني المصري رقم 15-2004 لعام 2004، كما كفلت فرنسا والولايات المتحدة الأمريكية وانجلترا وفرنسا والجزائر في إطار نصوص الجريمة المعلوماتية .

تثير التجارة الالكترونية مشكلات عملية وقانونية ، من أهمها جرائم الاعتداء على التاجر وجرائم الاعتداء على المستهلك سواء تعلق الأمر بحماية بياناته الخاصة أو تلك المتعلقة بتعاملاته المالية . وعليه سنبحث الحماية الجنائية للتاجر في التجارة الالكترونية **(المبحث الأول)**، ثم الحماية الجنائية للمستهلك في التجارة الالكترونية **(المبحث الثاني)**

المبحث الأول

الحماية الجنائية للتاجر في التجارة الالكترونية

تثير التجارة الالكترونية مشكلات عملية وقانونية في القانون الجنائي، من أهمها جرائم الاعتداء على التاجر، ومن هنا برزت الحماية الجنائية للتاجر في التجارة الالكترونية وبصفة خاصة من الاعتداء على مواقع التجارية الالكترونية.

تعد مواقع التجارة الالكترونية الوسيلة الأساسية للقيام بالتجارة الالكترونية، لذلك تحتاج إلى حماية جنائية، على أساس أنها تتضمن مختلف المعلومات المتعلقة بالأفراد والشركات، وقد أدركت كثير من التشريعات هذه الحقيقة فجاءت بنصوص خاصة لحمايتها.

وتحتاج مواقع الانترنت خدمات وسيطة يقوم بها مزودي خدمات الانترنت ينحصر دورهم في تمكين المستخدم من الدخول إلى شبكة الانترنت مثل متعهد الوصول والدخول إلى شبكة الانترنت ومقدم خدمات الإيواء (متعهد الإيواء) ، وكذلك مورد المعلومات أو منتجها ، ونظرا للدور الفني الكبير لهؤلاء ، قامت التشريعات بحماية التاجر من خلال تحميل هؤلاء المسؤولية الجنائية .

وعليه سنتناول جرائم الاعتداء على مواقع التجارة الالكترونية (المطلب الأول)، ثم جرائم المسؤولية الجنائية لوسطاء الانترنت (المطلب الثاني)، على التفصيل الآتي :

المطلب الأول: جرائم الاعتداء على مواقع التجارة الالكترونية

تعد جرائم الاعتداء على مواقع التجارة الالكترونية من أخطر الجرائم المعلوماتية , ذلك أن اغلب الجرائم لايمكن ارتكابها إلا بعد الدخول إلى النظام لذلك أولت لها التشريعات اهتماما كبيرا أبرزها التشريع الأمريكي المتعلق بجرائم الحاسوب الصادر سنة 1984 المعدل في سنة 1996 والتشريع الفرنسي الصادر بالقانون رقم 19/88 الصادر في سنة 1988 و المعدل في 1994 وكذلك بعض التشريعات العربية كالتشريع الجزائري بالقانون رقم 15/04 المؤرخ في 10 نوفمبر

2004 المعدل والمتمم للأمر 155/66 المتضمن قانون العقوبات [1]، والتشريع التونسي أيضا بالقانون رقم 89 لسنة 1999 المؤرخ في 2 أوت 1999.

وتقع جرائم الاعتداء على مواقع التجارة الالكترونية على نظام المواقع (الفرع الأول)، وبيانات المواقع (الفرع الثاني) [2]، على النحو الآتي :

الفرع الأول: جرائم الاعتداء على نظام مواقع التجارة الالكترونية

تتمثل جرائم الاعتداء على نظام المواقع في الدخول أوالبقاء غير المشروع والاعتداء على سير وسلامة المواقع بالتعطيل والتدمير ، على التفصيل الآتي :

أولا- جريمة الدخول أوالبقاء غير المشروع :

نص عليها المشرع الفرنسي في المادة 1/323، والمشرع الأمريكي في المادة 1/1030 والمشرع الانجليزي في المادة الأولى ، وكذا بعض التشريعات العربية كالتشريع الجزائري في المادة 394 مكرر من قانون العقوبات الجزائري ، [3] ونظمها أيضا التشريع التونسي في الفصل 199 في قانون العقوبات. وجريمة الدخول أوالبقاء غير المشروع تتكون من ركن مادي ومعنوي.

1- الركن المادي:

يتكون الركن المادي لهذه الجريمة من نشاط إجرامي يتمثل في فعل الدخول غير المرخص به إلى نظام المعالجة الآلية للمعطيات أو في جزء منه، أوالبقاء غير المصرح به، كالآتي :

---

[1] - القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 155/66 المؤرخ في 08 جوان 1966المتضمن قانون العقوبات الجزائري ، ج رع 71 صادرة في 10/10/ 2004.

[2] - على خلاف التشريع الجزائري والتونسي لم ينص المشرع المصري على جرائم الاعتداء على مواقع التجارة الالكترونية.

[3] - تنص المادة 394 مكرر من قانون العقوبات الجزائري على معاقبة كل من يدخل عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك وتضاعف العقوبة إذا ترتب على الدخول أو البقاء حذف أو تغيير معطيات المنظومة أو تخريب النظام .

أ-الدخول غير المشروع :

لم تحدد التشريعات المقارنة المقصود بالدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات ، ويمكن تعريفه بأنه الدخول إلى المعطيات المخزنة داخل نظام الحاسوب دون رضا المسؤول عن هذا النظام [1].

ويلاحظ أن المشرع التونسي استعمل عبارة النفاذ عوضا عن عبارة الدخول ليؤكد الخاصية اللامادية لهذه الجريمة[2]، فعبارة الدخول قد يكون لها مدلول مادي في حين أن النفاذ له مدلول [3].

لكن الحقيقة أن النفاذ له مدلول معنوي، ومدلول مادي يتمثل في محاولة الشخص الدخول أو الدخول بالفعل إلى النظام المعلوماتي، فاعتماد المدلول المعنوي فقط للنفاذ يجعل الجريمة مقتصرة على فئة محددة من المجرمين الحاذقين، في حين أن الجريمة يمكن أن ترتكب من أي شخص تمكن من الولوج إلى النظام، أومن خلال عمليات مادية تنفذ على النظام المعلوماتي[4].

ولم يحدد المشرع في أغلب الدول وسيلة الدخول ، لذا تقع هذه الجريمة بأي وسيلة ، من ذلك استعمال كلمة السر الحقيقية متى كان الجاني غير مخول له في استخدامها أو استخدام برنامج أو شفرة خاص، أو الدخول من خلال شخص غير مسموح له بالدخول، أو عن طريق تجاوز نظام

---

[1] – وقد أشار المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد في البرازيل لسنة 1994بشأن جرائم الكمبيوتر إلى هذا المعنى ، حين اعتبر أن الدخول غير المرخص به هو التوصل أو الولوج دون تصريح إلى نظام ما عن طريق انتهاك إجراءات الأمن ، ولم يحد وسيلة أو طريقة الدخول. للتفصيل راجع نائلة عادل قورة ، مرجع سابق ص316.

[2] -عماد بوخريص وحسنى غديره ، جرائم الإعلامية ، ملتقى بمحكمة الاستئناف بسوسة 2 جوان 2001، ص 18.

2- Gassin ® la protection pénale d'une nouvelle universalité de fait en droit français : le système de traitement automatisé des données, Dalloz 1989, 4ème cahier, P17

3-Deveze (J) Atteinte au système automatisé des données, Juris classeur pénal, 4ème , 1997, p294.

الحماية[1]، أو عن طريق إدخال برنامج فيروس أو باستخدام الرقم الكودي لشخص آخر أو تجاوز نظام الحماية إذا كان ضعيفا ، أو باستعمال كلمة السر الحقيقية متى كان الجاني غير مخول له في استخدامها ،أو الدخول من خلال شخص غير مسموح له بالدخول، أو عن طريق تجاوز نظام الحماية [2]، ويستوي أن يتم الدخول مباشرة أو بطريق غير مباشرة كما هو الحال في الدخول عن بعد عن طريق شبكات الاتصال التلفونية[3].

ولم يشترط المشرع الجزائري والتونسي، أسوة بالمشرع الفرنسي لتوافر جريمة الاعتداء على نظام المعالجة الآلية على ضرورة توافر الحماية الفنية لهذا النظام، بل أن يكون غير مأذون له في ذلك، إلا أن هناك جانب من الفقه يرى ضرورة وجود نظام أمني لقيام الجريمة خاصة ، وأن توفر هذه الحماية الفنية والدخول بالرغم من ذلك إلى نظام المعالجة الآلية من شأنه أن يكون دليلا قاطعا على توفر القصد لدى الجاني ، الذي لايمكن أن يدخل صدفة ، بل باستعمال طرق تقنية لخرق الحماية [4]، غير أن هذا الاتجاه لم يتبنى في فرنسا والجزائر وتونس وقد تدعم ذلك بموقف القضاء الفرنسي من خلال القرار الاستئنافي الصادر عن محكمة باريس في 5 أفريل 1994 الذي جاء به أنه " لا يشترط لقيام الجريمة وجود وسائل حماية لنظام المعالجة المعلوماتية"، وبالتالي فلا يشترط إذا لقيام هذه الجريمة أن يقع اختراق لنظام حماية ، بل يكفي أن يكون النفاذ غير مشروع [5].

---

[1] – عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص 29.

[2] – عبد القدر القهوجي، مرجع سابق، ص 29. مدحت رمضان، مرجع سابق، ص50-51.

[3]-Gassin. R. op. cit. P16.

[4]– تنص المادة 02 من الاتفاقية الدولية للإجرام المعلوماتي تسمح للدولة العضو أن تشترط بأن ترتكب الجريمة عن طريق خرق الحماية الفنية للنظام بهدف الحصول على المعطيات الموجودة بداخله . راجع عبد الحليم رمضان، مرجع سابق ص52 . عبد القادر القهوجي، مرجع سابق، ص 124.

[5] –CA Paris, 5 Avril 1994, petite Affiche 1995, n° 80, P.13. note Alvarez « qu'il n'est pas nécessaire pou que l'infraction existe que l'accès soit limité par un dispositif de protection ».

ويتحقق الدخول غير المشروع متى كان ذلك مخالفا لإرادة صاحب النظام أو من له حق السيطرة عليه، من ذلك الأنظمة المتعلقة بأسرار الدولة أو التي تتضمن بيانات شخصية أو سر المهنة ، أو معلومات لايمكن الاطلاع عليها [1].

ولا عبرة في هذه الجريمة بصفة مرتكب الفعل الإجرامي ، فقد يكون الفاعل يعمل في مجال الأنظمة أو لا يعمل ، وسواء كان يفهم أو لا يفهم أسلوب تشغيل النظام ، فيكفي أن يكون الجاني ليس ممن لهم الحق في الدخول إلى النظام حتى تتوفر جريمة الدخول غير المشروع.

وبالتالي فإن الركن المادي لجريمة الدخول غير المرخص به يتحقق بمجرد شروع أي شخص في الدخول أو الدخول بالفعل إلى نظام المعالجة الآلية للمعطيات بأي طريقة، وتقع هذه الجريمة بالدخول إلى كل النظام أو جزء منه [2].

كما تقع الجريمة بمجرد الدخول دون اشتراط تحقق النتيجة ، فلا يشترط لقيامها مثلا التقاط متدخل المعلومات أو البرامج التي يحتويها النظام فجريمة الدخول غير المشروع من جرائم السلوك المحض فالسلوك الإجرامي مجرم في حد ذاته بغض النظر عن النتيجة [3].

[4]، الاأنه لم يتفق على

كونها جريمة وقتية أم مستمرة أم متتابعة ، إلا أن الاتجاه الراجح يعتبرها جريمة وقتية[5].

وعليه فان جريمة الدخول غير المرخص به تتحقق بمجرد الدخول أو محاولة الدخول من ليس له الحق أيا كانت صفته في كل أو جزء من نظام المعالجة الآلية للمعطيات ،

---

[1] – شيماء عبد الغني عطاء الله ، مرجع سابق ، ص102.

[2] – عبد القادر القهوجي، مرجع سابق ، ص131

[3] – محمد أمين الرومي، مرجع سابق، ص101. شيماء عبد الغني عطاء الله، مرجع سابق ، ص97.

[4] – إلا أن تشريعات أخرى تتطلب أن يتم الوصول إلى معلومات النظام لقيام الجريمة مثل التشريع الأمريكي في 1030/أ/1/ ، 1030/أ/2، 1030/أ/3 من القانون الفيدرالي لجرائم الحاسوب .

[5] – عبد الحليم رمضان، مرجع سابق، ص51.

الدخول غير المرخص حذف أو تغيير لمعطيات المنظومة أو تخريب نظام اشتغالها فان المادة 394 مكرر فقرة 2 من قانون العقوبات الجزائري ، والمادة 2/323 من قانون العقوبات الفرنسي نصتا على مضاعفة العقوبة[1].

ب- البقاء غير المشروع:

ويقصد به التواجد داخل نظام مواقع التجارة الالكترونية ضد إرادة من له الحق في السيطرة على هذا النظام ، وقد يتحقق البقاء المعاقب عليه مستقلا عن الدخول إلى النظام إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ لكن المتدخل لم ينسحب و بقي رغم ذلك فيعاقب في هذه الحالة على جريمة البقاء غير المشروع إذا توافر ركنها المعنوي[2].

ويعتبر البقاء أيضا جريمة في الحالة التي يستمر فيها الجاني داخل النظام بعد المدة المحددة له للبقاء داخله ، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها برؤيتها والاطلاع عليها فقط[3].

وقد يجتمع الدخول مع البقاء غير المصرح بهما معا ، وذلك في الحالة التي لا يكون فيها للجاني له الحق في الدخول إلى النظام ويدخل إليه فعلا ضد إرادة من له حق السيطرة عليه ثم يبقى داخل النظام بعد ذلك ، وقد ثار تساؤل بين الفقه فيما إذا كان فعل الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه بدون إذن يشكل تعدد مادي للجرائم أم أنه جريمة واحدة[4].

---

[1] – تنص المادة 394 مكرر فقرة 2 من قانون العقوبات الجزائري ، على انه "تضاعف العقوبة إذا ترتب عن الدخول أو البقاء غير المرخص به حذف أو تغيير لمعطيات المنظومة أو تخريب نظام اشتغالها، وتكون العقوبة بالحبس من 6أشهر إلى سنتين والغرامة من 50 ألف إلى 150 ألف دينار".

[2] – عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية،الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص 29. عبد القادر القهوجي ، مرجع سابق ، ص 133.

[3] – عبد القادر القهوجي، مرجع سابق، ص 133.

[4] – محمد أمين الشوابكة ، مرجع سابق ، ص 133. عبد الحليم رمضان، مرجع سابق ، ص52.

ذهب البعض إلى القول بأننا أمام جريمة واحدة ، لان الجاني قصد بالدخول البقاء داخل النظام ، بينما ذهب البعض الآخر إلى تحقق الاجتماع المادي بين الجريمتين وهو الراجح في [1].

المعلوماتي ، فإن جريمة البقاء غير المشروع تبدأ منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام أو يستمر بعد انتهاء الوقت المحدد [2]، لكن إن ظل ساكنا تظل الجريمة جريمة دخول غير مشروع ، أما إذا بدأ في التجول فان جريمة البقاء غير المشروع تبدأ منذ تلك اللحظة ، لأنه يتجول في نظام يعلم مسبقا أن مبدأ دخوله و استمراره فيه غير مشروع [3].

ويكفي لتحقق تلك الجريمة البقاء داخل النظام كله أو في جزء منه البقاء داخل النظام بدون اشتراط تحقق نتيجة ما كالتقاط البرامج أو المعلومات لكونها من جرائم السلوك المحض أي من الجرائم الشكلية التي تقوم بجرد توافر السلوك المجرم دون اشتراط نتيجة معينة
الغالب في الفقه يعتبرها كذلك إلا أن الفقه لم يتفق على كونها جريمة وقتية أم مستمرة أم متتابعة لكنها في الحقيقة مستمرة يستمر فيها النشاط الإجرام لمدة معينة[4].

تعد هذه الجرائم من الجرائم الشكلية كالجريمة السابقة، لا يشترط فيه حدوث أي نتيجة إجرامية فيكفي البقاء في نظام المعالجة غير مسموح بدخوله. كما أنها تعد من الجرائم المستمرة فتبقى الجريمة قائمة طالما أن الجاني ما زال باقيا على الاتصال بالنظام المعلوماتي.

---

[1] – شيماء عبد الغني عطاء الله ، مرجع سابق ، ص121

[2] - يتحقق الركن المادي لهذه الجريمة منذ اللحظة التي يقرر فيها الجاني الإبقاء على الاتصال و عدم الخروج منه، فهذه الجريمة من جرائم الامتناع ويتمثل في الامتناع عن قطع الاتصال مع النظام. راجع محمد أمين الرومي، م س، ص 105.

[3] – اختلف الفقهاء في بداية جريمة البقاء في حالة الاجتماع المادي لجريمة الدخول مع البقاء، فذهب رأي إلى تحققها منذ لحظة الدخول، و آخر منذ علمه بأن بقاءه غير مشروع، وذهب رأي آخر إلى تحققها منذ إنذاره.

[4] – عبد القادر القهوجي، مرجع سابق، ص 126.

وقد نص المشرع الجزائري في المادة 394 مكرر02 المقابلة للمادة 1/323عقوبات فرنسي على مضاعفة العقوبة إذا نتج عن البقاء عن البقاء أما محو أو تعديل معطيات النظام وأما عدم صلاحية النظام لأداء وظائفه [1].

ويكفي لتوافر هذا الظرف وجود علاقة سببية بين البقاء غير المشروع وتلك النتيجة الضارة سواء محو أو تعديل معطيات النظام أو عدم قدرته على تنفيذ المعالجة الآلية للمعطيات ، إلا إذا أثبت الجاني انتفاء تلك العلاقة، كأن يثبت أن تعديل أو محو المعطيات أو عدم صلاحية النظام يرجع إلى القوة القاهرة [2].

2- الركن المعنوي:

جريمة الدخول أو البقاء داخل مواقع التجارة الالكترونية جريمة عمدية لابد فيها من توافر القصد الجنائي بعنصريه العلم والإرادة ، فيلزم أن تتجه إرادة الجاني إلى فعل الدخول أو البقاء في مواقع التجارة الالكترونية ، وأن يعلم أنه ليس له الحق في الدخول إلى الموقع أو البقاء فيه [3].

ومن ثمة فلا يتوافر القصد الجنائي إذا كان دخول الجاني داخل النظام مسموح به أي مشروع أو إذا وقع في خطأ كأن يجهل وجود حظر للدخول أو البقاء[4]، ويكفي فيها توافر القصد الجنائي العام ، ولا يشترط أيضا توافر قصد جنائي خاص [5].

---

[1] – عاقب المشرع الجزائري في المادة 394 مكرر فقرة 2 على الدخول أو البقاء غير المصرح بهما إذا ترتب عنه الإخلال بسير النظام بالحبس من 6 أشهر إلى سنتين وبغرامة من 50الف إلى 150الف د ج.

[2] - عبد القادر القهوجي ، مرجع سابق ، ص 127.

[3] - شيماء عبد الغني عطاء الله ، مرجع سابق ، ص126

[4] – مدحت عبد الحليم رمضان، مرجع سابق، ص52.

[5] – لقد اشترطت بعض التشريعات قصد خاص يترتب عليه تشديد العقوبة ن كالتشريع الدانمركي الذي يشدد العقوبة متى ارتكب الفعل بقصد الإحاطة بأسرار عمل إحدى الشركات ، وفي استراليا إذا كان بقصد الإضرار بالغير ، وكذلك التشريع النرويجي بنية الحصول على ربح أو إلحاق ضرر بالغير .

كما لا يشترط أن يترتب على دخول الجاني إلى نظام المعلومات تحقق نتيجة معينة ، ولا عبرة بالباعث الذي يجعل الجاني يبقى على اتصال بالنظام المعلوماتي غير المسموح له البقاء فيه، فقد يكون باعثه هو الفضول أو المزاح أو الحصول على المعلومات أو غير ذلك[1].

وبالتالي لقيام جريمة الدخول غير المرخص به يجب أن يتوافر بجانب الركن المادي نية الغش، ويقصد بالغش أن يباشر الفاعل سلوكه عن سوء نية وبغرض خداع الغير[2].

ويمكن للقاضي الجنائي أن يستدل على توافر القصد الجنائي لدى الجاني إذا كان النظام المعلوماتي محاط بنظام أمني وتم اختراقه ، فنظام الأمن لا يعدو إلا أن يكون وسيلة إثبات سوء النية من قام بانتهاك النظام ودخل بطريقة غير مشروعة .

إلا أن جانب من الفقه يرى أن النظام الأمني ضروري لتجريم الدخول النظام المعلوماتي إذ يقتضي المنطق والعدالة توافر هذا الشرط، حيث أن القانون الجنائي لا ينبغي أن يقوم بحماية الأشخاص الذين لا يأخذون الاحتياط اللازم المتطلب من إنسان متوسط الذكاء [3]، فوجود نظام حماية يمكن أن يكون التزاما مفروضا قانونا على كل من يقوم بإدارة نظام معلوماتي، ومن ثمة يفترض أن تقع الجريمة على نظام لايجوز الدخول إليه من أشخاص محددين[4].

---

[1] –تطبيقا لذلك قضت محكمة باريس في 25 فيفري 2000 بوقوع الجريمة من مهندس أراد أن يثبت لأحد البنوك قدرته الفنية على اختراق أنظمة البنك حتى يفوز بعقد تدريب كوادر البنك ، فقام باختراق أنظمة هذا البنك على الرغم من تعدد وسائل الحماية التي وضعها البنك ضد الاختراق .

[2] – محمد أمين الرومي ، مرجع سابق ، ص 103– 104. أمين أعزان ، مرجع السابق ، ص170 وما بعدها . شيماء عبد الغني عطاء الله ، مرجع السابق ، ص126.

[3] – محمد أمين الرومي، مرجع سابق ، ص 103.

[4] – فعدم ذكر شرط الحماية الفنية يعني أن المشرع أراد استبعادها، طالما لم ينص المشرع صراحة على ذلك فان المبادئ المستقرة في القانون الجنائي تأبى تقييد النص المطلق وتخصيص النص العام، والحقيقة أن اشتراط هذا الشرط قد يؤدي إلى الحد من الحماية الجنائية لنظم المعلومات الآلية المشمولة بالحماية الأمنية لهذا اكتفى المشرع الفرنسي ونظيره الجزائري في النص النهائي بأن يكون الدخول قدتم بطريق الغش.

وبالتالي فإنه إذا توافر الركن المادي الذي يتخذ صورة الدخول أوالبقاء داخل النظام والركن المعنوي المتمثل في القصد الجنائي العام بعنصريه العلم والإرادة قامت جريمة الدخول أوالبقاء.

ثانيا- جريمة الاعتداء على سلامة مواقع التجارة الالكترونية:

نص المشرع الفرنسي على جريمة الاعتداء على سلامة مواقع التجارة الالكترونية في المادة 2/323 ، وكذلك المشرع التونسي في الفصل 199 مكرر ، وعاقب المشرع الجزائري أيضا علي على تخريب النظام في المادة 394 مكرر/ف2 كظرف مشدد [1]. ويلزم لتحقق هذه الجريمة توافر الركن المادي والركن المعنوي، كالآتي :

1-الركن المادي:

يتمثل الركن المادي لجريمة الاعتداء على سلامة مواقع التجارة الالكترونية في التشريع الفرنسي والتونسي فعل التعطيل والإفساد.

أ-تعطيل وتوقيف المواقع:

تتعلق هذه الجريمة بتجريم كل فعل من شأنه أن يؤدي إلى توقيف تشغيل نظام المعالجة ، ويقصد به إحداث عطب أو خلل بالشيء بما يجعله لا يقوم بعمله بصورة طبيعية، وقد يكون ذلك بالحد من سرعة النظام المعلوماتي وجعله بطيئا أو يعطي نتائج غير مطلوبة[2].

ولا يشترط وقوع التوقف على كل عناصر النظام جملة، بل يكفي أن يكون جزئيا على أحد هذه العناصر سواء المادية أو المعنوية [3].

---

[1] – تنص المادة 394 مكرر/2 من قانون العقوبات على أنه : " تضاعف العقوبة ..... بتخريب نظام اشتغال المنظومة وتكون العقوبة بالحبس من 6 أشهر إلى سنتين والغرامة من 50 ألف إلى 150 ألف دينار".

[2] – محمد أمين محمد الشوابكة، مرجع سابق، ص 223، 224 .

[3] – عبد الحليم رمضان ، مرجع سابق ، ص54. وانظر أيضا: Gassin ®, Op.cit, P34

مادام المشرع لم يشترط وسيلة معينة للتوقيف أو التعطيل ، فقد يكون بوسيلة مادية أو معنوية وتكون وسيلة التعطيل مادية إذا وقعت على الأجهزة المادية للنظام مثل تخريبها أو قطع شبكات الاتصال ، وتكون وسيلة التعطيل المعنوية إذا وقعت على الكيانات المعنوية مثل البرامج والمعطيات ، كاستخدام القنبلة المعلوماتية يقع من خلالها تسريب برنامج يحتوى على تعليمات لإفساد سير النظام في وقت وتاريخ معين أو في صورة وقوع حدث معين ، أو بإدخال فيروس أو تعديل برامج كلمة السر على الدخول ، أو جعل النظام يتباطأ في أدائه لوظائفه [1].

وحتى يعاقب على التوقيف أو التعطيل يجب أن يكون بنشاط إيجابي يؤدي إلى توقيف النظام لا نشاط سلبي بالامتناع ، والذي لا تقوم الجريمة به ، لكن إن كان على عاتق الجاني واجب قانوني أو اتفاقي يتوقف على تدخله تشغيل النظام، وامتنع عن التدخل بقصد تعطيل النظام يتوافر أسباب الإباحة ، لا يتوفر

الركن المادي ولا تقوم الجريمة[2].

2- :

يعني الإفساد كل فعل يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم ، بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها ، أي أن الإفساد يعني إعدام الشيء وجعله غير صالح للاستعمال مطلقا، أي التأثير في المال بجعله غير قابل للاستعمال ولا يشترط وقوع الإفساد على كل النظام جملة، بل يكفي أن يكون جزئيا[3].

---

[1] –ويستوي أن يكون التعطيل دائما كما في حالة إدخال فيروس تدميري ، أو مؤقتا أو متقطعا على فترات منتظمة كما إذا تم إدخال قنبلة معلوماتية زمنية مبرمجة ينجم عنها شل النظام منذ البدء في تشغيله ، كما يستوي أن يكون التوقيف بالنسبة لجميع مستعملي النظام ، أم بالنسبة لأحده . للتفصيل راجع معبد القادر القهوجي، مرجع سابق، ص139.

[2] – عبد القادر القهوجي، مرجع سابق، ص139–140.

[3]– المرجع نفسه ، ص 140.

ومن هذه الناحية يختلف الإفساد عن التعطيل، من حيث أن التعطيل يتيح فرصة إصلاح لته الطبيعية، إلا أن الإفساد يترتب عنه انعدام صلاحية النظام المعلوماتي[1].

ويتحقق الإفساد بواسطة طرق عديدة ومتنوعة ، ويمكن أن تكون وسيلة التدمير مادية وذلك بتخريب الأجهزة المادية للنظام المعلوماتي أو قطع شبكات الاتصال أو بسكب أي مادة على الأجهزة، يترتب عنها تدمير النظام[2].

كما يمكن أن تكون وسيلة التدمير معنوية، عبر استعمال البرامج والفيروسات التي تؤدي إلى إعدام سير نظام المعالجة الآلية للمعلومات من أمثلها برامج الدودة التي تستهدف أكبر نطاق ممكن من النظام المعلوماتي، وتقوم بأعمال تخريب للبرامج والبيانات استخدام القنبلة المعلوماتية واستخدام فيروس حصان طروادة ، والذي يقوم بتغيير في المعطيات والبرامج[3].

والملاحظ أن فعل الإفساد بالمعنى السابق يشترك في جانب منه مع جريمة الإتلاف العادية ولما كان نص الجريمة الأخيرة عاما ، بينما نص جريمة الاعتداء القصدي على نظام المعالجة الآلية للمعطيات خاصا، فإنه يغلب النص الخاص على النص العام [4].

وتجدر الإشارة إلى أن اتفاقية بودابست لسنة 2001 والمتعلقة بالجريمة المعلوماتية تطرقت إلى الاعتداء على سلامة النظام المعلوماتي في المادة 05 ، إذ نصت على انه يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية للتجريم تبعا لقانونه المحلي

---

[1] – ويختلف الإفساد أيضا عن التخريب الذي صادفناه في جريمة الدخول أو البقاء غير المشروع ، في أن التخريب في حال الظرف المشدد لا يشترط فيه أن يكون قصديا ، بينما يتطلب فيه هذا الشرط بالنسبة لهذه الجريمة . راجع عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق ، ص41. انظر أيضا عبد القادر القهوجي ، مرجع سابق ن ص 141.

[2]– Gassin ® ,op.cit ,P35.

[3] –عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية ، الكتاب الثاني :الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص41–42.

[4] – عبد القادر القهوجي، مرجع سابق ، ص141

الإعاقة الخطيرة ، إذا تم ذلك عمدا وبدون حق ، لوظيفة نظام الحاسوب عن طريق إدخال ، أو نقل أو ، إضرار ، أو محو أو تعطيل أو إتلاف أو طمس البيانات المعلوماتية .

وبالتالي هذه الاتفاقية تهدف إلى تجريم الإعاقة للنظام ، ويقصد بها الأفعال التي تحمل اعتداءا على حسن تشغيل المنظومة المعلوماتية ، ويجب أن تكون الإعاقة جسيمة [1]، وأن تكون عمدية

و إدخال ، أو إضرار ، أو محو أو تعطيل أو إتلاف أو طمس البيانات المعلوماتية .

2- الركن المعنوي:

تعتبر جريمة الاعتداء على سلامة مواقع التجارة الالكترونية بالتعطيل ، والإفساد والتدمير جريمة عمدية ، يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة ، إذ يجب أن تتجه إرادة الجاني إلى فعل الإفساد ، كما يجب أن يعلم بأن نشاطه الإجرامي يؤدي إلى إفساد المواقع الالكترونية [2].

إهمال، فلا وجود لجريمة [3] كان لا يرتب مسؤوليته الجزائية فإنه

---

[1] - توضح المذكرة التفسيرية أن الإعاقة للنظام المعلوماتي تكون جسيمة ، عندما تكون البيانات المرسلة من الحجم أو التواتر ما يحمل ضررا جسيما لقدرة المالك والمشغل بالنسبة لاستخدام الجهاز أو الاتصال بالأجهزة الأخرى مثال ذلك البرامج والفيروسات التي تمنع أو تبطئ عمل النظام ، أو البرامج التي تؤدي غالى إرسال كم هائل من رسائل البريد الالكتروني من أجل شل النظام . للتفصيل راجع هلالي عبد الله أحمد ، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية ،الطبعة الأولى ، دار النهضة العربية ، القاهرة مصر 2003، ص. 93

[2] - نظرا لكون المشرع في فرنسا لم يحدد شكل الركن المعنوي بصورة واضحة ، فاختلف الفقه في تفسيره إلا أن الرأي الراجح يتجه إلى القصد الجنائي باعتباره الأصل في التجريم . للتفصيل راجع مدحت عبد الحليم رمضان، مرجع سابق، ص130-131.

[3] - عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني :الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص43. مدحت رمضان ، مرجع سابق ، ص55.

يمكن أن يرتب مسؤوليته المدنية ومطالبته بجبر الأضرار التي تسبب فيها، وبالتالي لا تقوم الجريمة لانتفاء القصد الجنائي .

وهكذا إذا توافر الركن المعنوي بعنصريه العلم والإرادة إلى جانب الركن المادي قامت الجريمة واستحق مرتكبها العقوبة المخصصة لهذه الجريمة، وتستخلص محكمة الموضوع توافر القصد الجنائي من ظروف وملابسات الواقعة [1].

الفرع الثاني: جرائم الاعتداء على بيانات مواقع التجارة الالكترونية

نصت التشريعات الأجنبية على جرائم الاعتداء على بيانات المواقع، ومن أبرزها التشريع الفرنسي، كما نصت عليها بعض التشريعات العربية كالتشريع الجزائري والتشريع التونسي،[2]

وعليه سنعالج هذه الجرائم في التشريع الفرنسي ، ثم في بعض التشريعات العربية كالآتي:

أولا – جرائم الاعتداء على بيانات المواقع في التشريع الفرنسي :

تتمثل هذه الجرائم في جريمة التلاعب ببيانات المواقع المنصوص عليها في المادة 3/323، وجريمة التزوير بموجب المادة 441 من قانون العقوبات الفرنسي، على النحو الآتي :

1-جريمة التلاعب بالبيانات :

نظم المشرع الفرنسي هذه الجريمة بموجب المادة 3/323 من قانون العقوبات ، والتي تنص على أنه يعاقب كل من اخل بطرق العش معطيات في نظام المعالجة الآلية للمعطيات ، أو محى ، أو عدل بطريق الغش ، بعقوبة الحبس حتى ثلاث سنوات وبغرامة حتى 300الف يورو.

---

[1] – شيماء عبد الغني عطاء الله، مرجع سابق، ص130.

[2] -كما نصت اتفاقية بودابست للجريمة المعلوماتية لسنة 2001 ، على الاعتداء على سلامة البيانات في المادة 04 بقولها: " يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية لتجريم ، إذا حدث عمدا ودون حق ، أي إضرار أو محو ، أو تعطيل ، أو إتلاف ، أو طمس لبيانات الحاسب ".

أ-الركن المادي:

يتضح لنا من المادة 323 أن الركن المادي لجريمة التلاعب بمعطيات المواقع يتخذ صور الإدخال ، أو التعديل ، أو الحذف [1]، كالآتي :

- إدخال بيانات في موقع التجارة الالكترونية:

ويقصد بالإدخال إضافة معطيات جديدة على الدعامة سواء كانت خالية أم كان يوجد بها معطيات من قبل، وقد يتم إدخال هذه المعطيات بقصد التشويش على صحة المعطيات القائمة، ولعل اصطناع المعلومات هو الأكثر سهولة في التنفيذ ولاسيما المؤسسات ذات الأموال [2].

ويتحقق هذا الفعل في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب والائتمان سواء من حاملها الشرعي ، أم من غيره في حالات السرقة أو الفقد أو التزوير، كما يتحقق فعل الإدخال بإدخال برنامج غريب (كفيروس ، أو قنبلة معلوماتية) يضيف معلومات جديدة [3].

وبالفعل قام أحد المسؤولين عن القسم المعلوماتي بإحدى الشركات الفرنسية بإعادة ملفات مستخدمين سابقين لهم حقوق مالية وقام بتحويلها إلى حسابه وحسابات أخرى ، ليتم بعد ذلك اختلاس أكثر من مليوني فرنك فرنسي[4].

---

[1] - ولا يشترط المشرع الفرنسي في المادة 3/323 اجتماع تلك الصور ، ولكن يكفي أن يصدر عن الجاني إحداها فقط لكي يتوفر الركن المادي لهذه الجريمة .

[2] – وفي حادثة أخرى قامت شركة أمريكية بلوس انجلوس باصطناع برنامج وهمي مخصص للغش المعلوماتي وبفضله اصطنعت وثائق وهمية لعدد من الأموات (64000) اقتصر دورها على إدارة الحسابات وقامت بتغيير عنوانهم وثائقهم لتبيعها بعد ذلك لأشخاص وحصلت مقابل ذلك على عمولات من شركات التامين التي تعمل لحسابها ، كما قام الجناة بوضع شفرة خاصة في البرنامج لا تظهر في الطباعة إلا الوثائق السليمة تماما ليتمكنوا بعد ذلك من الاستيلاء على مبلغ قدره 200مليون دولار من هذه العملية الوهمية . راجع عفيفي عفيفي كامل ، المرجع السابق ، ص .54 -55

[3] عبد القادر القهوجي ، مرجع سابق ، ص144.

[4] – محمد أمين الشوابكة، مرجع سابق ، ص 232.

- محو أو إزالة بيانات من الموقع:

يقصد بالمحو إزالة كل أو جزء من المعطيات الموجودة داخل النظام ، ويعتبر المحو جريمة إتلاف طالما وقع ثمة إتلاف الشيء بأي وسيلة [1]، فقد اعتبر المؤتمر الخامس عشر (15) للجمعية الدولية لقانون العقوبات المنعقد في البرازيل بتاريخ تشرين الأول 1994 بشأن جرائم الكمبيوتر في مقرراته وتوصيات أن الإدخال أو التعديل أو المحو يشكل جريمة تزوير ، كما اعتبر المحو للبرامج أو المعلومات جريمة إتلاف[2].

- تعديل بيانات مواقع التجارة الالكترونية:

يقصد بفعل التعديل تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى ويشكل التعديل الذي يقع علي المعطيات جريمة تزوير والتي تقوم على تغيير الحقيقة بقصد الغش يترتب عليه إلحاق ضرر بالغير.

ويلاحظ أن المشرع الفرنسي نص على جريمة التزوير وجريمة استعمال الوثائق المزورة في المادتين 5/462 و6/462 من قانون رقم 19/88 لسنة 1988 لكن تم إدراج مفهوم واسع للتزوير في المادة 1/441 من قانون العقوبات الجديد عام1994لاستيعاب التزوير المعلوماتي [3].

فالمشرع بذلك فصل بين التزوير في بيانات الحاسوب ، ومحررات الكترونية أخرى حيث أفرد للأولى نص خاص ، وشمل الثانية في النص العام للتزوير[4].

---

[1] - كما نصت اتفاقية بودابست في المادة 04 على ضرورة تجريم محو البيانات إذا حدث عمدا ودون وجه حق ، كما ، كما يشكل التعديل تزوير معلوماتي وفقا للمادة 07 من اتفاقية بودابست للجريمة المعلوماتية لسنة 2001..

[2] - عبد القادر القهوجي، مرجع سابق، ص144.

[3] - تنص المادة 1/441 من قانون العقوبات الفرنسي على أن التزوير هوكل تغيير للحقيقة بطريق الغش في محرر مكتوب أو في أي دعامة أخرى تحتوي تعبير عن الفكر .

[4] -عبد القادر القهوجي، مرجع سابق، ص149.

ويلاحظ أن المشرع الفرنسي في المادة 1/323 فقرة ثانية شدد العقوبة في حالة ماذا ترتب عن الدخول أو البقاء حذف أو تغيير للمعطيات [1].

ب-الركن المعنوي:

وهذه الجريمة عمدية تتطلب القصد الجنائي العام بعنصريه العلم والإرادة ، إذ يكفي أن تتجه إرادة الجاني إلى الاعتداء على بيانات المواقع بالإدخال أو التعديل أو المحو ، وأن يعلم بأن نشاطه ذلك يترتب عليه التلاعب في بيانات مواقع التجارة الالكترونية، ويعلم بأنه ليس له الحق في القيام بذلك [2].

ولكن لا يشترط لتوافر الركن المعنوي توافر القصد الجاني الخاص[3]، بل يتوافر بمجرد التلاعب بالمعطيات مع العلم بذلك واتجاه إرادته إلى ذلك [4].

وبالتالي فإنه إذا توافر القصد الجنائي العام بعنصريه العلم والإرادة إلى جانب الركن المادي تقع جريمة الاعتداء القصدي على المعطيات ويستحق مرتكبها العقوبة المقررة لها[5].

---

[1] – عبد القادر القهوجي، مرجع سابق، ص149.

[2] – شيماء عبد الغني عطاء الله ، مرجع سابق ، ص138. و عبد القادر القهوجي، مرجع سابق، ص145.

[3] – لم يشترط المشرع الجزائري في المادة 394 مكرر 1 توافر القصد الجنائي الخاص ، على غرار المشرع الفرنسي من خلال مصطلح الغش ، وفي المقابل اشترطت بعض التشريعات القصد خاص كالتشريع البرتغالي ، والتشريع الفنلندي .

[4] – كما نصت اتفاقية بودابست لسنة 2011 في المادة 04 على تجريم لاعتداء على بيانات الحاسوب ، إذا حدث ذلك عمدا ، وبالتالي تنتفي الجريمة إذا انتفى العمد

[5]– ومع ذلك عاقب التشريع الجزائري في المادة 394 مكرر فقرة 2 ، وكذا قانون العقوبات الفرنسي في المادة 1/323 ، على تعديل أو محو البيانات إذا تم ذلك بطريق الخطأ لكن كظرف مشدد للعقوبة وليس كجريمة خاصة مستقلة .

2 –جريمة التزوير المعلوماتي :

نص المشرع الفرنسي على هذه الجريمة في المادة 441 من قانون العقوبات الفرنسي، والتي تنص على أنه يعد تزوير كل تغيير بطريق الغش في مكتوب أو في أي دعامة أخرى تحتوي تعبيرا عن الفكر للحقيقة ، ولقيام هذه الجريمة لابد من توافر ركنين مادي ومعنوي، كالآتي:

أ–الركن المادي:

يتمثل الركن المادي لهذه الجريمة في تغيير الحقيقة في محرر الكتروني سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة أو كانت مرسومة عن طريق الراسم ويستوي في المحرر المعلوماتي أن يكون مدونا باللغة العربية أو لغة أخرى لها دلالتها ، كذلك قد يتم في مخرجات الكترونية محفوظة على دعامة كبرنامج منسوخ على أسطوانة [1]، ويشترط أن يكون المحرر الالكتروني أن يكون ذا أثر في إثبات حق أو أثر قانوني معين"[2].

وبالتالي وسع المشرع الفرنسي في محل التزوير، فبعد أن كان يقتصر على المحرر المكتوب امتد ليشمل أي محرر في أي دعامة أخرى تحتوي على الفكر[3] .

وعليه يشمل محل التزوير المعلوماتي كل المستندات المعلوماتية ، كالبرامج والمعلومات المسجلة على أقراص أو شرائط ممغنطة ، والبطاقات البنكية .

---

[1] – يرد التزوير المعلوماتي وثائق معلوماتية وهي تلك الوثائق التي يتم الحصول عليها بوسائل معلوماتية ، أي تكون ناشئة عن جهاز إلكتروني أو كهرومغناطيسي أو طبع ممغنط .

المبرمجة والوثائق المعلوماتية ، فالوثيقة المعلوماتية هي وثيقة لم تبرمج بعد.

[2] –عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص135 ا بعدها.

[3] – وهكذا يتضح أن التعديل الجديد أفضل من الوضع السابق الذي كان يقتصر فيه على تجريم تزوير المستندات المعالجة آليا في المادتين 462/5–462/6 من قانون العقوبات الملغى .

ولا يكفي جريمة التزوير المعلوماتي تغيير الحقيقة في محرر معلوماتي دون أن يترتب على ذلك أم أدبيا أم ، وسواء كان ينصب على المصلحة العامة أم على مصلحة شخص من الأشخاص وسواء كان ضرر واقع في الحال أو محتمل الوقوع .

ب-الركن المعنوي:

وهذه الجريمة من الجرائم العمدية ، يتطلب فيها القصد الجنائي العام بعنصريه العلم والإرادة حيث يجب أن يعلم الجاني بوقائع الجريمة وكونها من المحظورات ، ومع ذلك تتجه إرادته إلى الفعل المجرم ، بمعنى أن بأنه يرتكب فعل جرم أو سلوك غير مشروع معاقب عليه في التشريعات العقابية ومع ذلك أقدم على ارتكابه [1] .

كما ينتفي القصد الجنائي إذا أهمل المبرمج القائم بتحرير المحرر تغيير بيانات معينة دون قصد فالإهمال وعدم الاحتياط لا يحقق العلم في القصد الإجرامي .

وبالتالي لا يتصور وقوعها بطريق الخطأ، بل لابد من توافر القصد الجنائي بعنصريه العلم والإرادة لارتكاب جريمة التزوير [2].

و لايكفي هذا بل لابد من أن تكون إرادته متوجهة إلى إحداث النتيجة الإجرامية التي وقعت أو أية نتيجة إجرامية أخرى وهي الإضرار بالآخرين حتى وان كان هذا الإضرار محتمل الوقوع وعليه فان الركن المعنوي يتحقق في جريمة التزوير المعلوماتي .

---

[1] – الإجرامي وكذلك الحال إذا انتفى علم الجاني بأي ركن من أركان الجريمة فلا يترتب عليه توافر القصد الجنائي لأنه يفترض بالفاعل أن أركان جريمته كما قد لا يتحقق القصد الجنائي إذا كان الفعل الذي يقوم به الجاني غير واضح بصورة صريحة كما هو الحال بالنسبة لانتحال صفة الغير أو الاتصاف بصفة غير صحيحة فقد يقوم مبرمج بيانات بتغيير الحقيقة في المحررات .

[2] – عبد القادر القهوجي، مرجع سابق، ص152.

بالإضافة إلى القصد الجنائي العام، يتطلب القانون القصد الجنائي الخاص ، والذي يتمثل في اتجاه نية الجاني إلى استعمال المستند المزور فيما زور من اجله ، حتى ولو لم يستعمل هذا المستند فعلا [1].

ثانيا- جرائم الاعتداء على بيانات المواقع في التشريعات العربية:

لقد تناولت بعض التشريعات العربية حماية بيانات مواقع التجارة الالكترونية، من أبرزها التشريع الجزائري والتونسي، فيما خلا التشريع المصري من حمايتها.

1-جرائم الاعتداء على بيانات المواقع في التشريع الجزائري:

نص المشرع الجزائري على هذه الجرائم في المادتين 394 مكرر1، و394 مكرر2، وتمثلت في جريمة التلاعب بالمعطيات، والتعامل بمعطيات غير مشروعة ، على التفصيل الآتي :

أ-جريمة التلاعب في المعطيات :

نص عليها المشرع الجزائري في المادة 394 مكرر1 ، وعاقب عليها بالحبس من6 أشهر الى3 سنوات وبغرامة من500.000 د ج الى200.0000 دج كل من دخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها [2].

وحتى تقوم هذه الجريمة يجب أن يتوفر ركنيها المادي والمعنوي ، على التفصيل الآتي :

---

[1] - المرجع نفسه ، ص 152

[2] - ويقصد بالتلاعب بالبيانات إدخال بيانات غير مصرح بها أو تعديل بيانات موجودة أو إلغاء بيانات موجودة بالنظام ، و هي تتعلق بمعطيات النظام ، على خلاف جريمة الإخلال بسير النظام المتعلقة بالنظام ذاته.

-الركن المادي:

يتمثل الركن المادي لهذه الجريمة بالتلاعب ببيانات المواقع عن طريق الإدخال أو الإزالة أو التغيير، وهي نفسها الجرائم التي جاء بها المشرع الفرنسي[1]، ولا يشترط اجتماع تلك الصور ولكن يكفي توافر إحداها لقيام الجريمة .

ويتحقق الإدخال بإضافة معطيات جديدة إلى النظام[2]، أما المحو فيتحقق بإزالة جزء من معطيات النظام المعلوماتي بخلاف التعديل الذي يتحقق بتغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى[3].

لقد وردت الأفعال السابقة على سبيل الحصر، فهذه الجريمة لا تتحقق بغيرها، فحتى و ولو وقع اعتداء على معطيات المواقع، فلا يخضع لنص جريمة التلاعب، لأنها تتحقق بإدخال ومحو وتغيير المعطيات.

-الركن المعنوي :

يتمثل الركن المعنوي لهذه الجريمة في القصد الجنائي العام ، ولا يشترط توافر القصد الجاني الخاص [1]، إذ يكفي أن تتجه إرادة الجاني إلى الاعتداء على المعطيات بالإدخال أو التعديل أو المحو، وأن يعلم بأن نشاطه ذلك يترتب عليه التلاعب في المعطيات[2].

---

[1] – عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني :الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص 46 وما بعدها.

انظر أيضا شيماء عطاء الله ، مرجع سابق ، ص136. مدحت عبد الحليم رمضان، مرجع سابق، ص52. عبد القادر القهوجي، مرجع سابق ، ص143-144 .

[2] – ومن التطبيقات القضائية على هذه الصورة ماقامت به متهمة كانت تعمل في إحدى الشركات قبل تركها العمل بإدخال بيانات غير صحيحة تتعلق بمعدل احتساب الضريبة على القيم المنقولة.

[3] – عبد القادر القهوجي ، مرجع سابق ، ص144 .

وبالتالي فإنه إذا توافر القصد الجنائي العام بعنصريه العلم والإرادة إلى جانب الركن المادي تقع جريمة الاعتداء القصدي على المعطيات ويستحق مرتكب الجريمة العقوبة المقررة لها[3].

ويلاحظ أن المشرع الجزائري في المادة 394 مكرر فقرة 2 شدد العقوبة إذا ترتب على الدخول أو البقاء حذف أو تغيير معطيات المنظومة، ولا يشترط في هذه الصورة القصد الجنائي على خلاف جريمة التلاعب بالمعطيات الواردة في المادة 394 مكرر 1 [4].

ب- جريمة التعامل في معطيات غير مشروعة:

نظم المشرع الجزائري على جريمة التعامل في معطيات غير مشروعة في المادة 394 مكرر2 من قانون العقوبات، والتي عاقبت كل من يقوم عمدا وعن طريق الغش بالأفعال التالية:

- تصميم أو بحث أو تجميع أو توفير أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها جرائم هذا القسم.

-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كانت المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم .

ولقيام هذه الجريمة لابد من توافر ركنين، أحدهما مادي، والأخر معنوي.على التفصيل الآتي :

---

[1] - لم يشترط المشرع الجزائري في المادة 394 مكرر1 توافر القصد الجنائي الخاص ، وهو ما ذهب إليه المشرع الفرنسي بموجب المادة 3/323 الذي اكتفى بالقصد الجنائي العام من خلال مصطلح الغش ، وفي المقابل اتجهت بعض التشريعات إلى اشترط قصد خاص كالتشريع البرتغالي ، والتشريع الفلندي .

[2] - شيماء عبد الغني عطاء الله ، مرجع سابق ، ص138. و عبد القادر القهوجي، مرجع سابق، ص145.

[3]- ومع ذلك فقانون العقوبات الفرنسي يعاقب على تعديل أو محو البيانات إذا تم ذلك بطريق الخطأ وفقا للمادة 1/323 وكذلك التشريع الجزائري بموجب المادة 394 مكرر فقرة 2 .

[4] - راجع المادة 394 مكرر فقرة 2 من قانون العقوبات الجزائري .

-الركن المادي:

يتكون الركن المادي في هذه الجريمة من نشاط إجرامي يأخذ صورتين هما : التعامل في معطيات صالحة لارتكاب جريمة معلوماتية ، أوالتعامل في معطيات متحصلة من إحدى الجرائم المعلوماتية المنصوص عليها [1].

جريمة التعامل في معطيات غير مشروعة جريمة شكلية لايعتد فيه المشرع في قيامها بتحقق بأحد الأفعال التي نصت عليها المادة 394 مكرر02 حتى تقوم الجريمة[2] .

***التعامل في معطيات صالحة لارتكاب جريمة:**

يتحقق هذا السلوك الإجرامي بالقيام بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم [3].

---

[1] - وبالتالي كل معطيات غير مشروعة ، سواء كانت صالحة لارتكاب جريمة أو كانت متحصلة من جريمة قامت المادة 394 مكرر02 بتجريم التعامل فيها ، سعيا لمنع وقو ع الجريمة أو للتخفيف من آثارها، وبالتالي لم يكتف المشرع بتجريم التعامل في المعطيات صالحة لارتكاب جريمة ، فالغاية من تجريم هذه الأفعال هي وقائية لأن هذه الجريمة جرائم خطر يهدف المشرع من خلال تجريمها إلى منع وقوع الضرر. راجع محمد خليفة ، الحماية الجنائية لمعطيات الحاسوب في القانون الجزائري والقانون المقارن ، دار الجامعة الجديدة، الإسكندرية مصر 2007، ص209.

[2] - من خلال المادة 394 مكرر02 يتبين لنا أن محل هذه الجريمة يتمثل في معطيات معالجة ، أو مخزنة او مرسلة عن طريق منظوم معلوماتية ، وبالتالي لم يقصر المشرع هذه الجريمة على المعطيات المعالجة بهدف أن تشمل كل المعطيات الصالحة لارتكاب جريمة ن وتوسع المشرع الفرنسي أكثر من ذلك في المادة 1/3/323 ،عندما اقر بأن التعاملات المجرمة يمكن أن تقع على التجهيزات والأدوات أو على برنامج معلوماتي أو معلومات مصممة او معدة لارتكاب جريمة من جرائم المساس بالمعطيات . للتفصيل راجع خليفة محمد ، مرجع سابق، 197.

[3] - محمد خليفة ، مرجع سابق ، ص209.

و برامج

اختراق ، أما التوفير فيعني الوضع تحت التصرف وجعلها في متناول الغير ، والنشر هو إذاعة المعطيات وتمكين الغير من الاطلاع عليها ، أما الاتجار هو تقديمها للغير بمقابل نقدي أم عيني .[1]

ويهدف المشرع من خلال تجريمه للتعامل في معطيات صالحة لارتكاب جريمة إلى منع حدوث هذه الجريمة قبل وقوعها، فالغاية إذا هي وقائية ، لأن هذه الجرائم هي جرائم خطر يهدف المشرع من خلال تجريمها إلى منع وقوع الضرر[2].

*** التعامل في معطيات متحصلة من جريمة :**

يقوم الركن المادي لهذه الجريمة بالحيازة أو الإفشاء أو النشر أو الاستقبال لأي غرض كان للمعطيات المتحصل عليها من إحدى هذه الجرائم المعلوماتية.

الحيازة: وتتحقق الحيازة بسيطرة الحائز على المعطيات سيطرة مطلقة ، بحيث يقدر على محوها أو تعديلها أو استعمالها، وقد تكون محدودة باستغلالها فيوجه معين[3].

ولا تكفي سيطرة الجاني على المعطيات حتى تقوم جريمة الحيازة، بل لابد أن تكون السيطرة إرادية، أي مقترنة بنية احتباسها على الدوام أو لمدة معينة[4].

---

[1] – المرجع نفسه، ص 200 وما بعدها.

[2] – المرجع نفسه ، ص195.

[3] – محمد زكي أبو عامر قانون العقوبات، القسم الخاص، دار الجامعة الجديدة، الإسكندرية مصر، 2005، ص762.

[4] – ف تعديل كيانه أو تحطيمه أو نقله ، فهي إذا سيطرة إرادية للشخص على الشيء.

الإفشاء: بخلاف المشرع الجزائري لم يجرم المشرع الفرنسي إفشاء البيانات المتحصلة من جرائم هذا القسم ، لكنه جرم إفشاء البيانات الاسمية في المادة 22/226 من قانون نظم المعالجة الرقمية والحرية الصادر في 6 يناير 1978 [1].

ولا يتطلب المشرع الجزائري حدوث نتيجة معينة من جراء الإفشاء، ويختلف الإفشاء عن الحيازة في أن هذه الأخير تقوم الجريمة دون تقديمها للغير على خلاف الإفشاء فهو يفترض انتقال المعطيات المتحصلة من جريمة ، من حيازة شخص إلى شخص آخر.

النشر: يتحقق النشر بإذاعة البيانات الشخصية واطلاع الغير عليها مهما كانت وسيلة النشر, وسواء تم النشر بقابل أم بدون مقابل[2].

الاستعمال: ويتحقق باستخدام المعطيات المتحصلة من الجرائم المعلوماتية ، لأي غرض كان، أي مهما كان الهدف منه وفقا للمادة 2/394، كاستعمال كلمة العبور للحصول على معطيات ومعلومات أخرى[3].

-الركن المعنوي:

إن جريمة التعامل في معطيات متحصلة من الجرائم المنصوص عليها في هذا القانون من الجرائم العمدية [4]، ويأخذ الركن المعنوي صورة القصد الجنائي العام بعنصريه العلم والإرادة.

---

[1] – طبقا للمادة 22/226 يتحقق الإفشاء غير المشروع للبيانات الاسمية بتوفر الشروط الآتية :

– حيازة بيانات اسمية وأن يكون من شأن الإفشاء الإضرار بصاحب البيانات.

– أن يتم الإفشاء دون رضا صاحب البيانات، ذلك أن هذا الرضا يكون سببا لإباحة فعل الإفشاء .

– إفشاء هذه البيانات للغير الذي لا يكون له الحق في الإطلاع عليها.

[2] – محمد خليفة، مرجع سابق، ص109.

[3] – المرجع نفسه ، ص110.

[4] – وهوما يستفاد من نص المادة 394 مكرر2 من خلال عبارة كل من يقوم عمدا وعن طريق الغش .

فيتعين أن يكون الجاني عالما بأنه يقوم بالتعامل في معطيات غير مشروعة سواء كانت معدة لارتكاب جريمة ، أو معطيات متحصلة من الجرائم المعلوماتية المنصوص عليها في هذا القسم ، ويتعين كذلك أن تتجه إرادته نحو التعامل بالمعطيات غير المشروعة [1] .

ولا يشترط توافر القصد الجاني الخاص ، بل يكفي توافر القصد الجنائي العام إلى جانب الركن المادي حتى تقع هذه الجريمة ، ويستحق مرتكبها العقوبات المقررة لهذه الجريمة [2].

وتتطلب اتفاقية بودابست إلى جانب القصد الجنائي العام قصدا خاصا لقيام هذه الجريمة يتمثل في التعامل في الجهاز أو الوسائل محل الجريمة ، بنية استخدامها في ارتكاب جريمة.

2- جرائم الاعتداء على بيانات المواقع في التشريع التونسي :

يمكن أن تطال الاعتداءات ليس النظام المعلوماتي فقط بل البيانات التي يحتويها، وهنا تشتد خطورة مثل هذه الأفعال، ولقد جرم المشرع التونسي أفعال الاعتداء على بيانات النظام في الفصل 199 مكرر وتمثلت في جريمة الاعتداء القصدي على البيانات المعلوماتية ، والاعتداء غير القصدي ، وجريمة التدليس (التزوير) ، كالآتي :

أ-الاعتداء غير القصدي على بيانات المواقع:

اقتضى الفصل 199 مكرر في فقرته الثانية أنه "ترفع العقوبة إلى عامين سجن والخطية إلى ألفي دينار إذا نتج عن ذلك ولو عن غير قصد إفساد أو تدمير البيانات الموجودة بالنظام ".

ويعتبر تدمير أو إفساد البيانات في هذه الصورة كظرف تشديد لجريمة النفاذ أو البقاء بصفة غير شرعية، متى ثبتت العلاقة السببية بين هذا الدخول غير الشرعي لنظام المعالجة المعلوماتية والإضرار بالبيانات الموجودة به[1].

---

[1] – محمد خليفة، مرجع سابق، ص111-112.

[2] – ولا يتطلب القانون الفرنسي في المادة 1/3/323 من قانون العقوبات قصد خاصا. للتفصيل راجع خليفة محمد مرجع سابق ، ص115-116.

وما يلاحظ أن المشرع التونسي استعمل عبارات الإفساد والتدمير ، في حين استخدم المشرع الفرنسي والمشرع الجزائري استعملا عبارتي الحذف "Suppression" والتغيير "Modification" وعبارة الإفساد التي استعملها المشرع التونسي لها مدلول أوسع من التغيير باعتبار أن الإفساد يعني جعل الشيء غير قادر على أداء وظيفته بصورة طبيعية، أما التدمير فيعني حذف البيانات[2] .

ولا يشترط القصد الجنائي في جريمة إفساد أو تدمير البيانات لأن المشرع استخدم عبارة "ولو عن غير قصد" بالفصل 199 مكرر فقرة ثانية من المجلة الجزائية للدلالة على ذلك، فالمهم في هذه الحالة هو النتيجة لا القصد لإحداث تلك النتيجة، وطالما أن القصد الجنائي كان متوفرا في جريمة النفاذ أو البقاء بصفة غير شرعية بالنظام المعلوماتي الذي ترتب عنه الضرر اللاحق بالبيانات[3].

وفي هذا الإطار أصدرت المحكمة الابتدائية "Nanterre"حكما ابتدائيا بتاريخ 10 فيفري 2006[4] ، أدانت فيه المتهم " Hugues.B " من أجل حذف وتغيير البيانات نتيجة دخول غير شرعي لنظام المعالجة الالكترونية لشركة ".BCA " دون الخوض في وجود تعمد لتحقيق هذه النتيجة من عدمه.

---

[1] – كما نص المشرع الجزائري على هذا الظرف المشدد في المادة 394 مكرر فقرة 2 في حالة ما إذا ترتب على الدخول أو البقاء حذف أو تغيير معطيات المنظومة، بينما نص المشرع التونسي على وليس الاعتداء غير القصدي على بيانات المواقع بالإفساد والتدمير .

[2]– عماد بوخريص وحسني غديره ، جرائم الإعلامية ، ملتقى بمحكمة الاستئناف بسوسة 2 جوان 2001، ص 20.

[3] – كما أن المشرع الفرنسي لم يتعرض للقصد الجنائي في الفقرة الثانية للفصل 323–1 من قانون العقوبات، التي تقابل الفقرة الثانية من الفصل 199 مكرر من المجلة الجزائية التونسية،

[2]-Tribunal de grande instance de Nanterre 15ème chambre jugement du 10 février 2006 Fontaine sur w.w.w.authsecu.com

أما في حالة توفر النية لإحداث الضرر فإن الفعل يقع تحت طائلة جريمة الاعتداء القصدي على بيانات نظام المعالجة المعلوماتية[1] .

ب- الاعتداء القصدي على بيانات المواقع :

اقتضى الفصل 199 مكرر فقرة 4 أنه "يعاقب بالسجن مدة خمسة أعوام وخطية قدرها خمسة آلاف دينارا من يدخل بصفة غير شرعية بيانات بنظام معالجة معلوماتية من شأنه إفساد البيانات التي يحتوي عليها البرنامج أو طريقة تحليلها أو تحويلها، وتضاعف العقوبة إذا ارتكبت بمناسبة مباشرته لنشاطه المهني. والمحاولة موجبة للعقاب". يتبين من خلال هذا الفصل أن المشرع شدد العقاب إذا تم الاعتداء على البيانات التي يحتويها النظام المعلوماتي، نظرا لأهمية هذه البيانات الإلكترونية.

وقد اتخذ المشرع الفرنسي نفس الموقف حين عاقب على إدخال بيانات أو محو أو تعديل بيانات بنظام المعالجة الآلية التي خمس سنوات وبالخطية بـ75.000 أورو حسب منطوق الفصل 323-3 من ق ع ف[2].

فالجريمة إذا تقع على البيانات التي تمت معالجتها آليا، بذلك يخرج من نطاق البيانات التي انفصلت عن النظام وسجلت على وعاء خارجي قرص مدمج فالحماية الجزائية المقررة بالفصل 199 مكرر تتعلق بالمعطيات الموجودة بالنظام المعلوماتي لا البيانات الالكترونية في مجملها[3].

---

[3]- Gassin ®, article précité, p. 34 .

1-Art.323-3 : Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. Code pénal partie législative liée à la sécurité informatiqu par Sébastien Fontaine sur www.authsecu. com.

[3] – وقد طرح على القضاء الفرنسي إشكال بالنسبة للبيانات المبرمجة التي سيقع معالجتها، واعتبرها تخضع لمقتضيات المادة 3/323 من ق ع ف المقابل للفصل 199 مكررف4 من المجلة الجزائية التونسية .

ويتكون السلوك الإجرامي في هذه الجريمة من إدخال بيانات جديدة للنظام المعلوماتي ، من شأنها إفساد البيانات الأصلية أو طريقة تحليلها أو تحويلها[1].

وما يلاحظ أن المشرع التونسي قد جرم إفساد البيانات عبر إدخال بيانات جديدة للنظام المعلوماتي ، في حين أن الإفساد يمكن أن ينتج أيضا على استعمال طرق أخرى مثل حذف البيانات أو تغييرها ، وهو ما أشار له المشرع الفرنسي بالفصل 3/323 من ق ع ف ، الذي اقتضى أنه "إدخال بيانات بصفة غير شرعية في نظام المعالجة الآلية أو تعديل البيانات الموجودة به أو حذفها يعاقب عليه بالسجن لمدة خمس سنوات وبالخطية بمبلغ 75.000 أورو".

ولا يكفي إدخال بيانات بصفة غير شرعية لقيام هذه الجريمة ، ولابد أن ينتج عن الإدخال إفساد البيانات أو طريقة تحليلها أو تحويلها، فالمشرع ربط بين فعل الإدخال والنتيجة المتمثلة في إفساد البيانات، وبالتالي لا تقوم الجريمة إذا لم ينتج عنه أي أثر ، لكن يعاقب على الشروع إذا لم ينجح في إفساد البيانات[2].

وبالنظر للطبيعة المعقدة لهذه الجريمة فإنه غالبا ما يرتكبها الفنيين الذين لهم إلمام واسع بالمعلوماتية، وفي أغلب الأحيان بمناسبة مباشرتهم لنشاطهم المهني وتضاعف العقوبة إذا ارتكبها شخص بمناسبة مباشرته لنشاطه المهني[3].

---

[1] – وفعل الإدخال يتم إما بصورة مباشرة وذلك بالتواصل بين الفاعل وأجهزة الإعلامية إذا كان من العاملين بالنظام المعلوماتي، كما يمكن أن يكون النفاذ عن بعد عبر شبكة الانترنت ، ويكفي الحصول على كلمة السر أو مفتاح الدخول للولوج لهذه الأنظمة والعبث بالبيانات التي تحتويها.

[2] –عماد بوخريص وحسني غديره، مرجع سابق، ص 23.

[3] – حسب الفقرة الخامسة من الفصل 199 مكرر من المجلة الجزائية التونسية، إذا ارتكب هذه الأفعال شخص بمناسبة مباشرته لنشاطه المهني ، تضاعف العقوبة إلى عشرة أعوام والخطية عشرة آلاف دينار .

ج- جريمة التدليس الالكتروني(التزوير الالكتروني):

تعد هذه الجريمة من أخطر صور الغش المعلوماتي ، نظرا للدور الكبير للوثيقة الالكترونية واتساع مجالات استعمالها، لذلك كان التدخل التشريعي لتجريم تزويرها ذا أهمية بالغة ، خاصة وأن هذه الأخيرة أصبحت لها قيمة المحررات الورقية ووسيلة لإثبات الالتزامات والحقوق[1].

يقتضي قيام جريمة التدليس الالكتروني توفر ركنين مادي، ومعنوي ، كالآتي:

-الركن المادي :

انطلاقا من الفصلين 17و199 ثالثا من المجلة الجزائية يتضح أنه يستوجب لقيام جريمة التزوير تغيير الحقيقة في محرر إلكتروني ، وفق طرق معينة بشكل من شأنه إحداث ضرر بالغير[2].

*** تغيير الحقيقة :**

اشترط المشرع التونسي هذا التغيير لقيام جريمة التزوير سواء في الفصل 172 أو الفصل 199

التزوير لكون تغيير الحقيقة جوهر التزوير[3].

وقد عرف المشرع الفرنسي التزوير بأنه تغيير متعمد للحقيقة[4]، ولا يشترط أن يكون التغيير في كل بيانات الوثيقة، ويكفي أن يكون التغيير جزئيا.

---

[1]- عماد بوخريص وحسني غديره، مرجع سابق، ص 22.

[2] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر الإنترنت، مرجع سابق، ص145.

[3] - والمقصود بتغيير الحقيقة هو تغيير الحقيقة النسبية وليس بتغيير الحقيقة الواقعية المطلقة، أما الحقيقة فيقصد بها ما يتعين إثباته في الوثيقة الإلكترونية وفقا لقرينة يقررها القانون.

[4] -L'art 441-1du code pénal Français : constitue un faux toute altération Frauduleuse de la vérité.

والتغيير الواقع على الوثيقة الإلكترونية يلحق مضمونها أو شكلها ، دون أن يعدمها أو يتلفها، وينصب على الحقوق أو المراكز القانونية للغير التي تثبتها الوثيقة الإلكترونية، فتجعلها غير مطابقة للواقع[1].

ويجمع الفقه القضاء على أن تغيير الحقيقة في الوثيقة حتى يعد تزويرا يجب أن يقع على البيانات الجوهرية للوثيقة ، والبيانات الجوهرية هي التي أعدت لإثبات الوثيقة الالكترونية ، أي من شأنها إثبات حق أوصفة أو حالة قانونية[2].

***محل التدليس:**

يحدد الفصلين172و199 ثالثا من المجلة الجزائية محل جريمة التدليس الإلكتروني، وهو الوثائق الإلكترونية، التي تشمل البيانات داخل النظام وكذلك البيانات التي لم تعد موجودة بالنظام الموجودة في الأوعية المادية ، إلا أن هناك اختلاف بين النصين فالفصل 172 أشار إلى تغيير الحقيقة في كل وثيقة الكترونية أو معلوماتية مثبتة لحق أو واقعة منتجة لآثار قانونية، في حين لم يشترط الفصل 199 في الوثيقة الالكترونية أن تكون الوثيقة الإلكترونية ذات قيمة إثباتيه[3].

رفها في إطار
مجلة الالتزامات والعقود، في الفصل 453 مكرر بموجب القانون عدد 57 لسنة 2000 المؤرخ في 13 جوان 2000، بأنها وثيقة متكونة من مجموعة أحرف وأرقام أو إشارات رقمية أخري بما في

---

[1]–عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر الإنترنت، مرجع سابق، ص 151.

[2] – المرجع نفسه ، ص 137.

3 – اقتضى الفصل 172 في المجلة الجزائية أنه يعاقب بالسجن بقية العمر وبخطية قدرها ألف دينار كل موظف عمومي أو شبهه وكل عدل يرتب في مباشرة وظيفة زورا من شأنه إحداث ضرر عام أو خاص، وذلك بصنع وثيقة مكذوبة أو تغيير متعمد للحقيقة ، بأي وسيلة كانت في كل سند سواء كان ماديا أو غير مادي من وثيقة معلوماتية أو إلكترونية وميكروفيلم وميكروفيش، ويكون موضوعه إثبات حق أو واقعة منتجة لأثار قانونية.

كما اقتضى الفصل 199 ثالثا أنه يعاقب بالسجن مدة عامين وبخطية قدرها ألفي دينار كل من يدخل تغييرا بأي شكل كان على محتوى وثائق معلوماتية أو إلكترونية أصلها صحيح شريطة حصول ضرر للغير".

ذلك تلك المتبادلة عبر وسائل الاتصال ذات محتوى يمكن فهمه ومحفوظة على حامل إلكتروني يؤمن قراءتها والرجوع إليها عند الحاجة"، كما أصبح يعطي لها حجية المحررات الورقية بموجب المادة 453 مكرر فقرة 2[1].

* **طرق التزوير** : للتزوير طرق مادية وطرق معنوية ، على التفصيل الآتي:

الطرق المادية للتزوير :

بالنظر للفصول 172 و 199 ثالثا من المجلة الجزائية ، يتضح لنا أن طرق التزوير المادي تتمثل في صنع وثيقة مكذوبة أو تغيير مضمون وثيقة أصلية، على التفصيل الآتي :

- **صنع وثيقة الكترونية مكذوبة** :

أشار المشرع التونسي بالفصل 172 من المجلة الجزائية لأحد طرق التزوير المادي وهي "صنع وثيقة مكذوبة"، والصنع يت[2].

ووقوع تزوير الوثيقة الالكترونية بطريق الصنع ممكن إذ بإمكان الجاني أن يدخل ما يريد من معلومات أو بيانات إلى جهاز الحاسوب وينسب صدورها إلى شخص ما ، ثم يقوم باستخراجها من ذلك الجهاز بوصفها منسوبة لذلك الشخص تتم هذه العملية من خلال المسح الضوئي (Scénarisation)، أو عن طريق لوحة المفاتيح أو حتى عن طريق استدعاء المعلومات من

---

[1] – حيث اقتضى الفصل 453 مكرر في فقرته الثانية "تعد الوثيقة كتبا غير رسمي إذا كانت محفوظة في شكلها النهائي بطريقة موثوق بها ومدعمة بإمضاء إلكتروني".

[2] – ويختلف الاصطناع أو الصنع عن التقليد باعتبار أنه في الصنع لا يهم الجاني مدى التشابه بين خطة وخط الغير، ذلك أنه يصنع محرر جديدا بأكمله، بينما ا

منه قيمته القانونية.

شبكة الانترنت ثم صياغتها في شكل المحرر المزور[1] ، وأكثر الميادين التي تشهد تزوير الوثائق الالكترونية بالاصطناع ، ميدان المعاملات البنكية وبالتحديد البطاقات البنكية [2].

-تغيير محتوى الوثيقة الالكترونية:

يتحقق التزوير في الوثيقة الإلكترونية بتغيير محتواها حسب الفصل 172 في فقرته الثانية والفصل 199 ثالثا من المجلة الجزائية ، والتغيير قد يكون بالإضافة أو الحذف أو التعديل، والتغيير بالإضافة قد يتم بزيادة حرف أو كلمة أو رقم يؤدي إلى تغيير مضمون الوثيقة المعلوماتية، أما التغيير بالحذف فيكون بحذف كلمة أو رقم أو اسم أو عبارة وردت بالوثيقة المعلوماتية، أيا كانت الوسيلة المستعملة في ذلك، سواء كان بالشطب أو استعمال الممحاة الالكترونية، أما التغيير بطريقة التعديل فهو يجمع بين طريقتي الحذف والإضافة كأن يقع استبدال رقم بآخر أو حذف اسم وتعويضه بآخر[3].

وفي هذا الإطار أصدرت المحكمة الابتدائية بتونس حكما جزائيا بتاريخ 2005/03/26 قضت فيه بإدانة المتهمين من أجل تدليس وثيقة إلكترونية قاما بتحويل أموال وهمية لحساباتهما ولحساب المتواطئين معهم [4]، وقد ذهبت محكمة الاستئناف بتونس في نفس الاتجاه ، واعتبرت الأفعال المذكورة من قبيل التدليس الالكتروني في قرارها الصادر في15 ديسمبر2005 [5] .

---

[1]- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 202

3-Didier (j) « Les Truquages et usages Frauduleux des cartes magnétiques JCP.éd.G.I 1986, 3229 .

[3]– عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 187.

[4] – وتمثلت وقائع هذه القضية في قيام متهمين يعملان كموظفين ببنك الأمان بعمليات تحويل وهمية للأموال لحساباتهم الشخصية ولحسابات بعض المتواطئين معهم ، والإيهام أن هذه التحويلات للأموال يقابلها إيداع لصكوك بنكية، واعتبرت المحكمة الابتدائية ذلك من قبيل جريمة التدليس.

90 – وتتلخص وقائعها في قيام المتهمين باستعمال حساب الربط لتنزيل عمليات صكوك بنكية في شكل إيداعات لتلك الصكوك مسحوبة على نفس الفرع وهي عمليات غير قانونية استعملت في مقابلها حساب الربط وذلك للتضليل ، مما انجر عنه ضرر للبنك وصل إلى مليارين دينار ، مما يشكل جريمة التدليس .

-التغيير بوضع طابع أو إمضاء مدلس :

يتم ذلك بإضافة طابع أو إمضاء لشخص معين لوثيقة الكترونية ، وبالتالي نسبة هذا المحرر المزور لذلك الشخص بالرغم من أنه لم يصدر عنه، وبفضل تطور الأجهزة المرتبطة بالحاسوب يمكن نقل مختلف التوقيعات والأختام والصور إلى ذاكرة الجهاز والاحتفاظ بها عن طريق استخدام جهاز الماسح الضوئي، ومن ثمة يمكن إضافة هذا التوقيع أو الختم إلى أي ورقة يتم تغييرها أو تضمين بيانات فيها تخدم مصلحة الجاني، بحيث يتم الحصول على مستند صحيح من الناحية الشكلية إلا أنه مزور باعتبار أنه نسب إلى شخص بعد أن حمل إمضاءه أو ختمه على غير إرادته.

ب- الطرق المعنوية للتزوير :

اقتضى الفصل 172 في فقرته الثالثة أن تدليس كل سند سواء كان ماديا أو غير مادي يكون بصنع وثيقة مكذوبة أو تغيير متعمد للحقيقة بأي وسيلة كانت، بالتالي لم يحصر المشرع التونسي الوسائل التي يتم بها التزوير المعلوماتي وجاءت العبارات عامة ، بحيث يمكن أن تشمل طرق التزوير المادي أو المعنوي[1].

والطبيعة اللامادية للوثيقة الالكترونية ترجح إمكانية أن ترد طرق التزوير المعنوي عليها ، كأن

.[2]

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

[2]– ويبدو من هذه الناحية أن التزوير المعنوي يتشابه مع التزوير في الوثيقة الالكترونية عن طريق صنع وثيقة مكذوبة بما تقتضيه هذه الطريقة الأ

وثيقة الكترونية مصطنعة .

***الضرر :**

إضافة إلى تغيير الحقيقة في محرر ما، يقتضي قيام الركن المادي في جريمة التدليس إحداث ضرر حسب الفصلين 172 و199 ثالثا.

وقد انقسم الفقه فيما يتعلق بمفهوم الضرر في التزوير المعلوماتي بين موقف يرى أن الضرر لا يتوفر في التزوير المعلوماتي إلا إذ وقع التدليس على وثيقة الكترونية ذات أثر قانوني، أما الموقف الثاني يرى أن الضرر في التزوير المعلوماتي يرتبط واقعيا بالخسارة الناتجة عن التزوير ، ولا يرتبط بالبعد القانوني للوثيقة الالكترونية[1]، وهو الاتجاه الذي انتهجه المشرع التونسي باعتبار أنه لم بالنظر لأحكام الفصل 199

ثالثا م.ج.

والضرر يمكن أن يكون عاما أو خاصا، والضرر العام هو الذي يمس مصلحة جماعية تتمثل في المساس بالثقة العامة[2]، كما يمكن أن يكون الضرر عاما في صورة المساس بأموال الدولة بجعل الخزينة العامة مدينة أو تفويت حق أو كسب يعود لها قانونا، ومثال ذلك أن يقوم موظف عمومي بتغيير البيانات بوثيقة معلوماتية لإخفاء المبالغ التي اختلسها من الجهة الحكومية التي يعمل بها.

أما الضرر الخاص فهو الذي يصيب شخصا أو هيئة معينة، أي يمكن أن يقع على شخص طبيعي أو معنوي.

---

[1] -Gassin(R) article précité p.53.

[2] – كما يمكن أن يكون الضرر عاما في صورة المساس بأموال الدولة بجعل الخزينة العامة مدينة أو تفويت حق أو كسب يعود لها قانونا، ومثال ذلك أن يقوم موظف عمومي بتغيير البيانات بوثيقة معلوماتية لإخفاء المبالغ التي اختلسها من الجهة الحكومية التي يعمل بها.

وتجدر الإشارة إلى أن الفقه اختلف حول طبيعة هذا العنصر،هل هو شرط في جرائم التدليس أو ركن ؟ ، هذا وقد اعتبرت محكمة التعقيب التونسية في قرارها الصادر في 15 ماي 1991 أن الضرر ركن مستقل قائم بذاته في جريمة التدليس الالكتروني[1].

- الركن المعنوي :

جريمة تزوير الوثيقة الالكترونية هي من الجرائم العمدية ، يقتضي قيامها توفر القصد الجنائي العام ، والذي يتمثل في انصراف إرادة الجاني إلى القيام بفعل التزوير رغم علمه بمخالفته للقانون ، ولابد أيضا من توفر قصد جنائي خاص .

وقد اختلفت الآراء في تحديد المقصود من القصد الجنائي الخاص، ويذهب اتجاه إلى اعتبار أن القصد الجنائي الخاص في جرائم التزوير بصفة عامة يتمثل في نية الأضرار بالغير أي اتجاه إرادة الجاني إلى إلحاق ضرر بالمستهدف من التدليس، إلا أن هذا الرأي يقابله رأي آخر يعتبر أن القصد الجنائي الخاص في جريمة التدليس يتمثل في نية الغش ، أي نية التحصيل على منفعة غير مشروعة بطريق تغيير الحقيقة في سندها سواء كان ماديا أو الكترونيا، والمنفعة يمكن أن تعود للشخص القائم بالتغيير أو للغير، وتحقيق المنفعة يكون بالاحتجاج بالسند المزور اعتداءا على حق يحميه القانون.

وقد عرفت محكمة التعقيب الركن المعنوي لجريمة التدليس بأنه قصد الجاني عن سوء نية تغيير الحقيقة في أمر جوهري بنية الإضرار بالمدلس عنه [2].

أقر المشرع التونسي لجريمة التدليس الإلكتروني بموجب الفصل 199/ 3 عقوبات أصلية تمثلت في السجن مدة عامين وبخطية(غرامة) قدرها ألفا دينار، على كل من يدخل تغيير على

---

[1] – إذ جاء في قرارها الصادر في 15 ماي 1991 "من المسلم به فقها وقانونا أن جريمة الزور بنوعيها المادي والمعنوي لا تقوم إلا بتوفر أركان ثلاثة وهي : تغيير الحقيقة بإحدى الطرق المنصوص عليها بالقانون وحصول القصد الجنائي وحصول الضرر للغير ماديا كان أو معنويا".

[2] – قرار تعقيبي جزائي عدد 2809 مؤرخ في 18 جويلية 1979، ن.م.ت، قسم جزائي لسنة 1979، ص 195.

محتوى وثائق معلوماتية أصلها صحيح، ويضاعف العقاب إذا ارتكبت الأفعال المذكورة من موظف عمومي أو شبهه.

كما قرر المشرع التونسي عقوبات تكميلية بالفصل 5 متمثلة في منع الإقامة ، والمراقبة الإدارية، ومصادرة المكاسب في الصور التي نص عليها القانون، والحجز الخاص، والإقصاء في

مضامين بعض الأحكام .

المطلب الثاني :المسؤولية الجنائية لمقدمي خدمات الانترنت

إن تشغيل شبكة الانترنت يقتضي تضافر جهود العديد من الأشخاص تتنوع أدوارهم في النشاط الالكتروني وذلك لان الانترنت عبارة عن أنشطة وادوار متعددة في تشغيل أجهزة تخزين المعلومات وبثها وعرضها ، وهؤلاء الأشخاص يطلق عليهم الوسطاء في خدمة الانترنت [1].

والوسطاء هم مجموعة من الأشخاص ينحصر دورهم في تمكين المستخدم من الدخول إلى شبكة الانترنت والتجول فيها والاطلاع على ما يريد ، فهم يتولون تقديم الخدمات الوسيطة في الانترنت مثل متعهد الوصول والدخول إلى شبكة الانترنت الذي يتولى توفير الوسائل التقنية التي تسمح لعملائه بالدخول إلى الشبكة والتجوال فيها ، ومقدم خدمات الإيواء (متعهد الإيواء) الذي يتولى تخزين وحفظ البيانات والمعلومات لعملائه ويمدهم بالوسائل الفنية التي تسمح لهم بالحصول على هذه البيانات عن طريق الشبكة ، وكذلك مورد المعلومات أو منتجها الذي يقوم ببث المعلومات والرسائل المتعلقة بموضوع معين على الانترنت[2] .

---

[1] – عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص134-135.

[2] – ويتميز دور هؤلاء الأشخاص في عملية بث المعلومة عبر الشبكة بأنه لا يتعدى المساهمة المادية في بثها من خلال دور فني بحت ، ويتسم هذا الدور بأهمية بالغة، إذ من خلاله يتمكن المستخدم من الاتصال بالموقع المراد الدخول إليه والحصول على المعلومات المنشورة فيه.

إن طبيعة الدور الفني الذي يقوم به الوسطاء له اثر كبير في تحديد مسؤوليتهم فلما كان هؤلاء الوسطاء يرتبطون مع غيرهم بعقود اشتراك أو توريد ، فهنا لا تثور صعوبة في تحديد مسؤوليتهم تجاه هذا الغير ،إذ يمكن الركون إلى العقد لتحديد المسؤولية ، ولكن الصعوبة تثور بشأن تحديد المسؤولية الجنائية لهؤلاء .

وقد اختلفت التشريعات فيما يتعلق بالمسؤولية الجنائية لمقدمي الخدمات الوسيطة في شبكة الانترنت ، فبعضها تنطبق عليها القواعد العامة للقانون الجنائي وبعضها الأخرى نظمها بتشريعات خاصة كالتشريعات الخاصة بالصحافة والنشر والإعلام والاتصال ، والتشريعات الخاصة بالتجارة الالكترونية[1].

وعليه سنبحث المسؤولية الجنائية لمقدمي خدمات الانترنت من خلال ماجاء في التشريعات الأجنبية (الفرع الأول) ، والتشريعات والعربية (الفرع الثاني) .

[1] – جميل عبد الباقي ، القانون الجنائي والانترنت، دار النهضة العربية ،القاهرة مصر، 2002، ص4.

الفرع الأول :المسؤولية الجنائية لوسطاء الانترنت في التشريعات الأجنبية

لم تتول أغلب التشريعات الخاصة بالمعاملات الالكترونية تنظيم مسؤولية مقدمي خدمات الانترنت تاركة إياها للقواعد العامة ، ومع ذلك نصت بعض التشريعات صراحة على مسؤوليتهم كالتوجيه الأوربي والقانون الفرنسي والقانون الألماني.

أولا- في التوجه الأوربي :

تبنى البرلمان الأُوروبي بالإجماع في 8 جوان 2000 التوجيه رقم 2000/31 "

"،

وخصص القسم الرابع منه لتنظيم المركز القانوني للوسطاء في خدمات الإنترنت[1].

وأكد التوجه في المادة 43 أن مقدم الخدمة لا يسأل قانونا إذا كان عمله يقتصر على النقل والتخزين ، أما التدخل الفني الخاص بعملية النقل فلا يثير المسؤولية حيث أنه لا يمثل تدخلا في المعلومات والبيانات ذاتها [2].

وألزمت المادة 46 من يقوم بتخزين البيانات القيام بسحب البيانات غير المشروعة أومنع الوصول إليها بمجرد علمه بعدم مشروعية هذه البيانات المحزنة.

وألزمت أيضا المادة 12 من التوجيه الأُوروبي الدول الأعضاء عدم مساءلة من يقوم بتوصيل الخدمة إلا إذا كان هو مصدر المعلومات أو قام باختيار أو تعديل البيانات ، كما قررت المادة 14 عدم مسؤولية متعهد الإيواء عن البيانات التي يقوم بإيوائها بناءا على طلب العملاء بشرط ألا يكون عالما بعدم مشروعية المعلومات ، أما إذا علم بدلك فيجب عليه اتخاذ اللازم لمنع الاطلاع عليها أو سحبها ، مع عدم الإخلال بحق الجهات الإدارية أو القضائية في الدول الأعضاء في

---

[1] – أمين أعزان، مرجع سابق ، ص 108.

[2] –عبد الحليم رمضان، مرجع سابق، ص122-123.

توجيه مقدم الخدمة لمنع نقل بيانات غير مشروعة أو إخطارها بوجودها[1].

حظر الإلكت

تكشف الأنشطة غير المشروعة وفقا للمادة المادة 15[2] أن يتصرفوا بشكل مناسب لمنع الوصول إلى هذا المحتوى غير المشروع [3].

ثانيا- في القانون الفرنسي والقانون الألماني :

وقد جاءت المادة 22

نقل أحكامه إلى تشريعاتهم الداخلية بحلول سنة 2002. بعض الدول الأعضاء بتنظيم مسؤولية مقدمي خدمات الانترنت ، من أبرزها فرنسا وألمانيا .

1- موقف القانون الفرنسي :

نظم المشرع الفرنسي المسؤولية الجنائية لمقدمي خدمات الانترنت من خلال القانون رقم 719 /2000 المتعلق بتعديل أحكام قانون حرية الاتصالات ، والقانون الصادر في 21 جوان 20004 المتعلق بالاقتصاد الرقمي [4].

أ- القانون رقم 917/2000 الصادر في 01أوت 2000:

قبل صدور القانون رقم 719 /2000 المتعلق بتعديل أحكام قانون حرية الاتصالات وفي ظل ، ثار تساؤل كبير حول القانون الواجب التطبيق على مسؤولية مقدمي خدمات الانترنت هل قانون الصحافة أم قانون الإذاعة والتلفزيون ؟

---

[1] – شيماء عبد الغني عطاء الله ، مرجع سابق ، ص169.أمين أعزان ، مرجع سابق ، ص209.

[2] – عبد الحليم رمضان، مرجع سابق، ص123.

[3] – محمد حسين منصور المسؤولية الالكترونية ، دار الجامعة الجديدة ، الإسكندرية ، 2003 ، ص 149.

[4] – خصص قانون الاقتصاد الرقمي لسنة 2004 المواد من 05 إلى 09 من الفصل الثاني لتنظيم عمل مقدمي خدمات

حيث انقسم الفقه إلى اتجاهين، إذ يرى الاتجاه الأول إلى إعمال قانون الصحافة ، أي مساءلة مزود الخدمات باعتباره مديرا للتحرير ، ومادام مزود الخدمات يقوم بالنشر فهو يتماثل مع ما يقوم به مدير التحرير في الصحف[1].

وبناءا عليه يساءل مقدم الخدمات على أساس المسؤولية الجنائية المفترضة والتلقائية ، أي التوجيهية و التتابعية [2] ، بشرط أن تكون الرسالة غير المشروعة التي يجري بثها سابقة التخزين أي مسجلة قبل عرضها[3] .

أما الاتجاه الثاني يرفض مساءلة مقدم الخدمات على أساس المسؤولية المفترضة والتلقائية وفقا لقانون الصحافة، و قانون الاتصالات السمعية والبصرية لمخالفتها لقرينة البراءة ، مادام أنها تقيم قرينة قاطعة على مسؤولية رئيس التحرير وما يليه[4]، وهو الاتجاه الراجح في نظرنا، لأن مبدأ البراءة يحتم أن تقوم جهة الادعاء وهي النيابة العامة بإثبات الركن المادي والمعنوي في جانب المتهم ، ولا يكلف المتهم بإثبات براءته.

كما اختلف القضاء الفرنسي في هذا الشأن ، حيث أصدر قسم التقارير والدراسات بمجلس الدولة تقريرا في شأن الانترنت والخطوط الرقمية[5]، استبعد فيه تطبيق المسؤولية الجنائية التتابعية المطبقة في قانون الصحافة، و قانون الاتصالات السمعية والبصرية ، وأيد تطبيق القواعد العامة للقانون الجنائي بشأن الأعمال الوسيطة الخاصة بالانترنت ، واشترط لقيام مسؤولية مقدمات

---

[1] – شيماء عبد الغني عطا الله، مرجع سابق ، ص169.

[2] – وفقا للمادة 42 من قانون الصحافة والمادة 93–3 من قانون الاتصالات السمعية والبصرية الفرنسي، إذا لم يمكن مساءلة مدير التحرير، فانه يرجع على صاحب الرسالة ، وفي حالة عدم معرفة هذا الأخير يتم الرجوع على البائعين والموزعين والقائمين بوضع الدعاية والمنتج بصفته فاعلا أصليا .

[3] – جميل عبد الباقي ، القانون الجنائي والانترنت ، مرجع سابق ، ص129.

[4] –شيماء عبد الغني عطا الله، مرجع سابق ، ص170.

[5] – وافقت الجمعية العمومية لمجلس الدولة على هذا التقرير في 02 جويلية 1998 ، وتعرض هذا التقرير للمشكلات الخاصة بالانترنت والتجارة الالكترونية ومن بين المواضيع التي تناولها المسؤولية القانونية لمقدمي الخدمات الوسيطة بالانترنت في المادة 02.عبد الحليم رمضان، مرجع سابق ، ص124.

الوسيطة ضرورة معرفة المضمون غير المشروع وتوافر القصد الجنائي والإجراءات المتخذة لمراقبة هذا النشاط والقدرة على المراقبة[1]، وعلى خلاف ذلك قضت محكمة النقض الفرنسية في حكم صادر في 1998/12/08 بأن المدعو (س ر) يحاكم بوصفه منتجا، ومسؤولية المنتج تقوم حتى في حالة البث المباشر ، وحتى لو دفع بانعدام قدرته على الرقابة مسؤوليته مفترضة لا تقبل إثبات العكس ،وهو يتعارض مع مبدأ البراءة الذي يسمح للمتهم بإثبات عكس ما اتهم به[2].

وحكمت أيضا محكمة استئناف باريس في قرارها الصادر في 02 فيفري 1999بمسؤولية الشخص الذي قام بإيواء المواد المتعلقة بالانترنت على أساس أن هذه الخدمة تدخل ضمن الخدمات السمعية البصرية ، وأقامت مسؤوليته على أساس المسؤولية التلقائية [3].

كذلك حكمت محكمة باريس الابتدائية في حكمها الصادر في 10 تموز 1997 أن مساهمة

في ارتكاب الجريمة، مما يستوجب معه إدانته إلى جانب الفاعل الأصلي على هذا الفعل[4].

نتيجة للاختلاف الفقهي والقضائي تدخل المشرع الفرنسي فأصدر القانون رقم 719/2000 الصادر بتاريخ 01 أوت المتعلق بتعديل أحكام القانون المتعلق بحرية الاتصالات رقم 1067 /86 الصادر بتاريخ 30 أيلول 1986 ، والذي تنص المادة 8/43 منه على إن الأشخاص الطبيعيين والمعنويين الذين يتعهدون مجانا أو بمقابل بالتخزين المباشر والمستمر للمعلومات وكل ما من طبيعته إمكان استقباله فأنهم يكونون غير مسؤولين جزائيا عن مضمون هذه المعلومات أو الخدمة

---

[1] – عبد الحليم رمضان، مرجع سابق ، ص124.

[2]– أمين أعزان، مرجع سابق ، ص211.

[3] عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص148.

[4] – أمين أعزان، مرجع سابق ، ص211.

إلا إذا أصبحوا مختصين برقابتها بأمر من السلطة القضائية وامتنعوا عن أن يوقفوا بسرعة بث أو نشر هذه المعلومات عبر مواقع الانترنت[1].

"التجارة

الإلكترونية"،

فعلي بالمضمون الإلكتروني غير المشروع، وعلى الرغم من علمهم هذا لم يتخذوا الإجراءات اللازمة لشطبه، أو على الأقل لمنع وصول الجمهور إليه[2].

كما أوجبت الفقرة التاسعة من المادة 43 سالفة الذكر على متعهد الإيواء أن يزود عملائه بالوسائل الفنية التي تسمح بتحديد هوية كل من يسهم في وضع مضمون المعلومات على الانترنت ، حتى يمكن تحديد الشخص المسؤول [3].

كما أن الفقرة العاشرة من المادة المذكورة تشير إلى ضرورة الالتزام بالشروط الواردة في القوانين المنظمة للاتصال السمعي البصري ومنها أحكام القانون رقم 625 لسنة 1982 والمتعلق بقواعد

كان شخصا معنويا يجب تحديد اسم الشركة ومركزها واسم مديرها أو المسؤول عنها، وتهدف هذه الإجراءات إلى تمكين الجمهور من معرفة بيانات كل شخص يساهم في بث معلومة أو إذاعة

---

[1]– TGI Paris, 10 juillet 1997; cité par Guide Permanent Droit et Internet, E 3.3 Hébergement du site, précité, nº 25, p.18, « La participation de l'hébergeur à la diffusion des propos poursuivis pourrait seulement, si son caractère délibéré était établit, constituer une complicité des délits susceptibles d'avoir été commis ».

[2] – ويلاحظ على النص المتقدم إن المشرع الفرنسي لم يكتف بمبدأ عدم مسؤولية متعهد الإيواء فحسب ، بل ذهب إلى ابعد من ذلك في حصر مسؤوليته المحتملة في حالة واحدة هي عدم مبادرة المتعهد إلى إزالة المشكو منه بناء على طلب من السلطة القضائية وحدها ، فلا يسأل بالتالي إذا ورد مثل هذا الطلب إليه من غير هذه السلطة كالمتضرر أو الغير.

[3] – ، فإن القصد الإجرامي لهؤلاء ينتفي في حالة عدم علمهم الفعلي بالمضمون الإلكتروني غير المشروع، أو إذا ما قاموا بشطب هذا المضمون ، أو بمنع وصوله للجمهور.

خدمة عن طريق أي وسيلة من وسائل الاتصال حتى يكون من السهل عليه توجيه دعوى المسؤولية إلى الشخص المسؤول عن الضرر[1].

ووفقا للفقرة 11 من المادة المذكورة لا يجوز أن يفرض على متعهد الإيواء التزام عام بمراقبة المعلومات التي يقوم بنقلها أو تخزينها ولا التزام عام بالبحث عن الوقائع والظروف التي تكشف الأنشطة غير المشروعة ، ولا يكون مسؤولا إلا إذا علم بمحتوى المواقع أو تمادى على إبقاء الروابط رغم علمه ولم يعمل على منع دخولها أو وصولها[2].

ب –القانون الصادر في 21 جوان 2004 حول الثقة في الاقتصاد الرقمي :

مت الحكومة الفرنسية في 14 حزيران 2001 "شركات المعلوماتية"
المشروع الغي [3].

فجاءت الحكومة الفرنسية من جديد في 15 كانون الثاني 2003 حول الثقة في الاقتصاد الرقمي" 21 حزيران 2004
واعتبارا من هذا التاريخ أصبح لمقدمي خدمات الإنترنت نظامهم القانوني الخاص[4].

---

[1] – عامر محمود الكسواني ،التجارة عبر الحاسوب ، دار الثقافة للنشر والتوزيع ، الأردن ،2008، ص98

[2] – وقد ذهبت محكمة استئناف باريس إلى ذلك في احد أحكامها والذي جاء فيه (ينبغي على متعهد الإيواء أن يضمن التخزين المباشر والمستمر للرسائل والمعلومات ووضعها تحت تصرف عملائه ولا يكون مسؤولا عن العرض الشائن أو الفاضح الذي يقدم للمستخدمين ، إلا إذا امتنع عن وقف بث هذه المعلومات بسرعة
فور علمه بطبيعتها غير المشروعة وذلك طبقا لأحكام المادة (43) من القانون رقم 2000/719 .

[3] - Luc GRYNBAUM, "LCEN. Une immunité relative des prestataires de services Internet", Communication- Commerce électronique, Études, Septembre 2004, nº 28, p. 36

[4] - Loi nº 2004/575 du 21 juin 2004 sur la Confiance dans l´économie numérique, JO, 22 juin 2004, p.11168.

خصص هذا القانون المواد من 05 إلى 09 من الفصل الثاني لتنظيم عمل مقدمي خدمات الانترنت، ووفقا للمادة 1/6 يقتصر عملهم على تقديم خدمات الاتصال عبر الانترنت.

وألزم القانون هؤلاء بإخطار المشتركين في الخدمة عن وجود وسائل تسمح بغلق الخدمة أو توقيع جزاءات عليهم إذا توفرت شروط ذلك .

أكدت الفقرة 07 من المادة 06 أن مزودي الخدمة ليس عليهم التزام بالإشراف والرقابة على مضمون البيانات التي يقومون بنقلها، كما أمهم غير ملزمين بالبحث عن الوقائع التي تشير إلى الأنشطة غير المشروعة[1].

2- موقف القانون الألماني :

كان التشريع الألماني أول تشريع أوربي يحدد مسؤولية الوسطاء في الانترنت وذلك بمقتضى قانون خدمات المعلومات والاتصال الصادر 10أوت 1997، حيث اهتم بتحديد الأعمال التقنية الوسيطة في مجال الانترنت وتقرير مسؤولية وسطاء الانترنت سواء من الناحية المدنية أو الجنائية أو الإدارية[2].

وقد قرر في الفقرة(2) من المادة 05 مسؤولية مستضيفي المواقع (متعهد الإيواء) عن مضمون البيانات المخزنة إذا توفر شرطان هما :

أ-العلم بمحتويات الموقع :

إن مسؤولية وسطاء الانترنت تقوم على الخطأ الثابت ، وليست مسؤولية افتراضية عن مضمون المواقع التي يقوم بإيوائها ، بل يسأل عن السلوك الذي يجعله فاعلا أصليا للجريمة أو شريكا فيها، لأنه يتعامل مع مجموعة كبيرة من المواقع تتناول مسائل متعددة وأغراض ولغات متنوعة .

---

[1] - إن الفقرة 07 من المادة 06 تأكيد لما جاء في المادة 11/43 من قانون رقم 719/2000 والمادة 15 من التوجيه الأوربي.

[2] -cyril rojinsky.commerce électronique et responsabilité des acteurs de l'internet Europe www.droit-technologie.or

ب-استطاعة متعهد الإيواء منع نشر أو بث المضمون غير المشروع :

لا يكفي لتحقق مسؤولية متعهد الإيواء علمه بالمضمون غير المشروع للموقع الذي يتولى إيوائه بل يشترط أن يكون باستطاعته منع نشر أو بث المضمون من الناحية الفنية ، فإذا لم يكن باستطاعته ذلك ، فلا يسأل في هذه الحالة[1].

28 ماي 1998 أحد مقدمي خدمات

الإنترنت كشريك في جريمة نشر صور جنسية للأطفال .

[1]- TI MUNICH, 28 mai 1998, Aff. "Compuserve" in P. Coëtlogon, cite par P. KOCH, "Le régime de responsabilité des fournisseurs d´accès et d´hébergement sur internet en droitAllemand", Légipresse, décembre, 1999, chronique, p. 15

الفرع الثاني :المسؤولية الجنائية لمقدمي خدمات الانترنت في بعض التشريعات العربية

لم تتضمن قوانين الدول العربية الخاصة بالتعاملات الالكترونية نصوصا تنظم مسؤولية وسطاء الانترنت سوى البعض منها كالقانون البحريني [1]، والقانون التونسي ، والقانون الجزائري في

---

[1] – لقد كان المشرع البحريني أكثر وضوحا عند تصديه لمعالجة مسؤولية وسيط الشبكة في المادة 19 من قانون التجارة الالكترونية لسنة 2002 .

وفقا للفقرة المادة 19 تنتفي مسؤولية وسيط الشبكة مدنيا أو جنائيا عن أية معلومات واردة في شكل سجلات الكترونية تخص الغير ، إذا لم يكن هو مصدر هذه المعلومات أو اقتصر دوره على مجرد توفير إمكانية الدخول عليها ، وذلك إذا كانت المسؤولية قائمة على إفشاء أو نشر أو بث أو توزيع هذه المعلومات أو أية بيانات تتضمنها ، أو التعدي على أية حق من الحقوق الخاصة بتلك المعلومات[1].

ووفقا للفقرة الثانية من هذه المادة19 يشترط لانتفاء مسؤولية وسيط الشبكة عدم علمه بأنه ينشأ عن هذه المعلومات أية مسؤولية مدنية أو جزائية، وعدم علمه بأية وقائع أو ملابسات من شأنها أن تدل بحسب المجرى العادي للأمور على قيام مسؤولية مدنية أو جزائية ، كما يشترط قيام وسيط الشبكة على الفور في حالة علمه بما تقدم بإزالة المعلومات ووقف إمكانية الدخول إلى نظام المعلومات.

وفقا للفقرة الثالثة من هذه المادة 19 فانه لا تفرض أحكام هذه المادة على وسيط الشبكة أي التزام قانوني بشأن مراقبة أية معلومات واردة في شكل سجلات الكترونية تخص الغير بغرض تحقق علم الوسيط بان المعلومات ينشأ عنها مسؤولية مدنية أو جنائية ، أو لتحقق علمه بأية وقائع أو ملابسات من شأنها أن تدل بحسب المجرى العادي للأمور على قيام هذه المسؤولية إذا اقتصر دور وسيط الشبكة على مجرد توفير إمكانية الدخول على هذه السجلات.

ووفقا للفقرة الرابعة من هذه المادة 19، فأنه لا تخل أحكام هذه المادة بأية التزامات عقدية ، أو الالتزامات التي يفرضها أي تشريع بشأن تقديم خدمات الاتصالات اللاسلكية ، الالتزامات التي يفرضها أي تشريع آخر ، أو حكم قضائي واجب النفاذ ، بشأن تقييد أي منع أو إزالة أية معلومات أو الحيلولة دون الدخول .

ووفقا للفقرة الخامسة من هذه المادة 19، فانه يقصد بتوفير إمكانية الدخول على أية معلومات تخص الغير " إتاحة الوسائل الفنية التي تمكن من الدخول على معلومات واردة في شكل سجلات تخص الغير ، أو بثها ، أو مجرد زيادة فاعلية البث ، ويشمل ذلك الحفظ التلقائي أو المرحلي أو المؤقت لهذه المعلومات بغرض إمكانية الدخول عليها ويقصد بالغير فيما يخص وسيط الشبكة أي شخص ليس لوسيط الشبكة أية سيطرة فعلية عليه.

إطار قانون تكنولوجيات الإعلام والاتصال ، بينما جاء خاليا من أي تنظيم لهذه المسؤولية القانون الأردني رقم 85 لسنة 2001 الخاص بالتعاملات الالكترونية، وقانون المعاملات والتجارة الالكترونية رقم 02 لسنة 2002 لإمارة دبي .

أولا- المسؤولية الجنائية لمقدمي خدمات الانترنت في التشريع الجزائري :

تناول المشرع الجزائري المسؤولية الجنائية لمزودي خدمات الانترنت في قانون رقم 04/09 المؤرخ في 5أوت 2009 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1].

وقبل التعرض للمسؤولية الجنائية لمقدمي الخدمات سنبحث شروط استغلال خدمات الانترنت والتزامات مقدمي خدمات الانترنت في التشريع الجزائري.

1- الشروط القانونية لإقامة خدمات الانترنت :

نص المشرع الجزائري في المادة 04 من المرسوم التنفيذي 307/2000 الذي يضبط شروط وكيفيات إقامة خدمات الأنترنت واستغلالها[2]،على أنه لا يرخص بإقامة خدمات انترنت واستغلالها لأغراض تجارية ضمن الشروط إلا للأشخاص المعنويين الخاضعين للقانون الجزائري،الذين يدعون مقدمي خدمات الانترنت .

---

[1] - قانون رقم 04/09 المؤرخ في 05أوت 2009 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، الجريدة الرسمية عدد 47 الصادرة في 16 أوت لسنة 2009.

[2] - المرسوم التنفيذي 2000-307 المؤرخ في 14 أكتوبر سنة 2000 المعدل والمتمم للمرسوم التنفيذي 98-257 المؤرخ في 25 أوت 1998، الذي يضبط شروط وكيفيات إقامة خدمات الأنترنت واستغلالها،ج ر عدد15 صادرة 60 أكتوبر 2000.

وعليه يتضح لممارسة نشاط خدمات الانترنت يشترط أن يمارسها مقدم خدمات الانترنت بناء على ترخيص، على النحو الآتي:

أ-الترخيص (autorisation):

ويقصد بالترخيص عمل تسمح بموجبه السلطة الإدارية لمستفيد بممارسة نشاط أو التمتع بحق ممارسته ، ويمكن هذا الإجراء الإدارة من ممارسة رقابتها على الأنشطة الاقتصادية ، فنظام الترخيص أداة فعالة للرقابة الإدارية المسبقة [1].

أما من حيث الطبيعة القانونية للترخيص فهو تصرف قانوني في صورة قرار إداري إنفرادي[2]، وهذا القرار منشئ للحق وليس كاشف له [3].

ويشترط للحصول على ترخيص يجب على الطالب أن يقدم عرض مفصل عن الخدمات التي يقترح تقديمها وكذلك شروط وكيفية النفاذ إلى هذه الخدمات كذلك يشترط دراسة تقنية حول الشبكة المقترحة وحول التجهيزات والبرامج المعلوماتية التابعة لهان مع تحديد هيكلها وكذلك صيغ الوصل بالشبكة العمومية للاتصالات، كذلك يجب على المستثمر أن يقدم التزام من المصالح المختصة في الوزارة المكلفة بالاتصالات يثبت إمكانية إقامة الوصلة المخصصة، الضرورية لنقل خدمات الانترنت[4]، ولا يسلم الترخيص بالاستغلال إلا بعد تحقيق تأهيلي يأمر به وزير

---

[1]-Emmanual Derieux, Droit de la communication; 3eme éd, LGDJ 1999, P113

[2]- أعراب أحمد، السلطات الإدارية المستقلة في المجال المصرفي، رسالة ماجستير، كلية الحقوق جامعة بومرداس 2007/2006، ص64-65.

[3]-André CHAMINADE ? poste et communications électroniques 'Régime' Juridique des autorisations d'utilisation des préquences radioélectriques, JCP, la semaine juridique N°43,24 Octobre 2007,II10177,P36.

[4]- المادة 5 من المرسوم التنفيذي 98-257

الاتصالات[1] ، وكذلك بناءا على موافقة اللجنة المذكورة [2]، و يسلم الترخيص لمدة غير محددة ولا يمكن التنازل عنه[3] .

ب- شخص معنوي خاضع للقانون الجزائري :

تنص المادة 04 من المرسوم التنفيذي 307/200 على أنه " لا يرخص بالدخول لنشاط الانترنت إلا للأشخاص المعنويين الخاضعين للقانون الجزائري، الذين يدعون أدناه مقدمي خدمات الانترنت "[4].

يتضح بأن كل شخص معنوي خاضع للقانون الجزائريين يمكنه ممارسة هذا النشاط، سواء كان هذا الشخص عام أو خاص، وبغض النظر عن جنسيته.

إذ كان المشرع الجزائري يشترط الجنسية الجزائرية [5]، ثم تراجع بعد ذلك عن هذا التمييز بعد تعديل المادة 04 بموجب المرسوم التنفيذي 2000-307 ،حيث فتح باب الاستثمار أمام الأشخاص المعنويين الخاضعين للقانون الجزائري .

---

[1] - المادة 6 من نفس المرسوم.

[2] -المادة 7 من المرسوم التنفيذي 98-257، المعدل بموجب المرسوم التنفيذي 2000-307.

[3]-المادة 8 من نفس المرسوم

[4]- كانت المادة 04 من المرسوم التنفيذي 257/98 تنص على أنه لا يرخص بالدخول لنشاط الانترنت إلا للأشخاص المعنويين الخاضعين للقانون الجزائري، المدعوين أدناه مقدمو الخدمات، وبرأس مال يملكه فقط أشخاص معنويون خاضعون للقانون العام، و/أو أشخاص طبيعيون من جنسية جزائرية.

[5] - كان المشرع الجزائري يشترط أن يكون رأس مال هذا الشخص المعنوي مملوك لأشخاص معنويون خاضعون للقانون العام و/أو أشخاص من جنسية جزائرية ، وبذلك المشرع الجزائري يقصي الأجانب من الاستثمار في نشاط الانترنت، وهذا يمس بأحد أهم المبادئ التي جاء بها قانون المنافسة، وهو مبدأ عدم التمييز والتفرقة بين الوطنيين والأجانب.

2- التزامات مقدمي خدمات الانترنت :

عرف المشرع الجزائري في المادة 02/د أي كيان عام أوخاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية ، أونظام اتصالات ، وأي كيان أخر يقوم بمعالجة أوتخزين معطيات معلوماتية لفائدة خدمات الاتصال المذكورة أو لمستعمليها [1]، وفرض المشرع عليهم عدة التزامات .

ألزم قانون رقم 04/09 مقدمي خدمات الانترنت كمقدمي خدمات بصفة عامة ، بمساعدة السلطات العامة،، حفظ المعطيات المتعلقة بحركة السير ، كما فرض عليهم التزامات خاصة في المرسوم التنفيذي 257/98 المؤرخ في 25 أوت 1998، وفي قانون رقم 04/09 2009 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته[2]، على التفصيل الآتي :

ا-الالتزامات العامة:

-مساعدة السلطات العامة :

حيث يلتزم مقدمي الخدمات حسب المادة 10 من قانون قم 04/09 ، بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 تحت تصرف تلك السلطات[3].

---

[1] -عرف المشرع الفرنسي الصادر سنة 2000 مزودي الخدمات بأنهم الذين يقومون بمقابل أو بدون مقابل بالتخزين المباشر والدائم، ويضعون تحت الجمهور إشارات أو صور أو رسائل يمكن الحصول عليها بالخدمات التي يعرضونها.

[2] - راجع المادة 14 من المرسوم التنفيذي 257/98 المؤرخ في 25 أوت 1998 الذي يضبط شروط وكيفيات إقامة خدمات الأنترنت، واستغلالها ، وراجع المادة 12 من قانون رقم 04/09 2009 بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[3] - نص المشرع على إجراء حفظ المعطيات المتعلقة بحركة السير في المادة 11 من قانون 09-04 ن وتحدد مدة حفظ المعطيات المذكورة وفي هذه المادة بسنة واحدة ابتداء من تاريخ تسجيلها . وهي في الحقيقة مدة غير كافية مقارنة بأهمية المعطيات المنصوص عليها ، خاصة معطيات الهاتف .

كما يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذلك المعلومات المتصلة بها تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق وبالتالي إذا ساعد مقدمو خدمات الانترنت السلطات المكلفة بالتحري والتحقيق ،عليهم أن يلتزموا وبات [1].

- حظ المعطيات المتعلقة بحركة السير :

طبقا للمادة 11 من قانون 04/09 ، يلتزم مقدمو الخدمات بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة ، والمعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال والمعطيات التقنية وكذا تاريخ ووقت ومدة كل اتصال والمعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها والمعطيات التي تسمح بالعرف على المرسل إليه أو المرسل إليهم الاتصال ، كذا عناوين المواقع المطلع عليها[2].

ب- الالتزامات الخاصة:

نص المشرع الجزائري على التزامات مقدمي خدمات الانترنت في المرسوم التنفيذي 257/98 المؤرخ في 25 أوت 1998، الذي يضبط شروط وكيفيات إقامة خدمات الأنترنت، واستغلالها[3]، وكذلك في القانون رقم 04/09 المؤرخ في 5أوت 2009 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،على النحو الآتي :

---

[1] - راجع الفقرة الثانية (02) من المادة 10 من القانون رقم 04/09.

[2] - بالنسبة لنشاط الهاتف يقوم المتعامل بحفظ المطيات المذكورة في الفقرة (أ) وكذلك تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه. وتحدد مدة حفظ المعطيات بسنة من تاريخ التسجيل .

[3] - التنفيذي المرسوم التنفيذي 98-257 المؤرخ في 25 أوت 1998، الذي يضبط شروط وكيفيات إقامة خدمات الأنترنت، واستغلالها، والمعدل بموجب المرسوم التنفيذي 2000-307 المؤرخ في 14 أكتوبر سنة 2000 ، الجريدة الرسمية عدد 63 لسنة 1998.

***في المرسوم التنفيذي 257/98 المؤرخ في 25 أوت 1998:**

نص المشرع الجزائري على التزامات مقدمي خدمات الانترنت في المادة 14 من المرسوم التنفيذي رقم98 /257، بعضها تقنية ، وأخرى أخلاقية ، وبعضها متعلقة بالمسؤولية ، كالآتي :

الالتزامات التقنية:

فرض المشرع الجزائري على مقدمي خدمات الانترنت التزامات تقنية تتمثل في تسهيل النفاذ إلى خدمات الانترنت حسب الإمكانيات المتوفرة إلى كل الراغبين في ذلك باستعمال أنجع الوسائل التقنية ، وكذا إعطاء مشتركيه معلومات واضحة ودقيقة حول موضوع النفاذ إلى خدمات الانترنت وصيغة مساعدتهم كلما طلبوا ذلك ، وكذلك عرض أي مشروع خاص باستعمال منظومات الترميز على اللجنة .

كما ألزمهم باتخاذ كل الإجراءات اللازمة لتأمين حراسة دائمة لمضمون الموزعات المفتوحة لمشتركيه قصد منع النفاذ إلى الموزعات التي تحتوي معلومات تتعارض مع النظام العام أو الأخلاق .

الالتزامات غير التقنية:

حفظا على الحياة الخاصة لمشتركيه ألزم المشرع مقدمي خدمات الانترنت المحافظة على سرية كل المعلومات المتعلقة بحياة مشتركيه الخاصة وعدم الإدلاء بها إلا في الحالات المنصوص عليها في القانون ، إذ يلتزم بالحفاظ على معطيات مشتركيه والاعوقب بجريمة إفشاء الأسرار المنصوص عليها في المادة من قانون العقوبات 301[1] ، كما فرض عليهم التزام أخلاقي

[1] – تعاقب المادة 301 (قانون رقم 82-04 المؤرخ في 13 فيفري 1982) من قانون العقوبات على إفشاء السر المهني بالحبس من شهر إلى ستة أشهر و بغرامة من 500 إلى 5000 دج الأطباء و الجراحون و الصيادلة و القابلات و جميع الأشخاص المؤتمين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدى بها إليهم و أفشوها في غير الحالات التي يوجب عليهم فيها القانون إفشاءها و يصرح لهم بذلك.

متمثل في احترام قواعد حسن السيرة بالامتناع خاصة عن استعمال أي طريقة غير مشروعة سواء اتجاه المستعملين أو تجاه مقدمي خدمات الانترنت الآخرين [1].

إضافة إلى هذه الالتزامات فرض المشرع على مقدمي خدمات الانترنت التزامات متعلقة بالمسؤولية متمثلة في تحمل مسؤولية محتوى الصفحات وموزعات المعطيات التي يستخرجها

يتعلق بمحتوى الصفحات التي يستخرجونها وفقا للأحكام التشريعية المعمول به .

وبالتالي الالتزامات المنصوص عليها في المادة 14 من المرسوم التنفيذي إطار المرسوم التنفيذي 98-257 المتعلق بشروط وكيفيات إقامة خدمات الإنترنت واستغلالها، جاءت متنوعة وعديدة ، ولم تقتصر على مجال معين ، بحيث نص على التزامات تقنية ، وأخرى غير تقنية ولم يهمل المشرع حتى الجانب الأخلاقي وفرض عليهم احترام أخلاقيات المهنة [2].

***في القانون رقم 04/09 المؤرخ في 5أوت 2009 :**

نص عليها المشرع في المادة 12 من قانون قم 04/09 المؤرخ في 5أوت2009 التي تنص على أنه زيادة على الالتزامات المنصوص عليها في المادة 11[3]، يلتزم مقدمي خدمات الانترنت بما يلي :

---

[1] - راجع المادة 14 من المرسوم التنفيذي 257/98 المؤرخ في 25 أوت 1998 الذي يضبط شروط وكيفيات إقامة خدمات الأنترنت، واستغلالها ، المعدل والمتمم بموجب المرسوم التنفيذي 2000-307 المؤرخ في 14 أكتوبر سنة 2000.

[2] – وبالتالي جمع المشرع بين التزامات قانوني ، وأخرى أخلاقية ، اقتناعا منه أن القانون لوحده لايكفي بل لابد من التزام أخلاقيات المهنة ، باحترام قواعد حسن السيرة بالامتناع خاصة عن استعمال أي طريقة غير مشروعة سواء اتجاه المستعملين أو تجاه مقدمي خدمات الانترنت الآخرين.

[3] - ألزم المشرع في المادة 11 من قانون رقم 04/09 مقدمي خدمات الانترنت كمقدمي خدمات بصفة عامة، بمساعدة السلطات العامة،، حفظ المعطيات المتعلقة بحركة السير .

* التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أوغير مباشرة بمخالفتها للقوانين وتخزينها أوجعل الدخول إليها غير ممكن.

* وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العم أو الآداب .

3- قيام المسؤولية الجنائية لمقدمي خدمات الانترنت :

تقوم المسؤولية الجنائية لمقدمي الخدمات في حالتين ، هما جريمة إفشاء أسرار التحري والتحقيق المنصوص عليها في المادة 10 من قانون 09-04 ، جريمة عدم حفظ المعطيات المتعلقة بحركة السير والمنصوص عليها في المدة 4/11 ، كالآتي :

أ- جريمة إفشاء أسرار التحري والتحقيق:

نص عليها المشرع الجزائري في المادة 10/ف2 من قانون 04/09 المؤرخ في 5أوت2009 والتي تنص على أنه : "يتعين على مقدمي خدمات الانترنت كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق ". ولقيام هذه الجريمة لابد من توافر ركنين مادي ومعنوي.

-الركن المادي:

يتمثل الركن المادي لهذه الجريمة في إفشاء مزود الخدمات لأسرار التحري والتحقيق ، أي إذاعتها ونقلها واطلاع الغير عليها بعد أن كان العلم بها قاصرا على أصحابها أو الذين ائتمنوا عليها بحكم وظيفتهم[1].

ومادام مزود الخدمات مؤتمن على أسرار البحث والتحقيق ، فيتعين عليه كتمان سرية العمليات .

[1] -شيماء عبد الغني عطا الله، مرجع سابق، ص214.

وبالتالي يشمل محل هذه الجريمة إفشاء العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها ، والمتعلقة بالتحري والتحقيق [1].

وتجدر الإشارة إلى أن المشرع الجزائري لم يحدد عقوبة لهذه الجريمة، بل أحال على العقوبات المقررة لجريمة الإفشاء ، والمبينة في المادة301 من قانون العقوبات الجزائري والتي تعاقب كل من أفشى ير المهنة بالحبس من شهر إلى ستة أشهر،وبغرامة من 500 دج إلى 5.000 دج على إفشاء السر المهني [2].

-الركن المعنوي:

جريمة إفشاء أسرار التحري والتحقيق هي جريمة عمدية لابد فيها من توافر القصد الجنائي العام ، فيجب أن يعلم الجاني بأنه يرتكب جريمة إفشاء أسرار التحري والتحقيق، وأن تتجه إرادته إلى ارتكاب هذه الجريمة [3].

ولاعبرة بالباعث أو الغرض من الجريمة ، حيث تقوم الجريمة بتوافر القصد الجنائي العام دون الخاص إلى جانب الركن المادي للجريمة المتمثل في إفشاء أسرار التحري والتحقيق من قبل مزودي خدمات الانترنت .

---

[1] – وعليه يشمل محل هذه الجريمة أسرار التحري والتحقيق، فإجراءات التحري والتحقيق سرية وفقا للمادة 11 من قانون الإجراءات الجنائية، ما لم ينص القانون على خلاف ذلك ودون إضرار بحقوق الدفاع وبالتالي إذا أفشى مزود خدمات الانترنت معلومات غير متعلقة بأسرار التحري والتحقيق فلا يعاقب على جريمة إفشاء أسرار التحري والتحقيق المنصوص بالعقوبات المبينة في المادة 301 من قانون العقوبات .

[2] – بالإضافة إلى العقوبات المقررة للشخص الطبيعي المبينة في المادة301 من قانون العقوبات، عاقب المشرع أيضا الشخص المعنوي في المادة 303 مكرر3 بالعقوبات المنصوص عليها في المادة 18 مكرر ، والمادة 18 مكرر2 من قانون العقوبات عند الاقتضاء

[3] – أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ، الجزء الأول، دار هومة ، الجزائر 2014، ص 280.281.

ب- جريمة عدم حفظ المعطيات المتعلقة بحركة السير :

نظمها المشرع في المادة 11/فقرة 4-5 من قانون قم 04/09 [1]، والتي تنص على أنه دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية ، ويعاقب الشخص الطبيعي بالحبس من ستة(6) أشهر إلى خمس(5) سنوات وبغرامة من 50.000د ج إلى 500.000 د ج، أما الشخص المعنوي فيعاقب بالغرامة المقررة في المادة 18 من قانون العقوبات الجزائري[2]. وتقوم هذه الجريمة على ركنين مادي ومعنوي على التفصيل الآتي:

-الركن المادي :

يتمثل الركن المادي لهذه الجريمة في عدم احترام الالتزامات المنصوص عليها في المادة 11 من قانون 09-04، وهي عدم حفظ مزودي الخدمات للمعطيات المنصوص عليها في المادة 11 أو عدم حفظها للمدة المحددة قانونا وهي سنة ابتداء من تاريخ التسجيل وفقا المادة 11 [3].

وبالتالي يتمثل النشاط الإجرامي لهذه الجريمة في عدم حفظ المعطيات المتعلقة بحركة السير أصلا ، أو عدم حفظها في المدة القانونية ، أما محل الجريمة فيتمثل في المعطيات المتعلقة بحركة السير المنصوص عليها في المادة 11من هذا القانون [4].

---

[1] - تنص المادة 4/11-5على معاقبة الشخص الطبيعي بالحبس من ستة (6)أشهر إلى خمس(5) سنوات وبغرامة من 50.000 د ج إلى 500.000 د ج.أما الشخص المعنوي وفقا للمواد18 مكرر إلى 18 مكرر3 من قانون العقوبات الجزائري .

[2] -راجع المادة 11/ف4 -5من قانون قم 04/09 المؤرخ في أوت2009.

[3] - راجع المادة 3/11 من قانون قم 04/09 المؤرخ في أوت2009.

[4] -وفقا للمادة 1/11 تتمثل المعطيات بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة ، والمعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال والمعطيات التقنية وكذا تاريخ ووقت ومدة كل اتصال والمعطيات المتعلقة

ولا تقوم هذه الجريمة بمجرد توافر المشاط الإجرامي ، بل يتطلب المشرع لقيامها نتيجة معينة ، وهي أن يؤدي عدم حفظ تلك المعطيات إلى عرقلة وتعطيل حسن سير التحريات القضائية بسبب عدم حفظ مزودي الخدمات للمعطيات أو عدم حفظها للمدة المحددة قانونا .

ويعاقب الشخص الطبيعي بالحبس من ستة(6) أشهر إلى خمس(5) سنوات وبغرامة من 50.000د ج إلى 500.000 د ج، أما الشخص المعنوي فيعاقب بالغرامة المقررة في المادة 18 من قانون العقوبات الجزائري[1].

-الركن المعنوي:

هذه الجريمة عمدية لابد فيها من توافر القصد الجنائي العام [2]، فيجب أن يعلم الجاني بأنه نشاطه مجرم ، وأنه يتسبب في عرقلة حسن سير التحريات القضائية بسب عدم حفظه المعطيات المتعلقة بحركة السير.

كما يجب أن تتجه إرادته إلى ارتكاب هذه الجريمة، وتحقيق النتيجة الإجرامية المتمثلة في عرقلة حين سير التحريات القضائية [3].

بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها والمعطيات التي تسمح بالعرف على المرسل إليه أو المرسل إليهم الاتصال ، كذا عناوين المواقع المطلع عليها .

[1] -راجع المادة 11/ف4 -5من قانون قم 04/09 المؤرخ في أوت2009.

[2] - حتى تقوم الجريمة لابد من توافر القصد الجنائي ، وبالتالي لاتقوم الجريمة إذا تحقق الركن المادي المتمثل في عد حفظ المعطيات نتيجة خطأ أو إهمال ، كما لم يتطلب المشرع قصد جنائي خاص ن بل اكتفى بالقصد الجنائي العام بعنصريه العلم والإرادة .

[3] - لايكفي أن تتجه إرادته إلى ارتكاب الأفعال الإجرامية المتمثلة في عدم حفظ المعطيات المتعلقة بحركة السير أصلا أو عدم حفظها في المدة القانونية ، بل لابد أن تتجه إرادته إلى تحقيق النتيجة الإجرامية ، وهي انصراف نيته إلى عرقلة حين سير التحريات القضائية

ولم يتطلب المشرع في هذه الجريمة القصد الجنائية الخاص، فلا عبرة بالبعث والغرض من الجريمة، بل تقوم بمجرد توافر القصد الجنائي العلم بعنصريه العلم والإرادة، إلى جانب الركن المادي لقيام الجريمة.

ثانيا – المسؤولية الجنائية لمقدمي خدمات الانترنت في التشريع التونسي :

نظم المشرع التونسي المسؤولية الجنائية لمزود الخدمات في القانون المؤرخ في 9 أوت 2000 المتعلق بالمبادلات والتجارة الالكترونية، كالآتي :

1-جريمة عدم مراعاة الشروط القانونية لممارسة المصادقة الالكترونية

يقتضى الفصل 45 من قانون المبادلات والتجارة الالكترونية أنه "يعاقب كل مزود خدمات المصادقة الالكترونية لم يراع مقتضيات كراس الشروط المنصوص عليه بالفصل 12 من هذا القانون بخطية تتراوح بين 1.000 و 10.000 دينارا". ولقيام هذه الجريمة لابد من توافر ركنين مادي ومعنوي ، كالآتي :

أ-الركن المادي:

يتمثل الركن المادي لهذه الجريمة في عدم مراعاة مزود خدمات المصادقة للشروط والمقتضيات المنصوص عليها في الفصل 12 [1].

---

[1] – اقتضى الفصل 12 من قانون 83 لسنة 2000 المتعلق بالمبادلات والتجارة الالكترونية: ..."يتضمن كراس الشروط خاصة :

-كلفة دراسة ومتابعة ملفات مطالب الشهادات

-آجال دراسة الملفات

-الإمكانيات المالية والمادية التي يجب توفرها لتعاطي النشاط

-شروط تأمين التفاعل المتبادل لأنظمة المصادقة وربط سجلات شهادات المصادقة -القواعد المتعلقة بالإعلام والخاصة بخدماته والشهادات التي سلمها والتي يتعين على مزود خدمات المصادقة الالكترونية حفظها.

وبالتالي يتمثل النشاط الإجرامي في ممارسة مزود خدمات المصادقة الالكترونية خدمات المصادقة دون احترام الشروط الواردة في الفصل 12، ولم يتطلب القانون تحقق نتيجة معين بل تقوم بتوافر السلوك الإجرامي المتمثل في عد احترام شوط ممارسة المصادقة الالكترونية .

وعقوبة هذه الجريمة هي الغرامة التي تتراوح بين 1.000 و10.000 دينار ، وسحب ترخيص مباشرة خدمات المصادقة الالكترونية من مزود خدمات المصادقة كما يتم إيقاف نشاطه لعدم مراعاته الشروط القانونية الواردة في الفصل 12 من قانون المبادلات والتجارة الالكترونية [1].

ب-الركن المعنوي:

هذه الجريمة عمدية لابد فيها من توافر القصد الجنائي العام بعنصريه العلم والإرادة ، فيجب أن يعلم الجاني بأنه يرتكب هذه الجريمة ، وأن تتجه إرادته إلى ارتكاب جريمة عدم مراعاة الشروط القانونية لممارسة خدمات المصادقة الالكترونية[2].

واكتفى المشرع التونسي في بهذه الجريمة كالجرائم الأخرى بالقصد الجنائي العام ولم يتطلب القصد الجنائي الخاص .

2- جريمة التعامل في البيانات دون ترخيص :

اقتضى الفصل 46 من نفس القانون "يعاقب كل من يمارس نشاط مزود خدمات المصادقة الالكترونية بدون الحصول على ترخيص مسبق طبقا للفصل 11 من هذا القانون بالسجن لمدة

---

[1] ينص الفصل 44 من قانون المبادلات والتجارة الالكترونية على أنه بالإضافة إلى الخطية يسحب من مزود خدمات المصادقة الترخيص الممنوح له في مباشرة خدمات المصادقة الالكترونية، ويتم إيقاف نشاطه، وذلك حسب مقتضيات الفصل 44 من قانون المبادلات والتجارة الالكترونية .

[2] -لا يتطلب المشرع التونسي كنظيره الجزائري القصد الجنائي الخاص ، بل هي جريمة عمدية تأخذ صورة القصد الجنائي العام ، وعليه لاتقوم الجريمة إذا وقعت الجريمة نتيجة إهمال أو خطأ ، بل أن يتوافر لديه العلم ، وأن نشاطه مجرم ن وأن تتجه إرادته إلى ارتكاب هذا الجريمة .

تتراوح بين شهرين و3 سنوات وبخطية تتراوح بين 1000 و 10000 دينارا أو بإحدى هاتين العقوبتين".

وحسب المادة 11 من القانون التونسي فإنه لا يمكن لمزود خدمات التصديق أن يباشر عمله دون ترخيص من الوكالة الوطنية للمصادقة، يستوي أن يكون شخصا طبيعيا أو معنويا، وأن هناك شروط محددة ردت في المادة 01 لمن يمنح رخصة مزاولة هذا العمل.

ولقيام هذه الجريمة يجب توافر الركنين المادي و المعنوي، كالآتي:

أ- الركن المادي :

يتحقق الركن المادي في هذه الجريمة بمجرد التعامل في بيانات التجارة الالكترونية دون ترخيص من الجهة المختصة [1]، وحتى و إن لم يترتب على ذلك أي نتيجة إجرامية ، فالجريمة تعتبر سلوكية ، وليست من جرائم الضرر[2].

وتشرف الوكالة الوطنية للمصادقة الالكترونية على منح الترخيص اللازم لممارسة نشاط وخدمات المصادقة الالكترونية، لذلك كان لابد من زجر كل ممارسة لهذه الوظائف خارج مراقبة الوكالة الوطنية للمصادقة الالكترونية، ودون التحصيل على الترخيص المذكور.

---

[1] – وبالتالي تختلف هذه الجريمة عن جريمة عدم مراعاة شروط ممارسة المصادقة ، في أن *جريمة التعامل في البيانات دون ترخيص*

عدم مراعاة شروط ممارسة المصادقة تتعلق بعد احترام الشروط المنصوص عليها في الفصل 12 بعد أخذ الرخيص للممارسة نشاط المصادقة .

[2] – هدى قشقوش ، الحماية الجنائية للتجارة الالكترونية عبر الانترنت ، مرجع سابق ، ص38.

ب- الركن المعنوي :

هذه الجريمة هي جريمة عمدية يكفي لتوافرها توفر القصد الجنائي العام بعنصريه العلم والإرادة، أي أن يكون المزود على علم أنه غير مرخص له في مباشرة النشاط، ومع ذلك تتجه إرادته إلى القيام بتلك الجريمة[1] .

ولم يتطلب المشرع في هذه الجريمة القصد الجنائي الخاص، فلا عبرة بالبعث والغرض من الجريمة، بل تقوم بمجرد توافر القصد الجنائي العلم بعنصريه العلم والإرادة، إلى جانب الركن المادي لقيام الجريمة.

3-جريمة إفشاء الأسرار:

نص عليها المشرع التونسي في المادة 52 ، والتي تنص المادة 52 من قانون المبادلات والتجارة الالكترونية التونسي على أنه " يعاقب طبق لأحكام الفصل 254 من المجلة الجنائية مزود خدمات المصادقة الالكترونية وأعوانه الذين يفشون أو يحثون أو يشاركون في إفشاء المعلومات التي عهدت إليهم في إطار تعاطي نشاطاتهم باستثناء تلك التي رخص صاحب الشهادة كتابيا أو الكترونيا في نشرها أو الإعلام بها أو في الحالات المنصوص عليها في التشريع الجاري العمل به ". ولقيام هذه الجريمة لابد من توافر ركنين، مادي و معنوي، كالآتي:

[1] – عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص ، ص 277

أ_الركن المادي:

يتمثل الركن المادي لجريمة إفشاء الأسرار في إفشاء مزود الخدمات أو أحد أعوانه [1]، أو التحريض عليها أو المشاركة في إفشاء المعلومات التي عهدت إليهم في إطار نشاطاتهم [2] ،على التفصيل الآتي :

- إفشاء المعلومات :

جرم المشرع التونسي عملية إفشاء المعلومات التي عهدت إليهم في إطار تعاطي نشاطاتهم باستثناء تلك التي رخص صاحب الشهادة كتابيا أوالكترونيا في نشرها أو الإعلام بها أو في المجالات المنصوص عليها في التشريع الجاري العمل به [3]، سواء المتعلقة بالحياة العائلية لصاحب المعاملة أو سمعته أومركزه المالي آو الائتماني .

-المشاركة في الإفشاء:

جرم المشرع التونسي عملية *المشاركة في*إفشاء المعلومات التي عهدت إليهم في إطار تعاطي نشاطهم ، قد يقع ارتكابها من قبل أكثر من شخص، بأن يكون أحدهم فاعلا أصليا والآخر شريكا

---

[1] – يلاحظ أن هذه الجريمة يقتصر نطاقها من حيث الأشخاص على مزود خدمات المصادقة الالكترونية أو أحد أعوانه الذي الذين يفشون أو يحثون أو يشاركون في إفشاء المعلومات التي عهدت إليهم في إطار تعاطي نشاطاتهم .

[2] –ولم يكتف المشرع التونسي بتجريم إفشاء المعلومات , بل جرم عملية الإفشاء أو التحريض عليها أو المشاركة في إفشاء المعلومات التي عهدت إليهم في إطار تعاطي نشاطاتهم باستثناء تلك التي رخص صاحب الشهادة كتابيا أو الكترونيا في نشرها أو الإعلام بها أو في الحالات المنصوص عليها في التشريع الجاري العمل به ". و لم يحدد أيضا عقوبة لهذه الجريمة, بل أحال على الفصل 254 من المجلة الجنائية التونسية

[3] – يلاحظ أن المشرع جرم عملية الإفشاء أو التحريض عليها أو المشاركة في إفشاء المعلومات التي عهدت إليهم في إطار تعاطي نشاطاتهم ، لكنه استثنى الإفشاء للمعلومات إذا توافر أسباب إباحة متمثلة في الترخيص من صاحب الشهادة ن فيجوز إفشاء معلوماته التي رخص صاحب الشهادة كتابيا أو الكترونيا في نشرها أو الإعلام بها ن كما يجوز لهم إفشاءها في الحالات المنصوص عليها في التشريع الجاري العمل به ".

وهو ما حدا بالمشرع إلى تجريم المشاركة في الإفشاء، لإقرار حماية أكثر نجاعة لسرية المعلومات، ويسلط على المشارك نفس عقوبة الفاعل الأصلي وفقا الفصل 33 من المجلة الجزائية.

-الحث على الإفشاء :

يقصد بالحث على ارتكاب الجريمة الإرشاد وتشجيع الجاني على ارتكاب الفعل المجرم. وبالنظر للقواعد الجزائية العامة يعد الحث إحدى صور المشاركة، وهي تدخل ضمن ما يطلق عليها بالمشاركة السابقة [1].

وبالتالي يتحقق الركن المادي إذا قام مزود الخدمات أو أحد أعوانه [2]، بإفشاء معلومات أو التحريض أو المشاركة في إفشاء المعلومات التي عهدت إليهم في إطار ممارسة نشاطاتهم غير أن المشرع جاء بأسباب إباحة لا تقوم فيها الجريمة نشاطاتهم ، إذا رخص صاحب الشهادة كتابيا أو الكترونيا في نشرها أو الإعلام بها ، أو في الحالات المنصوص عليها في التشريع الجاري العمل به ، وعليه إذا كان هناك الترخيص من صاحب الشهادة ، فيجوز إفشاء معلوماته التي رخص صاحب الشهادة كتابيا أو الكترونيا في نشرها أو الإعلام بها ، كما يجوز لهم إفشاءها في الحالات المنصوص عليها في التشريع الجاري العمل به ".

---

[1] – تم التنصيص عليها بالفقرة الأولى من الفصل 32 من المجلة الجزائية التي جاء بها يعد ويعاقب بصفة مشارك، الأشخاص الذين أرشدوا لإيقاع الجرائم أو تسببوا في إيقاعها بعطايا أو مواعيد أو تهديدات أو تجاوز في السلطة أو حيلة.

[2] – يلاحظ أن هذه الجريمة يقتصر نطاقها من حيث الأشخاص على مزود خدمات المصادقة الالكترونية أو أحد أعوانه الذي الذين يفشون أو يحثون أو يشاركون في إفشاء المعلومات التي عهدت إليهم في إطار تعاطي نشاطاتهم . بينما يقتصر نطاقها من حيث الموضوع على إفشاء معلومات أو المشاركة أو التحريض على إفشاء معلومات سرية

الركن المعنوي:

يأخذ الركن المعنوي لجريمة الإفشاء غير المشروع من قبل مزود الخدمات أو أحد أعوانه المعلومات التي عهدت إليهم في إطار ممارسة نشاطاتهم، صورة القصد الجنائي العام بعنصريه العلم والإرادة [1].

فيتعين أن يكون الجاني وهو مزود الخدمات أو أحد أعوانه، عالما بأن يقوم بإفشاء المعلومات التي عهدت إليهم في إطار ممارسة نشاطاتهم، ويعلم بان نشاطه هذا مجرم، ويتعين كذلك أن تتجه إرادته نحو تحقيق ذلك السلوك المجرم المتمثل في إفشاء معلومات أو المشاركة أوالتحريض على إفشائها [2].

---

[1] – اكتفى المشرع بالقصد الجنائي العام دون الخاص، فلا عبرة بالبعث والغرض من الجريمة، بل تقوم بمجرد توافر القصد الجنائي العلم بعنصريه العلم والإرادة، إلى جانب الركن المادي لقيام الجريمة.

[2] – أمين أعزان ، مرجع سابق ، ص216.

المبحث الثاني

الحماية الجنائية للمستهلك في التجارة الالكترونية

تثير التجارة الالكترونية العديد من الإشكاليات القانونية، من أهمها جرائم الاعتداء على المستهلك في التجارة الإلكترونية ، وخاصة جرائم الاعتداء على بطاقته الائتمانية ، أو توقيعه الإلكتروني أو بياناته الشخصية ، والتي هي في تزايد ، فاقتضى الأمر توفير حماية جنائية لهذه الوسائل نظرا للخسائر الفادحة المترتبة على الاعتداء عليها.

وبناءا على ذلك اهتمت لجنة الأمم المتحدة للقانون التجاري الدولي بحماية المستهلك من خلال القانون النموذجي للتجارة الالكترونية لعام 1996، والقانون النموذجي للتوقيعات الالكترونية لعام 2001 ، وكذلك تبنت دليل عام 1990 متعلق بالمعالجة الآلية للبيانات الشخصية ، كما أصدر الاتحاد الأوربي التوجيه رقم 97- 07 المتعلق بحماية المستهلك في العقود عن بعد والتوجيه رقم 97- 489 بشان الدفع الالكتروني ،والتوجيه رقم 99-93 بشأن التوقيع الالكتروني.

كما اهتمت بعض الدول بحماية المستهلك في إطار التجارة الالكترونية كفرنسا التي أصدرت قانون رقم 91-1382 المتعلق بأمن الشيكات وبطاقات الوفاء ، وحماية البيانات الشخصية في إطار قانون العقوبات كما اهتمت بعض الدول العربية بحماية المستهلك كالتشريع التونسي في إطار قانون المبادلات والتجارة الالكترونية التونسي لعام 2000، وقانون التوقيع الالكتروني المصري رقم 15-2004 لعام 2004، بينما لم يهتم التشريع الجزائري بالمستهلك في إطار التجارة الالكترونية.

وعليه سنبحث الحماية الجنائية للمستهلك من خلال تجريم الاعتداء على بطاقة الائتمان و التوقيع الإلكتروني (المطلب الأول)، والحماية الجنائية للبنات الشخصية للمستهلك (المطلب الثاني)

المطلب الأول: الحماية الجنائية لبطاقة الائتمان و التوقيع الإلكتروني:

تعتبر بطاقة الائتمان من أهم وسائل الدفع الحديثة ، بينما يعد التوقيع الإلكتروني وسيلة تنفيذ التجارة الإلكترونية ، لذا وفرت لهما التشريعات الجنائية حماية خاصة .

وعليه سنبحث الحماية الجنائية لبطاقة الائتمان (الفرع الأول) والحماية الجنائية للتوقيع الإلكتروني (الفرع الثاني)، كالآتي:

الفرع الأول: الحماية الجنائية لبطاقة الائتمان

إن بطاقات الوفاء من المستجدات الحديثة التي نشأت نتيجة لما يشهده العالم من تقدم علمي و تطور تكنولوجي على كافة المستويات.

ولقد عرف المشرع الفرنسي بطاقة الوفاء في المادة 02 من القانون رقم 1382/91 الصادر في 30 ديسمبر 1991 ، بأنها أداة تصدر من إحدى مؤسسات الائتمان، أو إحدى الجهات المنصوص عليها في المادة 08 من القانون رقم 46/84 و الصادر في 1984/01/24 والخاص بنشاط و رقابة مؤسسات الائتمان، وتسمح لحاملها بسحب أو تحويل النقود من حسابه[1].

كما عرف المشرع الجزائري بطاقات الدفع والسحب في المادة 543 مكرر23 من القانون التجاري [2]، وبطاقة الدفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل أموال ، أما بطاقة السحب تعتبر كل بطاقة صادرة عن البنوك أو الهيئات المالية المؤهلة قانونا وتسمح لصاحبها فقط في سحب الأموال [3] .

---

[1]- عمر سالم، الحماية الجنائية لبطاقة الوفاء، دار النهضة العربية، القاهرة مصر ، 1995، ص 10

[2] – القانون رقم 05-02 المؤرخ في 06 فبراير 2005 ن المعدل والمتمم للأمر 75-59المؤرخ في 26 سبتمبر 1975والمتضمن القانون التجاري ن ج. ر. رقم 11 المؤرخة في2005/02/09

[3] – عرف المشرع الفرنسي بطاقة الوفاء في المادة 02 من القانون رقم 1382/91 الصادر في 30 ديسمبر 1991 بأنها أداة تصدر من إحدى مؤسسات الائتمان، أو إحدى الجهات المنصوص عليها في المادة 08 من القانون رقم 46/84 و الصادر في 1984/01/24 و الخاص بنشاط و رقابة مؤسسات الائتمان، وتسمح لحاملها بسحب أو تحويل النقود من حسابه

وذهب جانب فقهي إلى تعريفها بأنها عقد يتعهد بمقتضاه مصدر البطاقة بفتح اعتماد بمبلغ معين لمصلحة شخص آخر هو حامل البطاقة، الذي يستطيع بواسطتها الوفاء بمشترياته لدى المحلات التجارية التي ترتبط مع مصدر البطاقة بعقد يتعهد فيه بقبول الوفاء بمشتريات حاملي البطاقات الصادرة عن الطرف الأول، على أن تتم التسوية النهائية بعد كل مدة محددة[1].

وبشأن الطبيعة القانونية لبطاقة الائتمان، اختلف الفقهاء بينها من يعتبرها نوع من النقود الإلكترونية لتتم تداولها إلكترونيا، و ذهب رأي آخر إلى أن فكرة الوكالة يقوم بموجبها حامل البطاقة بتوكيل البنك في دفع ثمن السلعة أو الخدمة التي حصل عليها خصما من حسابه لديه واتجه جانب آخر من الفقه إلى اعتبارها أداة وفاء بطبيعتها، مثل الشيك [2].

وعليه سنبحث الحماية الجنائية لبطاقة الوفاء في هذه التشريعات في مواجهة حاملها ثم في مواجهة الغير.

أولا- الاستعمال غير المشروع لبطاقة الائتمان من قبل حاملها :

يتحقق الاستخدام غير المشروع لبطاقة الوفاء من قبل حاملها، يتجاوز رصيده المسموح به خلال فترة صلاحيتها استخدامها بعد انتهاء مدة صلاحيتها أو إلغائها كالآتي[3]:

1-تكييف تجاوز حامل البطاقة للرصيد:

و يتم من خلال قيام حامل البطاقة الشرعي خلال فترة صلاحيتها بالحصول على سلع و خدمات رغم علمه بأن رصيده بالبنك لا يكفي لتغطية هذه المبالغ [4].

---

[1]- جهاد رضا الحباشنة، الحماية الجزائية لبطاقة الوفاء، دار الثقافة، عمان الأردن، 2008، ص 23. عماد علي الخليل، الحماية الجزائية لبطاقة الوفاء (دراسة تحليلية مقارنة)، دار وائل للنشر، عمان، الأردن، 2000، ص 7.

[2]- ألا أنها و إن كانت تحل محل الشيك في الوفاء، لكن في الحقيقة أن لبطاقة الوفاء أحكام مختلفة، بدليل أن بعض التشريعات الأجنبية قد أفردت حماية خاصة لها كالتشريع الفرنسي الذي اصدر قانونا جديدا أسماه قانون أمن الشيكات و بطاقات الوفاء، وهذا بخلاف التشريعات العربية التي لم تنظم أحكامها رغم انتشارها في الحياة اليومية . للتفصيل راجع جهاد رضا الحباشنة ، مرجع سابق ، ص 41-46.

[3]- عمر سالم، مرجع سابق، ص 44.

[4]- سليمان أحمد فضل، مرجع سابق ، ص 172.

و لقد ساد خلاف في الفقه و القضاء الفرنسيين بشأن تكييف هذا الفعل على النحو الآتي:

أ- اتجاه تحميل حامل البطاقة المسؤولية الجنائية :

يرى أنصاره أن فعل العميل يشكل جريمة، ويخضع لقانون العقوبات، لكن اختلفوا فيما بينهم حول التكييف الصحيح، على النحو الآتي[1]:

-الرأي الأول : تصرف العميل جريمة سرقة

ذهب إلى القول بأن نشاط حامل البطاقة يشكل جريمة سرقة و قد انقسم الفقهاء القائلين لهذا الرأي إلى قسمين:

***الفريق الأول:** وهو القائل بأن تصرف العميل يشكل جريمة سرقة مستندا إلى أن جهاز الصراف الآلي هو آلة صماء و لا إرادة له ويقتصر دوره على تنفيذ تعليمات موظفي البنك ، وبالتالي لا يعتبر التسليم الصادر منه تسليما إراديا و اختياريا نافيا لفعل الأخذ الذي يقوم به جريمة السرقة [2].

كما ذهب أنصاره إلى تشبيه حالة العميل الذي يسحب مبلغا يزيد رصيده مستخدما، بحالة الدائن الذي يأخذ من المدين أكثر من حقه دون رضا مدينه، ومن ثم فإنه يعاقب على جريمة السرقة[3].

واستندوا أيضا إلى حكم محكمة جنح (Lille) الفرنسية التي أدانت شخصا بجريمة السرقة لأنه قام بإعطاء الآلة قطعة من النقود الأجنبية، أقل من العملة المحلية، وأخذ مقابلها كمية من المشتريات[4].

---

[1]- عمر سالم، مرجع سابق، ص 46.

[2]- سامح محمد عبد الحكيم، الحماية الجنائية لبطاقات الائتمان، درا النهضة العربية، القاهرة مصر، 2003، ص 66.

[3]- جميل عبد الباقي الصغير، الحماية الجنائية و التقنية لبطاقات الائتمان الممغنطة، دار النهضة العربية للنشر، القاهرة مصر، 2003

[4]- كما أدانت محكمة (Lyon) الفرنسية شخصا بتهمة السرقة لقيامه بسحب مبالغ نقدية تتجاوز رصيده في إدارة الشيكات . للتفصيل راجع جهاد رضا الحباشنة، مرجع سابق، ص 11.

كما استندوا إلى حكم محكمة ليون الفرنسية [1]، الذي أدانت فيه تصرف العميل بجريمة السرقة عند سحبه لمبالغ نقدية تجاوز رصيده ، و قد أسست المحكمة حكمها على مضمون الالتزام العقدي القائم بين العميل و إدارة الشيكات البريدية، هو عدم السحب إلا ضمن حدود الرصيد مما يعني أن تسليم المبلغ الزائد عن الرصيد هو تسليم غير اختياري تقوم به جريمة السرقة [2].

***الفريق الثاني:**

ذهب أصحاب هذا الفريق إلى أن تحقق وصف السرقة بحق العميل مرتبط بمضمون الالتزامات العقدية القائمة بين البنك و العميل، أي أن البنك إذا لم يشترط على عملية صراحة عند إبرام عقد منح البطاقة، أن لا يتجاوز رصيده عند إجراء عملية السحب النقدي من الجهاز فإن البنك مفاد هذا الشرط انعدام رضا المصرف عن فعل الأخذ، و بالتالي التسليم غير اختياري و تقوم به جريمة السرقة[3].

-الرأي الثاني : نشاط حامل البطاقة جريمة نصب

هذا الفعل جريمة نصب لأن العميل قد ادعى صفة غير صحيحة و هي أن له رصيد دائنا في المصرف[4]، ويستند هذا الرأي إلى حكم محكمة (Douai) الذي أدان حامل البطاقة بتهمة النصب، لأنه استخدم بطاقة الضمان خاصة ودفتر الشيكات في سحب أوراق من فرع آخر للبنك خلافا للفرع القائم بمسك حساب العميل.

---

[1]- كما قضت محكمة (Troyes) بقيام جريمة السرقة لقيام المتهم باستخدام بطاقة ممغنطة و إجراء عمليات سحب النقود متجاوزا رصيده . للتفصيل راجع عماد علي، مرجع سابق، ص 126.

[2] – وقد انتقد جانب من الفقه الذي ذهب إلى مخالفة العميل للالتزامات العقدية بينه و بين المؤسسة المالية مما يشكل المسؤولية العقدية و ليس الجزائية. للتفصيل راجع جهاد رضا الحباشنة، مرجع سابق، ص 113.

[3]– عماد علي الخليل، مرجع سابق، ص 123.

[4]-Raynaud(Monique) et,Deveze(jean).Droit bancaire quatrième édition Dalloz.1986. N09.River .

كما استند أنصاره إلى حكم محكمة جنح Angers بفرنسا، والتي اعتبرت جريمة نصب استنادا إلى أن حامل البطاقة ادعى صفة غير صحيحة، وهي رصيد دائن في البنك[1]،

لكن انتقد هذا الرأي على أساس أن التاجر يعلم بموجب العقد بالحد الأقصى الذي يلتزم به البنك و يضمن سداده، فالتاجر يعد متصرفا في هذه الحالة على مسؤولية، كما أن حامل البطاقة لم يخدع البنك أو يتحايل عليه بأي وسيلة من وسائل التدليس، بل تعسف في استخدام الحق الذي قدمه له البنك[2].

- الرأي الثالث : نشاط حامل البطاقة جريمة خيانة أمانة

يرى هذا الرأي أن هذا التصرف يشكل خيانة أمانة، لأن تسليم العميل بطاقة الوفاء كان مشروطا بوجود رصيد كاف في رصيده، وعليه استعمالها وفق شروط العقد المبرم بينه و بين البنك، و إلا أساء التصرف وقام بسحب مبلغ أكثر من رصيده، فيعد مرتكبا لجريمة خيانة الأمانة[3].

إلا أن هذا الرأي لا تؤيده الأغلبية، إذ يرى العديد من الفقهاء أن هذا الفعل لا يشكل خيانة أمانة، بل شكل إخلالا بالتزام عقدي، وليس و ليس أمام المصرف في هذه الحالة إلا مطالبة العميل المتعسف برد ما أخذه دون وجه حق مع التعويض عن الأضرار التي لحقت بالبنك إن كان لذلك مقتضى[4].

---

[1]- وعلى النقيض قضت محكمة استئناف ليون باستبعاد وصف النصب على تجاوز الرصيد، وقد فضت أيضا محكمة النقض الفرنسية المساواة في مجال النصب بين استعمال صفة غير صحيحة و مجرد الكذب الخاص بصفة المتهم كدائن. للتفصيل راجع سامح محمد عبد الحاكم، مرجع سابق، ص 70.

[2] - Cabrillac (M.) et Mouly (C.) , Droit pénal de la bancaire et du crédit, Masson, paris, 1982, P 365.

[3]- جميل عبد الباقي الصغير، الحماية الجنائية و التقنية لبطاقات الائتمان الممغنطة ، مرجع سابق، ص 22.

[4]- محمد أمين الشوابكة، مرجع سابق، ص 196.

ورفضت محكمة ليون الفرنسية تكييف هذه الواقعة بأنها تشكل كل جريمة خيانة أمانة، على أساس أنه يحق للبنك مالكها طلبها من العميل في أي وقت، وأن العميل لم يكتم البطاقة أو يبددها، بل ردها للبنك عندما طلبت منه، و أن هذا التعسف في استعمال البطاقة ليس فيه خروج عن الغرض الذي وجدت من أجله البطاقة[1].

ب- اتجاه تحميل حامل البطاقة المسؤولية المدنية:

يذهب أصحاب هذا الاتجاه إلى أن تجاوز حامل البطاقة لرصيده خلال فترة صلاحيتها، لا يشكل جريمة، ورفضوا إدخاله تحت أي نص من نصوص قانون العقوبات، بل كيفوه على أنه إخلال بالتزام عقدي قائم بين المصرف و العميل استنادا على حكم محكمة النقض الفرنسية، و هو الرأي الراجح الذي تميل إليه لكون العميل الذي تجاوز رصيده يعد مرتكبا خطأ عقديا عليه المسؤولية العقدية.

لقد حسمت محكمة النقض الفرنسية هذا الخلاف بحكم فاصل في1983/02/24 وذلك حيث قضت بأن تجاوز حامل البطاقة لرصيده، لا يدخل تحت إطار قانون العقوبات، بل هو مخالفة لشروط العقد ، وبالتالي يترتب عليه لمسؤولية عقدية [2].

وتجدر الإشارة إلى أن المشرع الجزائري لم يجرم جريمة تجوز حامل البطاقة لرصيده كما لم يتخذ الفقه والقضاء موقفا من تكييف هذه الواقعة لكن في الحقيقة نرى أنها لا تشكل ة المدنية العقدية [3].

---

[1]- جهاد رضا الحباشنة، مرجع سابق، ص 114.

[2]- عماد علي، مرجع سابق، ص 123.

[3] – يلاحظ أن المشرع الجزائري جرم تجاوز حامل الشيك لرصيده في المادة 374 من قانون العقوبات ، لكنها لا تطبق على بطاقات الدفع والسحب رغم أنها وسيلة وفاء مثل الشيك ، فهذا النص خاص بالشيك وبالتالي لا يمتد تطبيقه إلى هذه البطاقات انطلاقا من مبدأ الشرعية المنصوص عليه في المادة 01 من قانون العقوبات التي تنص على أنه لاجريمة ولا عقوبة ولا تدبير أمن بغير قانون .

2-تكييف استخدام الحامل الشرعي للبطاقة بعد إلغائها و انتهائها:

يتحقق قيام حامل البطاقة باستعمالها على الرغم من عدم صلاحيتها، إما بسبب انتهاء مدة صلاحيتها، و إما سبب قيام البنك بإلغائها.

أ- الاستخدام غير المشروع لبطاقة ائتمان ملغاة:

قد يحدث أن يقوم البنك مصدر بطاقة الائتمان بإلغائها كجزاء لسوء استخدامها من جانب العميل، وهنا يجب على العميل إعادة البطاقة للبنك مصدرها، وعدم استخدامها و إلا عد مرتكبا لجريمة الاستخدام غير المشروع لبطاقة ائتمان ملغاة [1].

-احتفاظ العميل بالبطاقة على الرغم من مطالبته بردها:

علاقة البنك بالعميل حامل البطاقة علاقة تعاقدية قائمة على عقد عارية الاستعمال وهو أحد عقود الأمانة، فإذا امتنع حامل البطاقة الملغاة ردها يشكل ذلك اختلاسا تقوم به جريمة خيانة الأمانة، ويكفي لتوافر الاختلاس أن ينكر الحامل وجود البطاقة في حيازته لكي يتخلص من التزامه بالرد، ولا يشترط قيامه استعمالها غم مطالبة البنك بها أو سحبها[2].

وقد اتجه القضاء في فرنسا متمثلا في محكمة ليون الفرنسية إلى تكييف الفعل على أنه جريمة خيانة الأمانة بقولها، يرتكب جريمة خيانة الأمانة حامل البطاقة (VISA) الذي على الرغم من مطالبة البنك المتكررة له بردها إلا أنه استمر في الاحتفاظ بها[3].

---

[1]- سليمان أحمد فضل، مرجع سابق، ص 174.

[2]- جميل عبد الباقي، الحماية الجنائية و التقنية لبطاقات الائتمان الممغنطة، مرجع سابق، ص 78.

[3]- وبالتالي يترتب على استخدام بطاقة وفاء ملغاة مسؤولية مدنية إلا في حالة احتفاظ العميل بالبطاقة على الرغم من مطالبته بردها، فتشكل جريمة خيانة أمانة ، كما تشكل جريمة نصب في حالة تواطؤ حامل البطاقة مع التاجر فتشكل الواقعة جريمة نصب ، وعليه مسؤولية الحامل مدنية إلا في حالتين ترتبان المسؤولية الجنائية . للتفصيل راجع سالم عمر، مرجع سابق، ص 63.

-استخدام البطاقة الملغاة في الوفاء:

يشكل استخدام البطاقة الملغاة في الوفاء للتجارة جريمة نصب [1]، حيث أن مجرد تقديم البطاقة إلى التاجر يهدف إلى الامتناع بوجود ائتمان و همي لا وجود له في الواقع، وليس مجرد كذب، خاصة و أن إلغاء البطاقة يخلع عنها قيمتها كأداة ائتمان، الأمر الذي يدفع البنك إلى تسديد قيمة السلع والخدمات إلى التاجر [2].

وقد قضت محكمة جنح باريس بإدانة حامل شرعي لبطاقة ائتمان بتهمة النصب لقيامه بتقديم بطاقة مجردة من أي قيمة، لأنها ملغاة بواسطة البنك مصدرها، وذلك بهدف الإقناع بوجود ائتمان وهمي، و الحصول من البنك على الوفاء للتاجر الذي قدم سلعا لحامل البطاقة مما يشكل استيلاء على بعض ثروة الغير [3].

ب -الاستخدام غير المشروع للبطاقة منتهية الصلاحية:

إن علاقة البنك مصدر البطاقة بالعميل عقدية، تنقضي بانتهاء المدة المتفق عليها وفي الحالة يجب على الحامل تسليمها، لمصدرها، لكن قد يحتفظ حامل البطاقة بها و يستخدمها في الوفاء للتجارة على الرغم من انتهاء مدة صلاحيتها.

ولا يشكل استخدام الحامل للبطاقة بعد انتهاء مدة صلاحيتها جريمة نصب باستخدام طرق احتيالية، حيث أن الكذب الصادر من الحامل ينصب على مدى صلاحية البطاقة لا على الاقتناع بوجود ائتمان وهمي، وتقديم البطاقة لا يكفي لتحقيق المناورة التي تقوم بها الطرق الاحتيالية، ويمكن اكتشافه بسهولة بمعرفة التاجر الذي يلتزم تعاقديا للاطلاع على تاريخ صلاحية

---

[1]- Gavala(c), le cartes de paiment et de credit, dalloz.1994.P.82

[2] - أما بالنسبة لاستعمال البطاقة الملغاة في سحب النقود، فلا يشكل أية جريمة أو حتى الشروع فيها لوجود استحالة مادية تتمثل في عدم استجابة جهاز الصراف الآلي لطلبه، إما سحب البطاقة أو رفض إتمام العملية . للتفصيل راجع جهاد رضا الحباشنة، مرجع سابق ، ص 129.

[3]- نائلة عادل قورة، مرجع سابق، ص 524.

المدون عليها و لذا يتحمل التاجر الضرر في حالة قبوله الوفاء باستخدام بطاقة منتهية الصلاحية[1].

أما إذا اتفق التاجر مع الحامل الشرعي للبطاقة على قبول الوفاء بالبطاقة منتهية الصلاحية أضرارا بالبنك، وذلك بأن يقوم التاجر بتزوير تاريخ انتهاء صلاحية البطاقة في الفاتورة أو يقوم بتقديم تاريخ عمليات الوفاء المنفذة، فهنا تتوافر الطرف الاحتيالية اللازمة لقيام جريمة النص فيسأل العميل بصفته فاعلا أصليا، و يعاقب التاجر كشريك له في جريمة النصب[2].

وبالتالي يسأل حامل البطاقة في حالة استخدامه لبطاقة وفاء منتهية الصلاحية مسؤولية مدنية لا جزائية، وكذلك التاجر يتحمل المسؤولية العقدية إلا في حالة تواطئه مع حامل البطاقة فإن يساءل جزائيا بجريمة النصب .

أما بالنسبة لموقف المشرع الجزائري فلم يشر إلى استعمال حامل بطاقات الدفع والسحب منهية الصلاحية ، كما لم يتخذ الفقه والقضاء موقفا من هذه المسالة ، لكن نرى أن هذه الواقعة ترتب المسؤولية العقدية كأصل ، والمسؤولية الجنائية في حالة عدم ردها رغم مطالبته برده كجريمة خيانة أمانة ، أوتواطؤه مع التاجر فيسآلان كلاهما عن جريمة النصب [3].

---

[1]- جهاد رضا الحباشنة، مرجع سابق ، ص 131.

[2]– عمر سالم، مرجع سابق، ص 79.

[3] – وهو الرأي الراجح في الفقه والقضاء الفرنسيين ، انطلاقا من إن علاقة البنك مصدر البطاقة بالعميل عقدية تنقضي بانتهاء المدة المتفق عليها وفي الحالة يجب على الحامل تسليمها، لمصدرها، لكن قد يحتفظ حامل البطاقة بها ويستخدمها في الوفاء للتجارة على الرغم من انتهاء مدة صلاحيتها. فيسآل مدنيا بالتعويض ، إلا إذا كان هناك خيانة أمانة، أو تواطؤ من التاجر مع حاملها فيترتب عليها المسؤولية المدنية .

ثانيا-الاستخدام غير المشروع لبطاقة الائتمان من قبل الغير:

إن الاستخدام غير المشروع لبطاقة الائتمان، قد يقع من حامل البطاقة، وقد يقع من الغير أي غير صاحب الرصيد [1].

ويتحقق بالاستخدام غير المشروع لبطاقة مسروقة أو مفقودة، أو تزوير البطاقة واستخدام بطاقة ائتمان مزورة، على التفصيل الآتي :

1-الاستعمال غير المشروع لبطاقة مسروقة أو مفقودة:

قد يتم الاستعمال غير المشروع لبطاقة مسروقة أو مفقودة بواسطة الغير إما لسحب النقود أو الوفاء بواسطتها للتجار، على النحو الآتي:

أ-الاستعمال غير المشروع لبطاقة مسروقة أو مفقودة لسحب النقود:

لا يمكن استعمال بطاقة مسروقة أو مفقودة لسحب النقود بدون إدخال الرقم السري أو الشفرة الخاصة بالبطاقة و التي لا يعلمها عادة سوى الحامل الشرعي للبطاقة، فمجرد الحيازة غير المشروعة للبطاقة لا يكفي لسحب النقود، بل يلزم أن يرتبط نشاط الفاعل بسرقة شفرة الطاقة أو الرقم السري[2].

ولم تثر هذه الحالة خلافا في الفقه حول التكييف القانوني لها، حيث استقر الرأي على أن الواقعة تشكل جريمة نصب[3]، و قد استبعدت السرقة، حيث أن الجهاز قد تمت برمجته لتسليم النقود بع إدخال البطاقة و تدوين الرقم السرين فالتسليم كان إراديا، غلا أنه يمكن أن تنسب إليه سرقة

---

[1]- إذا سرقت البطاقة أو فقدت، فإن مالك الطاقة الشرعي بمجرد إبلاغه لمدرها بفقدها أو سرقتها بفقد حقه كمالك من هذه اللحظة، وينظر إليه على أنه من الغير.

[2]- سامح محمد، مرجع سابق، ص 81.

[3]- وقد قضت محكمة النقض الفرنسية بتوافر أركان جريمة النصب في حق الحامل الشرعي للطاقة إذ استعملها بعد الإعلان الكاذب عن سرقتها و فقدها.و لمزيد من التفصيل راجع:

Cabrillac (M.) et Mouly(c.) op. cit; p.239-240.

البطاقة أو رقمها السرين حيث يرتكب الجاني جريمتين مستقلتين ،وهما السرقة كجريمة وسيلة و النصب كجريمة غاية[1].

ب-الاستعمال غير المشروع لبطاقة مسروقة أو مفقودة في الوفاء:

ويبدو استعمال الطاقة في هذه الحالة أيسر من الحلة السابقة، حيث لا يقتضي الأمر في كثير من الحالات معرفة الرقم السري للبطاقة، بل تتم المعاملة بتوقيع حامل البطاقة على فاتورة الشراء ، ومن ناحية أخرى لا يمكن اكتشاف تزوير التوقيع من قبل البائع لعدم خبرته .

وقد استقرت العديد من الأحكام القضائية الفرنسية و الآراء الفقهية على معاقبة من يستخدم بطاقة مسروقة أو مفقودة في الوفاء بجريمة النصب، على اعتبار أن المتهم انتحل اسما كاذبا و هو اسم الحامل اشرعي للبطاقة [2].

وبالتالي فقد استخدم وسائل احتيالية من أجل الاستيلاء على أموال الغير، وتكتمل الجريمة بحدوث عملية التسليم ، ولكنها قد تقف عند الشروع إذا لم يسلم المال لسبب خارجي[3].

وقد يحدث أن يكون هناك تعدد مادي مع الارتباط بين جريمة النصب و جريمة أخرى كالسرقة أو التزوير، أو إخفاء أشياء مسروقة، ففي هذه الحالة تطبق عقوبة الجريمة ذات الوصف الشد و مثال على ذلك ما قضت به محكمة استئناف باريس بإدانة متهم عن جريمة إخفاء أشياء مسروقة بالإضافة إلى النصب[4].

---

[1]- نائلة عادل قورة، مرجع سابق، ص 541.

[2] - وفي ذلك قضت محكمة النقض الفرنسية أنه يعد مرتكبا لجريمة نصب الجاني الذي يحصل عل سلع أو خدمات من التاجر و دفع له الثمن بمقتضى بطاقة مسروقة، لأنه يكون بذلك قد اتخذ اسما كاذبا، وهو اسم صاحب البطاقة الشرعي.

[3]- سامح محمد، مرجع سابق ، ص 84-85.

[4]- سلمان أحمد فضل، مرجع سابق، ص 176.

2-تزوير بطاقة الائتمان:

يعد تزوير بطاقات الائتمان من أخطر التزوير المعلوماتي، ولقد ثار خلاف فقهي بشأن تطبيق أحكام جريمة التزوير على بطاقات الائتمان، وانقسم الفقه إلى فريقين:

أ-الاتجاه الأول:

ذهب أنصاره إلى القول بعدم إمكانية تطبيق النصوص التقليدية لجريمة التزوير البيانات الإلكترونية ، ومنها بيانات بطاقة الائتمان، بحجة عدم إمكانية القراءة البصرية لمحتويات هذه المحررات الالكترونية إلا بواسطة الحاسوب والتزوير يفترض تغييرا في علامات أو رموز مرئية[1].

وقد أيد هذا الرأي للفقيه الألماني (UirichSiber) الذي يرى أن تزوير البيانات الإلكترونية لا يمكن أن ينطوي تحت النصوص التقليدية لجريمة التزوير، لأنه لا يمكن قراءتها بصريا، كما يرى الفقيه الفرنسي (Cassin) أن جريمة التزوير بمفهومها التقليدي لاتقوم لانتفاء الكتابة [2].

ب-الاتجاه الثاني:

يرى أصحابه قيام جريمة التزوير أن حدث تغيير في بيانات بطاقات الائتمان استنادا إلى أن المعلومات المعالجة إلكترونيا متى دونت على أسطوانات أو شريط ممغنط تعتبر محررا، فإذا كان

---

[1]- حماد رضا الحباشنة، مرجع سابق، ص 72. انظر أيضا:

Devez(Jean.) Op. cit. p.328,

[2]- فكرة المعالجة الإلكترونية لمدة البيانات و المعلومات، لا تعبر عن فكرة بشرية، بل هي محض فكرة ميكانيكية للآلة القارئة البيانات الإلكترونية المخزنة في الشرطة الممغنطة لا يمكن قراءتها إلا بالحاسوب، وذك ينفي عنها صفة المحرر. للتفصيل راجع علي، مرجع سابق، ص 61-62.

من غير الممكن قراءته بصريا، إلا أنه يمكن قراءته عن طريق الحاسوب ، وبالتالي فإن تغيير الحقيقة في هذه المحررات الإلكترونية يؤدي إلى قيام الركن المادي لجريمة التزوير[1].

ونحن بدورنا نميل إلى الرأي الثاني القائل بتوافر جريمة التزوير على بطاقات الائتمان، لكون نصوص جريمة التزوير جاءت عامة هذا من جهة، ومن جهة أخرى عدم إمكانية القراءة البصرية للمحررات لا ينفي عنها صفة المحرر.

وأمام هذا الاختلاف الفقهي الكبير نصت بعض التشريعات على التزوير المعلوماتي بتعديل نصوصها القائمة، كما هو الحال في التشريع الكندي الصادر عام 1985، والتشريع الأسترالي لعام 1983، أو بإصدار نصوص خاصة، كما هو الحال بالنسبة للمشرع الفرنسي الذي استحدث قانون أمن الشيكات وبطاقات الوفاء رقم 1382/91 لسنة1991، حيث كفل به حماية جزائية خاصة لبطاقة الوفاء عن التقليد و التزوير و استعمال البطاقة المقلدة أو المزورة، و قبول الدفع ببطاقة الوفاء على الرغم من علمه بتقليد البطاقة أو تزويرها، بموجب المادة 1331/67[2].

3-استعمال بطاقة ائتمان مزورة:

لقد اختلف الفقه والقضاء في تكييف استعمال بطاقة ائتمان مزورة، كالآتي:

أ-الاتجاه الأول:

يرى هذا الاتجاه أن هذه الواقعة تشكل جريمة سرقة باستعمال مفتاح مصطلح لأن المال خرج من ذمة صاحبه دون رضائه، و المفتاح المصطنع في هذه الحالة هو البطاقة المزورة ، ويؤيد

---

[1]- من غير المنطقي القول بتوافر التزوير في حالة تغيير الحروف والأرقام المطبوعة على البطاقة وعدم توافره إذا وقع على إحدى البيانات المعالجة إلكترونيا على البطاقة نفسها .

[2]- يمكن توفير حماية جزائية عامة في إطار القواعد العامة من قانون العقوبات من خلال نصوص جرائم الأموال كالسرقة والنصب والاحتيال وخيانة ألأمانة ، بالإضافة إلى هذه الحماية كفل المشرع الفرنسي حماية جنائية خاصة وجريمة التزوير خاصة لبطاقة الوفاء من قانون أمن الشيكات وبطاقات الوفاء رقم 1382/91 لسنة1991، في المادة 1331/67 من خلال تجريم تقليد و تزوير و استعمال بطاقات الوفاء المقلدة أو المزورة، و كذا قبول الدفع ببطاقة الوفاء على الرغم من علمه بتقليد البطاقة أو تزويرها، للتفصيل راجع عماد علي خليل، مرجع سابق ص 67/66.

هذا الفقه رأيه بأن قانون العقوبات لم يحدد مفهوم المفتاح المصطنع[1] ،
الفقهاء المفتاح المصطنع، بأنه كل أداة تقوم بذات الوظيفة التي يقوم بها المفتاح الأصلي بغض النظر عن شكلها أو حجمها أو مادة صنعها ويدخل في حكمه كافة الأدوات التي تستخدم في فتح الأقفال ومنها الأدوات المزورة التي كانت أداة للوصول إلى سحب النقود أو كأداة وفاء[2].

لكن رفض جانب من الفقه التسليم بفكرة السرقة باستعمال مفتاح مصطنع، على أساس أن الأمر يتعلق بتسليم إرادي ، مما ينفي الاختلاس ولا يمكن تشبيه بطاقة الائتمان بالمفتاح المصطنع الذي هو كل أداة مخصصة لفتح الأقفال التي تغلق أبواب الأماكن ،كما ذهب إلى أن اعتبار بطاقة الائتمان بمثابة مفتاح مصطنع يتعارض مع قاعدة عدم جواز القياس في التجريم أن القول بأننا بصدد سرقة باستخدام مفتاح مصطنع نقود من الناحية العملية إلى إلغاء جريمة استعمال محرر مزور في كل حالة يستخدم فيها عند المحرر للاستيلاء على مال الغير[3].

ب-الاتجاه الثاني:

يتجه هذا الاتجاه إلى اعتبار واقعة استعمال بطاقة ائتمان مزورة تشكل جريمة احتيال و نصب، إذ يتخذ الجاني اسم كاذب وصفة غير صحيحة المالك الحقيقي للحصول على منفعة مادية.

فقد قضت محكمة (Rennes) بأن استخدام البطاقة المزورة يشكل جريمة نصب ، وعلى العكس قضت محكمة (Lille) بأن هذا الفعل لا يشكل جريمة نصب، لأن الطرق الاحتيالية تتم بين شخصين، الجاني و المجني عليه، بينما هذه الحالة العلاقة بين شخص و شيء هو الجهاز

---

[1] – لم يحدد قانون العقوبات الجزائري المقصود بالمفتاح المصطنع، وكذلك قانون العقوبات المصري، والفرنسي .

[2]– جهاد رضا الحباشنة، مرجع سابق، ص87-88.

[3]- واستند أيضا إلى أن الأمر يتعلق بتسليم إيرادي مما ينفي الاختلاس كعنصر مكون بجريمة السرقة
ولا يمكن تشبيه بطاقة الائتمان بالمفتاح المصطنع الذي هو كل أداة مخصصة لفتح أقفال أبواب الأماكن. واعتبار بطاقة الائتمان بمثابة مفتاح مصطنع يتعارض مع قاعدة عدم جواز القياس في التجريم ، أن القول بأننا بصدد سرقة باستخدام مفتاح مصطنع نقود من الناحية العملية إلى إلغاء جريمة استعمال محرر مزور في كل حالة يستخدم فيها عند المحرر للاستيلاء على مال الغير.

ولكن قضت محكمة النقض الفرنسية قضت بأنه يمكن خداع الجهاز الآلي لأنه يوجد خلف الجهاز صاحبه[1].

ج-الاتجاه الثالث:

وفقا للرأي الراجح في الفقه الفرنسي، يسأل من استعمل بطاقة ائتمان مزورة عن جريمة استعمال محرر مزور[2].

وأخذ بهذا الرأي المشرع الفرنسي، حيث عاقب على جريمة استعمال محرر مزور في قانون الغش المعلوماتي لعام 1988 بموجب المادة 6/462 و في قانون العقوبات الجديد المعمول به في سنة 1994 بموجب المادة 1/441، وجاءت هذه الحماية الجنائية عامة[3]، على خلاف قانون 1382/91 الصادر في عام 1991 المتعلق بأمن الشيكات و بطاقات الوفاء[4]، والذي جاء بحماية جنائية خاصة لبطاقات الوفاء من التزوير و استعمال محرر مزور، حيث عاقب المشرع على جريمة استعمال محرر مزور في المادة 2/67 [5].

تقوم هذه الجريمة على ركن شرعي و ركن مادي متمثل في فعل استعمال بطاقة مزورة ، وركن معنوي يتخذ صورة القصد الجنائي العام بعنصريه العلم والإرادة بأن يكون الجاني عالما بأن البطاقة التي يستعملها مزورة أو مقلدة، وتتجه إرادته إلى ارتكاب ذلك الفعل المجرم[6].

---

[1]- جميل عبد الباقي، الحماية الجنائية و التقنية لبطاقات الائتمان الممغنطة، مرجع سابق ، ص 111.

[2]- عمر سالم، مرجع سابق، ص 37. وأنظر أيضا: Gavala(c.),op. cit., p.92

[3] – عماد علي، مرجع سابق، ص 74 وما بعدها.

[4] _ قانون 91 رقم /1382 الصادر في عام 1991 المتعلق بأمن الشيكات و بطاقات الوفاء الفرنسي.

[5]- تنص المادة 2/67 من قانون أمن الشيكات و بطاقات الوفاء على أنه " يعاقب بالحبس من عام إلى سبعة أعوام، و العامة من 3600 إلى 500ألف فرنك، و بإحدى هاتين العقوبتين كل من استعمل أو حاول استعمال بطاقة مزورة أو مقلدة و هو عالم بذلك" .

[6]- عمر سالم، مرجع سابق، ص 80 وما بعدها.

ويلاحظ أن المشرع الفرنسي عاقب على الشروع في استعمال بطاقة مزورة أو مقلدة بنفس العقوبة المقررة للجريمة التامة، ويتحقق الشروع بفضل المتهم في تحقيق النتيجة الإجرامية المترتبة على هذا الاستعمال و على الحصول على الخدمة أو السلعة أو النقود[1].

الفرع الثاني: الحماية الجنائية للتوقيع الكتروني

مع التقدم التكنولوجي في وسائل الاتصال والمعلومات، فلم يعد التوقيع التقليدي ملائمة للمعاملات الالكترونية، لذلك ظهر التوقيع الإلكتروني كبديل عن التوقيع التقليدي ليتوافق وطبيعة المعاملات الالكترونية، ويعد التوقيع الإلكتروني أحد الوسائل الأساسية في تنظيم الخدمات المصرفية الإلكترونية فالكثير منها يستند إلى التوقيع الإلكتروني في إثباتها وقبولها، إذ تستلزم عقود التجارة الإلكترونية لصحة تمامها توقيع الأطراف المتعاقدة [2].

أولا- ماهية وحجية التوقيع الإلكتروني :

سنتطرق إلى ماهية التوقيع الالكتروني من خلال تعريفه وصوره ، وحجيته على النحو الآتي :

1-ماهية التوقيع الإلكتروني:

سنتطرق إلى ماهية التوقيع الالكتروني من خلال تعريفه في القوانين الأجنبية ، وبعض القوانين العربية ، ثم نتعرض إلى صوره، على التفصيل الآتي :

---

[1]- جهاد رضا، مرجع سابق، ص 84 وما بعدها.

[2] -ويهدف التوقيع الإلكتروني إلى الحفاظ على سرية المعلومات أو الرسائل المرسلة، و عدم قدرة أي شخص آخر على الاطلاع أو تعديل المعلومات ، كما أنه يحدد هوية المرسل و المستقبل، ويتم التأكد عن طريقه من صدق و صحة المعلومات .

أ- تعريف التوقيع الإلكتروني:

عرفت المادة 4/1316 من القانون المدني الفرنسي[1]، التوقيع الذي يتم باستخدام وسيلة الكترونية آمنه لتحديد هوية الموقع وضمان صلته بالتصرف الذي وقع عليه [2].

"صوت أو رمز أو معالجة
إلكترونية مرفقة أو متحدة بعقد أو بغيره من السجلات يتم تنفيذها أو إقرارها من شخص تتوافر لديه نية التوقيع على السجل[3].

وعرف المشرع في ولاية نيويورك للتوقيع الإلكتروني بموجب قانون صادر في 6 أغسطس سنة 2002 على أنه"التوقيع الإلكتروني هو صوت أو رمز أو معالجة إلكترونية ملحقة بسجل إلكتروني أو متحدة منطقيا به ويجريها أو يقرها شخص تتوافر لديه نية التوقيع في هذا السجل"[4].

ويتماثل هذا التعريف مع القانون الاتحادي الأمريكي، كما أنه يكاد يتماثل مع التعريف الذي أورده الشارع الإنجليزي للتوقيع الإلكتروني ، إذ نص الفصل الأول من لائحة التوقيع الإلكتروني

---

[1] – المعدلة والمضافة بقانون التوقيع الإلكتروني الفرنسي 23/ 2000 الصادرفي2000/3/13.

[2]-La loi no 2000-2230 du 13 mars 2000, J.O.14 mars 2000.P.3986.J.C.P.2000,III , 20259.
"an electronic sound, symbol, or process" that is attached to or logically associated with" a contract or other record, and that is "executed or adopted by a person with the intent to sign the record. "E-Sign Law 106.

[3]-Report to the Governor and Legislature on New York State's Electronic Signatures and Records Act, p. 11.

[4]- "Electronic signature" shall mean an electronic identifier, including with out limitation a digital signature, which is unique to the person using it, capable of verification, under the sole control of the person using it, attached to or associated with data in such a manner that authenticates the attachment of the signature to particular data and the integrity of the data transmitted, and intended by the party using it to have the same force and effect as the use of a signature affixed by hand". ESRA 102 (3). Report to the Governor and Legislature, p. 7 note 3.

الصادرة في 8 مارس 2002 على أن التوقيع الإلكتروني يعني بيانات في شكل الكتروني ملحقة أو متحدة منطقيا بغيرها من البيانات الإلكترونية والتي تصلح كوسيلة للتوثيق"[1].

كما أنه يكاد يتطابق مع التعريف الذي نص عليه الشارع الألماني في المادة الثانية من قانون التوقيع الإلكتروني [2].

ويلاحظ أن اتجاهات التشريعات المقارنة تتجه إلى التوسع في الوسائل التي تصلح لإجراء التوقيع الإلكتروني، وعلة ذلك هي توفير مرونة أكبر للمتعاملين في اختيار الوسيلة التي يرونها تكفل الأمن والثقة في هذا التوقيع[3].

غير إنه إذا كانت للمتعاملين حرية اختيار الوسيلة الفنية للتوقيع الإلكتروني؛ فإن الجهات العامة قد يفرض عليها القانون استخدام وسيلة معينة دون غيرها في التصرفات التي تدخل فيها مع الغير أو فيما بينها، وعلة ذلك أن هذه الوسيلة قد يتوافر فيها قدر من الحماية للمصلحة العامة أكثر من غيرها، والسلطة التي بيدها تحديد وسيلة التوقيع الإلكتروني في هذه الحالة هي السلطة الإدارية [4].

"بيانات في شكل الكتروني مدرجة في رسالة بيانات أو مضافة إل

---

[1]- Electronic signature shall mean an electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record."Laws of 2002, Chapter 314, 2.

[2]- Report to the Governor and Legislature on New York State's Electronic Signatures and Records Act, p. 7 note 4.

[3]–"Electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication". Statutory Instrument 2002 No. 318, The Electronic Signatures Regulations 2002, op-cit. Draft of a Law on the Framework Conditions, (2), P. 4

[4] -Report to the Governor and Legislature on New York States Electronic Signatures and Records Act, p.7-8.

أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ولبيان موافقة الموقع على معلومات رسالة البيانات[1]".

أما المشرع الجزائري فلم يعرفه، واكتفى في الفقرة 02 من المادة 37 ق م بالنص على أنه " بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر 1 " [2].

" ما يوضع على محرر إلكتروني ويتخذ
شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ، ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره"[3].

ويقصد به وفقا للمادة 2 من قانون المعاملات الالكترونية الأردني ،البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها وتكون مدرجة بشكل الكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة في رسالة معلومات أو مضافة عليها أو مرتبطة بها ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره من اجل توقيعه وبغرض الموافقة على مضمونه[4].

" مجموعة من الإجراءات
التقنية التي تسمح بتحديد من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته"[5].

---

[1] – نهلا عبد القدر مومني ، الجرائم المعلوماتية ، دار الثقافة ، عمان الأردن، 2008، ص 135.

[2]– محمد رايس ، حجية الإثبات بالتوقيع الالكتروني طبقا لقواعد القانون المدني الجديد ، محاضرات ألقيت على طلبة ماجستير –مسؤولية مهنية– كلية الحقوق جامعة تلمسان ، 2009، ص02

[3] – القانون 15/04 الصادر في 2004/4/22 المتعلق بالتوقيع الإلكتروني ، ج رع 71 في 2004/4/22.

[4] – وفي هذا المقام لا بد من التفريق بين التوقيع الالكتروني والتوقيع الرقمي ، إذ وفق البيان المتقدم فان التوقيع الالكتروني يكون بأية صورة بما فيها الرسم الضوئي ، في حين إن التوقيع الرقمي (والذي يصنعه برنامج خاص) هو مجموعة مزايا رقمية مأخوذة من جسم الرسالة المرسلة تنقل بشكل مشفر ويتبين من فك تشفيرها مدى صحة أو عدم صحة التوقيع .

[5] - DAVIO (E) , internet face au droit ,cohiers du C.R.I.D. story – scientica, 1997 , P. 80.

كما عرفه بعض الفقهاء المصريين بأنه" كل إشارات أو رموز أو حروف مرخص بها من الجهة المختصة باعتماد التوقيع ومرتبطا ارتباطا وثيقا بالتصرف القانوني ، ويسمح بتمييز صاحبها وتحديد هويته ، ويتم دون غموض عن رضائه بهذا التصرف القانوني"[1].

ب- صور التوقيع الإلكتروني:

يتخذ التوقيع الإلكتروني أشكالا عدة بحسب الوسيلة أو التقنية التي تستخدم في إنشائه، لاسيما وأن القوانين التي نظمته لم تنص على شكل محدد له ، وأن كانت قد حددت ضوابطه العامة .

وتتمثل أهم صور التوقيع الإلكتروني في التوقيع الرقمي، والتوقيع البيومترى والتوقيع باستخدام القلم الإلكتروني وأخيرا التوقيع الرقمي.

- التوقيع الرقمي أو الكودي:

يقصد به استخدام مجموعة من الأرقام أو الحروف أو كليهما ، يختارها صاحب التوقيع لتحديد هويته وشخصيته ، ويتم تركيبها أو ترتيبها في شكل كودي لا يعلمها إلا صاحب التوقيع فقط ومن يبلغه بها[2]، والتوقيع الرقمي يقوم على ترميز المفاتيح ما بين مفتاح عام[3] ، وآخر خاص[4]،

---

[1] – ثروت عبد الحميد ، مرجع سابق ، ص 50.

[2] – غالبا ما ترتبط بالبطاقات الذكية ، البلاستيكية الممغنطة ، وغيرها من البطاقات الحديثة المشابهة والمزودة بذاكرة إلكترونية كبطاقة الفيزا والمستر كارت وأمريكان اكسبريس. للتفصيل راجع إبراهيم الدسوقي،الجوانب القانونية للتعاملات الإلكترونية ، مجلس النشر العلمي ، جامعة الكويت 2003 ، ص 158 .

[3] – المفتاح العام عبارة عن أداة إلكترونية متاحة للكافة ، تنشأ بواسطة عملية حسابية خاصة وتستخدم في التحقق من شخصية الموقع على المحرر الإلكتروني ، وللتأكد من صحة وسلامة محتوى المحرر الإلكتروني الأصلي . ممدوح محمد على مبروك ، المرجع السابق ص 17.

[4] – المفتاح الخاص عبارة أداة إلكترونية خاصة بصاحبها ، تنشأ بواسطة عملية حسابية خاصة وتستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية ، ويتم الاحتفاظ بها في بطاقة ذكية مؤمنة .

وهذه المفاتيح تعتمد في الأساس على تحويل المحرر المكتوب من نمط الكتابة الرياضية إلى معادلة رياضية ، وتحويل التوقيع إلى أرقام ، فإضافة التوقيع إلى المحرر عن طريق الأرقام يستطيع الشخص قراءة المحرر والتصرف فيه ، ولا يستطيع الغير التصرف فيه إلا عن طريق هذه الأرقام[1] .

من شأن هذه الطريقة للتوقيع الإلكتروني أن تحقق الثقة والأمان للمحرر وتضمن تحديد هوية الأطراف بدقة ، والعيب الوحيد في هذه الطريقة يتمثل فقط في حالة سرقة هذه الأرقام من قبل .[2]

-التوقيع بالقلم الإلكتروني:

يعد هذا النوع من التوقيعات الإلكترونية الأكثر شيوعا، ويتم فيه نقل التوقيع المحرر بخط اليد على المحرر المراد نقله إليه باستخدام الماسح الضوئي [3].

وتم تطوير هذا النوع من التوقيع باستخدام قلم إلكتروني حسابي يمكنه الكتابة على شاشة الحاسوب عن طريق استخدام برنامج خاص بذلك، يقوم بالتقاط التوقيع والتحقق من صحته، وقبوله إذا كان صحيحا ، أو رفضه إذا كان غير ذلك .

كانت تمتاز بالمرونة والسهولة في الاستعمال ، إلا أنها قد تؤدي في بعض الأحيان إلى زعزعة الثقة ، لأنه باستطاعة الشخص المستقبل الاحتفاظ بهذا التوقيع ووضعه

---

[1] – محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع للإنترنت ، مرجع سابق ص 241.

[2] – ويحتاج التوقيع الإلكتروني الرقمي باستخدام تقنية شفرة المفتاحين العام والخاص إلى سلطة إشهار أو جهة تصديق إلكتروني مرخص لها أو معتمدة ، تقوم بالتحقق من هوية الأشخاص المستخدمين لهذا التوقيع الرقمي والتأكد من نسبة المفتاح إلكتروني ،تفيد صحة توقيع العملاء بموجبها ، وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع.

[3] – نهلا عبد القدر مومني ، مرجع سابق، ص 137.

على مستندات أخرى ، كما أنه لا يمكن التأكد من أن الشخص صاحب التوقيع هو من قام بالتوقيع على المحرر لأنه باستطاعة أي شخص أن يضع هذا التوقيع ، إذا حصل عليه [1].

-التوقيع البيومترى (باستخدام الخواص الذاتية):

يعتمد هذا النوع من التوقيع على طرق التحقق من الشخصية التي تعتمد على الخواص الفيزيائية والطبيعية والسلوكية للأفراد ، ويتم التحقق من الشخصية بأخذ صورة دقيقة جدا للعين البشرية ، أو بصمة الأصابع ، أو ملامح الوجه وفي كل حالة يتم تخزين البيانات الخاصة في الحاسب الآلي واسترجاعها متى دعت الحاجة إليها للتأكد من شخصية صاحبها، والسماح له الدخول إلى نظام الحاسوب[2].

2- حجية التوقيع الإلكتروني في الإثبات :

إن شيوع عمليات التجارة الالكترونية وتنامي استخدام السندات والعقود الالكترونية التي تفرض هذا التوقيع.

بالأمم المتحدة (بموجب القرار رقم 162/51 تاريخ 16/1/1996، بالقوة الثبوتية للسند والتوقيع كما اعترف التوجيه الصادر عن البرلمان الأوروبي بتاريخ 1999/12/13 بالتوقيع الالكتروني وحث الدول الأعضاء على تسهيل استعماله من أجل حسن سير العمل في السوق الأوروبي[3].

---

[1]- محمد عبيد الكعبي ،الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، مرجع سابق ص239.

[2] – ويعد من أشهر أنواع التواقيع الإلكترونية ، ويقصد به بيان أو معلومة يتصل بمنظومة بيانات أخرى أو صياغة منظومة في صورة شفرة ، والذي يسمح للمرسل إليه إثبات مصدرها ، والتأكد من سلامة مضمونها . للتفصيل راجع ممدوح محمد على مبروك، مرجع سابق ، ص 12 . محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت ، مرجع سابق ، ص 23.

[3] – و 2000/6/8 حول التجارة الالكترونية والتأكيد على الاهتمام بتوقيع العقود بالطرق الالكترونية. راجع نهلا عبد القدر مومني ، مرجع سابق، ص 146.

واعترف أيضا بحجية التوقيع الالكتروني قانون الأونسترال النموذجي بشأن التوقيعات الالكترونية، الذي اعتمدته لجنة القانون التجاري الدولي لدى الأمم المتحدة في دورتها ال34 بتاريخ 5/7/2001، لتنظيم التوقيع الالكتروني .

أما على صعيد التشريعات الداخلية نجد أن كثيرا من الدول عملا بتوصيات لجنة اليونسترال عدلت في قوانينها ونصت على حجية الدليل الإلكتروني ومساواته بالدليل العادي[1]، أهمها بريطانيا عام 1995، وألمانيا وايطاليا 1997، والولايات المتحدة الأمريكية ، وفرنسا عام 2000، وتونس عام2000، ومصر لعام 2004.

كما اعترف المشرع الجزائري بالتوقيع الإلكتروني في المادة2/327 من قانون10/05[2]، والتوقيع المحمي طبقا للمادة 02 من المرسوم 272/2001 هو الذي أعطى له القانون قرينة قانونية مفترضة على صحته إلى غاية إثبات العكس[3] .

---

[1]- هناك بعض التشريعات كتشريع الكبك (Québec) أعطت حجية أقل للمحرر الإلكتروني مقارنة بالدليل الكتابي العادي. وانظر أيضا :

Rapport fait sur le projet de loi portant adaptation du droit de la preuve aux technologies de l information et relatif à la signature électronique , par M. Christian Paul (député)

[2] – نصت المادة2/327 ق م ج على أنه يعتد بالتوقيع الالكتروني وفق الشروط المذكورة في المادة 323 مكرر1 ، والمتمثلة في إمكانية التأكد من هوية مصدرها وأن تكون معدة ومحفوظة في ظروف أنة سلامتها .

[3] - Article (2) du décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, stipule que < La fiabilité d' un procède de signature électronique est présumée jusqu'a preuve contraire lorsque ce procède met en œuvre une signature électronique sécurisée , établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification du cette signature repose sur l'utilisation d'un certificat électronique qualifié "

ثانيا- جرائم الاعتداء على التوقيع الإلكتروني:

نظرا لخطورة جرائم الاعتداء على التوقيع الإلكتروني، كفلت لها بعض التشريعات الأجنبية والعربية حماية جنائية كالآتي:

1- جرائم الاعتداء على التوقيع الالكتروني في التشريعات الأجنبية:

وفرت بعض التشريعات الأجنبية حماية جنائية للتوقيع الالكتروني ومن أبرزها التشريع الفرنسي في إطار قانون العقوبات ، وفي التشريع الأمريكي في إطار قانون جرائم الكمبيوتر الفيدرالي.

أ-جرائم الاعتداء على التوقيع الالكتروني التشريع الفرنسي:

أصدرت فرنسا بتاريخ 13 /2000/3 قانونا خاصا بالتوقيع الإلكتروني رقم 230 لسنة 2000 في صورة تعديل للنصوص المنظمة للإثبات في القانون المدني الفرنسي بما يجعلها متوافقة مع تقنيات المعلوماتية، وكثرة استخدام التوقيع الإلكتروني في المعاملات الإلكترونية وقد أدرج هذا التعديل في نص المادة 1316 من القانون المدني الفرنسي في ست فقرات [1].

ماية جنائية خاصة للتوقيع الالكتروني بل تركها للنصوص العامة[2]، وبالرجوع لها نجد أنه تطبق عليه جرائم الاعتداء على النظام المعلوماتي وبياناته الواردة في المواد 1/323-7/323 وجريمة التزوير المعلوماتي في المادة 441 من قانون العقوبات الفرنسي [3]:

---

[1] - لقد كرس هذا القانون مبدأين أساسين: الأول ينصرف إلى عدم التميز بين الكتابة المعدة للإثبات بسبب الدعامة التي تتم عليها و الوسيط الذي تتم من خلاله، والثاني ينصرف إلى المساواة الوظيفية بين التوقيع الإلكتروني والتوقيع التقليدي ، للتفصيل راجع عبد الحميد ثروت ، مرجع سابق ، ص 173 .

[2] - نص المشرع الفرنسي على الجرائم المعلوماتية في المواد 1/323-7/323والمادة 441 من قانون العقوبات الفرنسي

[3] - أيمن رمضان محمد، التوقيع الإلكتروني، رسالة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق بجامعة عين شمس 2010، ص 167.

-الاعتداء على النظام المعلوماتي للتوقيع الالكتروني وبياناته :

يوفر المشرع الفرنسي حماية جنائية للنظام المعلوماتي ومحتوياته في المواد 323/1-323/7 من قانون العقوبات ، وباعتبار التوقيع الالكتروني نظام معلوماتي ، فيعاقب بالدخول أو البقاء غير المشروع على قاعدة بيانات التوقيع الالكتروني ، والاعتداء على سلامته بـ التوقيع ، ويعاقب أيضا على التلاعب ببيانات التوقيع الالكتروني .

***الاعتداء على النظام المعلوماتي للتوقيع الالكتروني:**

الدخول أوالبقاء غير المشروع :

يتمثل الركن المادي في الدخول أو البقاء غير المشروع في قاعدة بيانات تتعلق بالتوقيع الإلكتروني، وتصنف هذه الجريمة من جرائم الخطر حيث يتم تجريم السلوك دون توقف ذلك على نتيجة معينة ، فهذه الجريمة ليست من جرائم الضرر التي يشترط فيهاالحاق ضرربالمجني عليه[1].

وتعد هذه الصورة من الجرائم العمدية وبالتالي فإنه لا يتصور وقوعها بطريق الخطأ ، وصورة الركن المعنوي فيها هو القصد الجنائي العام .

:

نص عليها المشرع الفرنسي في المادة 323/ف 2، ويتمثل الركن المادي لهذه الجريمة *في التعطيل والتوقيف*[2] ، أو بإفساده بأي وسيلة ، ويبدو ذلك أمر منطقيا بالنظر لتعدد الوسائل ولغلبة الصبغة التقنية عليها بحيث يعسر حصرها أو تبويبها[1].

---

[1] – عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص296.

[2] -Gassin ®, Op.cit, P34.-

هذه الجريمة من الجرائم العمدية يتطلب فيها الأمر توافر القصد الجنائي العام عنصريه العلم والإرادة ، وهو ما يستفاد من المادة 323/ف.

وبالتالي إذا ترتب إفساد أو تدمير سير النظام عن خطأ أو إهمال، فلا وجود لجريمة، مثال ذلك الشخص الذي يستعمل اسطوانة ممغنطة تحتوي على فيروس مدمر، دون علمه بوجوده [2].

***الاعتداء على بيانات التوقيع الالكتروني :**

نص المشرع الفرنسي على جريمة التلاعب ببيانات النظام المعلوماتي بموجب المادة 2/323 من قانون العقوبات الفرنسي .

يتمثل الركن المادي لهذه الجريمة
الالكتروني ، أو إزالة ومحو بيانات التوقيع أوتغيير بياناته[3].

أما الركن المعنوي لهذه الجريمة فيتمثل في القصد الجنائي العام، بعنصريه العلم والإرادة، ولا يشترط توافر القصد الخاص، بل يكفي القصد الجنائي العام لتحقق الركن المعنوي .

-تزوير التوقيع الإلكتروني:

وجاء النص على هذه الجريمة في المادة 441 التي نصت على أنه " يعد تزويرا كل تغيير تدليسي للحقيقة ، يكون من شأنه أن يحدث ضررا ، ويقع بأي وسيلة كانت ، سواء وقع في محرر

---

[1] – بما ن المشرع الفرنسي لم يبين وسيلة *تعطيل* نظام المعالجة الآلية للبيانات، لتعدد هذه الوسائل وتطورها وعليه يتم بأي وسيلة تقنية . راجع اعبد القادر القهوجي ، مرجع سابق، ص140 .

[2] –

الأضرار التي تسبب فيه. راجع مدحت رمضان ن مرجع سابق ، ص55.

[3] – عبد القادر القهوجي ، مرجع سابق ، ص 50 وشيماء عبد الغني عطاء الله ، مرجع سابق ، ص 99

أو سند أيا كان موضوعه والذي أعد مسبقا كأداة لإنشاء حق أو ترتيب أثر قانوني معين[1]. ولقيام هذه الجريمة لابد من توافر ركنين مادي ومعنوي ، على النحو الآتي :

***الركن المادي :**

يتمثل الركن المادي لهذه الجريمة في فعل تغيير الحقيقة في توقيع الكتروني بأي وسيلة ، ومن أشهر وسائل تزوير التوقيع الإلكتروني استخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك ، يتم تصميمها على غرار البرامج والأنظمة المشروعة أو محاولة البعض كسر الشفرة والوصول إلى ة استخدامها[2].

***الركن المعنوي:**

تعد هذه من الجرائم العمدية ، صورة الركن المعنوي فيها القصد الجنائي العام بعنصريه العلم والإرادة ، حيث يجب أن يعلم الجاني بوقائع الجريمة وكونها من المحظورات ، ومع ذلك تتجه إرادته إلى الفعل المجرم .

ب –جرائم الاعتداء على التوقيع الالكتروني في التشريع الأمريكي :

وبالإضافة إلى قانون إساءة استعمال الكمبيوتر أصدر المشرع الأمريكي في03 جوان سنة 2000 قانونا اتحاديا "للتوقيع الإلكتروني والتجارة الوطنية" ، وقد سبق هذا القانون جهودا تشريعية ومنها القواعد الاتحادية للتوقيع والسجلات الإلكترونية الصادرة في 20 مارس سنة 1997 والتي

---

[1] –يلاحظ أن المشرع الفرنسي في المادة 441 لم يحدد وسيل التزوير ن وبالتالي تقع جريمة تزوير التوقيع بأي وسيلة، ويعاقب على التزوير واستعمال المحرر المزور بالسجن ثلاث سنوات وبغرامة لا تتجاوز300.000 أورو".

[2] – عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص290، ص304–305.

وضعت لتطبيقها في مجال شركات الأجهزة والقانون الاتحادي للغذاء والدواء ومستحضرات التجميل وقانون الخدمة الصحية العامة[1].

وقد وضعت مجموعة العمل تقريرا في يوليه سنة 1992 اقتصرت فيه على إلقاء الضوء على القواعد المتصلة بالتوقيع الإلكتروني؛ غير أنها في 31 أغسطس 1994 أصدرت تقريرا وضعت فيه القواعد المتعلقة بالسجلات الإلكترونية، كما وضعت قواعد للتوقيع والسجلات الإلكترونية صدرت في 20 مارس سنة 1997 [2].

يعد أول تشريع هو "قانون المعاملات الإلكترونية الموحد" الذي أصدرته ولاية كاليفورنيا في 16 سبتمبر سنة 1999 والذي دخل حيز النفاذ في 01 يناير سنة 2000، وقانون المعاملات الإلكترونية الموحد الذي أصدرته ولاية نورث كارولينا والذي دخل حيز النفاذ في 01 أكتوبر 2000[3].

وقد أصدرت ولاية نيويورك تشريعا في 28سبتمبر سنة 1999 للسجلات والتوقيع الإلكتروني وكان هدف هذا التشريع هو تنظيم وتشجيع التعامل بالسجلات الإلكترونية وقبول التوقيع الإلكتروني في التعاملات التجارية[4]، كذلك أصدرت ولاية كونتكيت قانونا للمعاملات الإلكترونية

---

[1] – أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني(دراسة مقارنة)، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر:اكادمية شرطة دبي ، مركز البحوث والدراسات رقم العدد : 1 ، من26 إلى 28 نيسان 2003 ، بدبي – الإمارات العربية المتحدة .

[2] – كما صدر نموذج اختياري لقانون المعاملات الإلكترونية الموحد، وذلك بهدف توحيد قواعد المعاملات التجارية الإلكترونية بين تشريعات الولايات ، و

للبيانات المخزنة إلكترونيا تضمنتها تشريعات اتحادية منها ما ينص عليه الفصل 119 من القسم الأول من تقنين الولايات المتحدة والذي يحمل عنوان "اعتراض وسائل الاتصالات السلكية والإلكترونية والشفهية.

[3] –عبد الحميد ثروت ، مرجع سابق ، ص185 و مابعدها.

[4] – وقد كلف الشارع في ولاية نيويورك بموجب لمادة الثالثة من الفصل الرابع من هذا القانون ، مكتب تقنيات الولاية بوضع تقرير يتضمن وضع تنظيم ودليل عمل لإنشاء واستخدام وتخزين والمحافظة على التوقيع والسجلات الإلكترونية .

في فبراير سنة 2002 ودخل حيز النفاذ في الأول من أكتوبر في ذات السنة ، كما أصدرت ولاية بنسلفانيا قانونا مماثلا في 16 ديسمبر سنة999 1[1].

وبالرغم من تلك النصوص المتعلقة بالتوقيع الالكتروني ، إلا أن تلك القوانين الاتحادية والولائية لم تأت بحماية جنائية خاصة ، بل تركتها للنصوص العامة لجرائم الحاسوب .

وبالرجوع للقانون الفيدرالي الأمريكي المتعلق بالاعتداء على الحاسوب لسنة 1996 ، نجد أن الفصل 1030 تضمن نصوصا خاصة تجرم الاعتداء الحاسوب.

حيث يجرم المشرع الدخول العمدي على البيانات الموجودة بأجهزة الكمبيوتر بدون تصريح أويتجاوز التصريح الممنوح له أيا كانت الوسيلة المستخدمة والحصول عل معلومات سرية متعلقة بالدفاع الوطني أو العلاقات الخارجية أو الطاقة النووية، أو الحصول على معلومات موجودة في سجل اقتصادي لمؤسسة مالية ، أويخص مصدر بطاقات مالية أوتقرير يتعلق بالمستهلكين [2].

كما عاقب المشرع على الدخول في حاسوب يستخدم في التجارة أو الاتصال بين الولايات ويقوم عمدا بنقل برامج أومعلومات أوكود أونظام الكمبيوتر[3]. ويعاقب المشرع كذلك كل من يمنع أو يحرم أو يتسبب في منع أو حرمان الغير من استعمال كمبيوتر أو خدماته أو نظام أو شبكة أومعلومات أو بيانات أو برامج[4]. كما يعاقب المشرع على نقل أي مكونات لبرامج أومعلومات أو كود أو أمر دون موافقة المسؤولين على الكمبيوتر المستقبل للبرامج أو المعلومات أو الكود أو الأمر إذا أدى هذا النقل إلى خسارة لشخص أو أكثر [5].

---

[1] – أشرف توفيق شمس الدين، مرجع سابق، ص7.

[2] – محمد أمين الشوابكة، مرجع سابق ، ص20.

[3] – عبد الحليم رمضان ، مرجع سابق ، ص42.

[4] – نافذ ياسين، مرجع سابق ، ص348. أيمن رمضان، مرجع سابق ، ص176.

[5] – عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص356.

وتجدر الإشارة إلى أنه يمكن توفير حماية جنائية عامة للتوقيع الالكتروني ، لكن يلاحظ أن المشرع اهتم بالتفصيل أكثر لان القانون الأمريكي من القوانين التي تهتم بالأمن القومي والجانب الاقتصادي ، تطلب أن تتعلق المعلومات المحصل عليها متعلقة بالأمن القومي ،أو بإحدى المؤسسات الاقتصادية ، ولا يجرم الدخول إلى النظام المعلوماتي ، بل لابد أن يترتب على الدخول إتلاف المعلومات أو البرامج التي تهتم بالأمن القومي والجانب الاقتصادي.

2-جرائم الاعتداء على التوقيع الإلكتروني في التشريعات العربية:

خصت بعض التشريعات العربية التوقيع الإلكتروني بحماية جنائية، أبرزها التشريع المصري والتشريع التونسي، على خلاف التشريع الجزائري الذي شمله في إطار القواعد العامة في قانون العقوبات [1]. وعليه سنبحث جرائم الاعتداء على التوقيع الإلكتروني في التشريع الجزائري والمصري والتشريع التونسي، على النحو الآتي:

أ-جرائم الاعتداء على التوقيع الإلكتروني في التشريع الجزائري:

لم يخص المشرع الجزائري التوقيع الالكتروني بحماية جنائية خاصة على غرار التشريع الفرنسي بل يمكن حمايته جنائيا في إطار قانون العقوبات من خلال جرائم الاعتداء على أنظمة المعالجة[2]، وجريمة التزوير.

- **جرائم الاعتداء على النظام المعلوماتي للتوقيع الالكتروني :**

يتحقق الاعتداء على التوقيع الالكتروني بالاعتداء على النظام المعلوماتي للتوقيع الالكتروني من خلال الدخول أوالبقاء غير المشروع .

---

[1] - تجدر الإشارة إلى أن المشرع الجزائري بصدد إصدار قانون التوقيع الالكتروني ، وهو قيد الدراسة في البرلمان ، ولم يرى النور بعد ، في انتظار صدوره لاحقا إن شاء الله .

[2] - راجع المواد 394 مكرر394- مكرر7 من قانون العقوبات الجزائري المقابلة للمواد 323/1-7/323 من قانون العقوبات الفرنسي .

عالج المشرع الجزائري جريمة الدخول أو البقاء غير المشروع في المادة 394 مكرر ق ع ج يتمثل الركن المادي في الدخول أو البقاء غير المشروع في قاعدة بيانات التوقيع الإلكتروني[1].

وتصنف هذه الجريمة من جرائم الخطر ، حيث يتم تجريم السلوك دون توقف ذلك على نتيجة معينة، فهذه الجريمة ليست من جرائم الضرر المتطلب فيها حصول ضرر بالمجني عليه[2].

وتعد هذه الصورة من الجرائم العمدية ، وبالتالي فإنه لا يتصور وقوعها بطريق الخطأ ، ويتخذ فيها صورة القصد الجنائي العام بعنصرية العلم والإرادة .

تضاعف العقوبة ، وتكون العقوبة الحبس من ستة أشهر(6) إلى سنتين (2)، والغرامة من 50.000 إلى 150.000دج [3].

ويلاحظ أن المشرع الجزائري لم ينص على جريمة الاعتداء القصدي على سلامة النظام المعلوماتي ، بل اكتفى بالنص عل الاعتداء على النظام كظرف مشدد ، على خلاف المشرع الفرنسي الذي نص عليها في المادة 323 /2 من قانون العقوبات الفرنسي ، وتتحقق هذه الجريمة بتعطيل النظام [4]، أو [5].

---

[1] – عبد القادر القهوجي، مرجع سابق، ص128.

[2] – عبد القادر القهوجي، مرجع سابق، ص129ومابعدها.

[3] – راجع الفقرة 2 من المادة 394 مكرر من قانون العقوبات الجزائري .

[4] – يتحقق توقيف نظام التوقيع الالكتروني بإحداث عطب أو خلل بالتوقيع بما يجعله لا يقوم بعمله بصورة طبيعية، وقد يكون ذلك بالحد من سرعة النظام المعلوماتي وجعله بطيئا أو يعطي نتائج غير منتظرة .

[5] – يتحقق إفساد التوقيع الالكتروني بإعدامه وجعله غير صالح للاستعمال مطلقا، على خلاف التعطيل عن الذي يتيح .

-جريمة الاعتداء على بيانات التوقيع الالكتروني :

نص المشرع الجزائري على جريمة التلاعب ببيانات النظام المعلوماتي بموجب المادة394 مكرر2 ، ولهذه الجريمة ركنان مادي ومعنوي. يتمثل الركن المادي لهذه الجرائم في إدخال إزالة ومحو أو تغيير بياناته[1].

أما الركن المعنوي لجريمة التلاعب ببيانات التوقيع الالكتروني ، فيتمثل في القصد الجنائي العام، بعنصريه العلم والإرادة [2]. ولا يشترط توافر القصد الجاني الخاص،إذ يكفي أن تتجه إرادة الجاني إلى الاعتداء على بيانات التوقيع الالكتروني بالإدخال أو التعديل أو المحو، وأن يعلم بأن نشاطه ذلك يترتب عليه التلاعب في بيانات التوقيع الالكتروني .

-جريمة تزوير التوقيع الالكتروني:

لم ينص المشرع الجزائري على جريمة التزوير المعلوماتي بصراحة كما فعل المشرع الفرنسي في المادة 441 من قانون العقوبات الفرنسي[3]

جريمة التزوير على التوقيع الالكتروني[4].

ويتمثل الركن المادي في تغيير الحقيقة في بيانات التوقيع الالكتروني بطرق مادية أو معنوية ومن شأن ذلك التغيير أن يؤدي إلى حصول ضرر[5].

التي يتطلب فيها المشرع النتيجة الإجرامية .

أما الركن المعنوي فيتمثل في القصد الجنائي العام ، حيث يجب أن يعلم الجاني بوقائع الجريمة وكونها من المحظورات، ومع ذلك تتجه إرادته إلى ارتكاب الفعل .

---

[1] -عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت ، مرجع سابق ، ص190 .

[2] – محمد رايس ، الحماية الجنائية للسند الالكتروني في القانون الجزائري ، مرجع سابق ، ص100.

[3] - راجع المادة 441 من قانون العقوبات الفرنسي

[4] – راجع الفصل السابع من المواد197– 253 مكرر من قانون العقوبات الجزائري .

[5] – عبد القادر القهوجي ، مرجع سابق ، ص155.

إلى جانب القصد الجنائي العام، لابد من توافر قصد جنائي خاص يتمثل في استعمال التوقيع الالكتروني من أجل غرض معين [1].

ب- جرائم الاعتداء على التوقيع الإلكتروني في التشريع المصري:

نص المشرع المصري على جرائم التوقيع الإلكتروني في المادتين 21، 23 من قانون رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني.

-الجرائم المنصوص عليها في المادة 21 من قانون التوقيع الالكتروني:

نصت المادة 21 من قانون التوقيع الإلكتروني المصري على :"أن بيانات التوقيع الإلكتروني والوسائط الالكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني سرية، ولا يجوز لمن قدمت إليه أو بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجله ".

ويتضح من المادة 21 من قانون التوقيع الالكتروني ، أن المشرع المصري يجرم إفشاء بيانات التوقيع الالكتروني، وجريمة استخدام هذه البيانات في غير الغرض المخصص لها، على التفصيل الآتي :

***جريمة إفشاء بيانات التوقيع الالكتروني:**

يتضح من خلال المادة 21 من قانون التوقيع الإلكتروني المصري ، أنه يتطلب لقيام هذه الجريمة ، توافر ركنين مادي يتمثل في إفشاء للغير بيانات التوقيع الإلكتروني والوسائط الالكترونية والمعلومات من قبل الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني للغير أو استخدامها في غير الغرض الذي قدمت من أجله .

---

[1]- لايتحقق الركن المعنوي في جريمة التزوير إلا بتوافر القصد الجنائي العام بعنصريه العلم والإرادة ، وتوافر القصد الجنائي الخاص وهو استعمال التوقيع المزور في غرض معين .

كما يتطلب فيها إلى جانب الركن المادي ركن معنوي يتخذ صورة القصد الجنائي العام دون القصد الجنائي الخاص، على التفصيل الآتي :

الركن المادي:

يتمثل الركن المادي في هذه الجريمة في إفشاء بيانات التوقيع الإلكتروني ،أي نشرها واطلاع الغير عليها، السرية بعد أن كان العلم بها قاصرا على الذين ائتمنوا عليها بحكم وظيفتهم[1].

ويتحقق الركن المادي للجريمة بمجرد انتهاك سرية البيانات وخصوصيتها حتى ولو لم يترتب على الفعل أي نتيجة ، فالجريمة سلوكية يكتفي فيها المشرع بتحقق السلوك المادي [2].

الركن المعنوي:

هذه الجريمة العمدية يلزم لقيامها اتجاه إرادة الجاني إلى إفشاء بيانات التوقيع الإلكتروني أو إساءة استخدامها، مع علمه بذلك وقبول النتائج المترتبة على هذا السلوك الإجرامي الذي لا يتصور وقوعه بطريق الخطأ.

***جريمة إساءة استخدام بيانات التوقيع الالكتروني:**

لقيام هذه الجريمة لابد من توافر ركنين مادي و معنوي، على النحو الآتي:

الركن المادي :

---

[1]- ويلاحظ أن التجريم هنا يقتصر على من قدمت إليه أو اتصل بها بحكم عمله ، في حين كان من المفروض أن يجرم المشرع انتهاك سرية بيانات التوقيع الالكتروني بصفة عامة .أنظر أيمن رضا محمد أحمد، مرجع سابق، ص 142.

[2] –لا يشترط المشرع المصري تحقق نتيجة معينة لتحقق الركن المادي لأن الغرض من التجريم هو الحفاظ على سرية وخصوصية البيانات وليس تحقق نتيجة إجرامية معينة ، وبالتالي جريمة سلوكية وليست من جرائم الضرر.

ويتحقق الركن المادي في هذه الجريمة بإساءة استخدام بيانات التوقيع الإلكتروني وذلك باستخدامها في غرض آخر غير ما قدمت من أجله [1]،ويقتصر هنا أيضا التجريم على من قدمت إليه أو اتصل بها بحكم عمله والذي استعملها في الغرض الذي قدمت من أجله [2].

الركن المعنوي:

هذه الجريمة العمدية يلزم لقيامها توافر القصد الجنائي باتجاه إرادة الجاني إلى إساءة استخدام بيانات التوقيع الالكتروني ، باستعمالها في غير الغرض المخصص لها، مع علمه بذلك و قبول النتائج المترتبة على هذا السلوك الإجرامي الذي لا يتصور وقوعه بطريق الخطأ[3].

ومتى تحقق الركن المادي والركن المعنوي وجب إنزال العقوبة على الجاني دون النظر إلى الباعث الذي دفعه إلى إساءة استخدام بيانات التوقيع الالكتروني [4].

-الجرائم المنصوص عليها في المادة 23 من قانون التوقيع الإلكتروني:

تنص المادة 23 من قانون 15 لسنة 2004 على أنه " مع عدم الإخلال بأية عقوبة اشد منصوص عليها في قانون العقوبات أو في قانون آخر يعاقب بالحبس و بغرامة لا تقل عن 10 آلاف جنيه و لا تجاوز مئة ألف جنيه، أو بإحدى هاتين العقوبتين كل من :

أ- أصدر شهادة تصديق دون الحصول على ترخيص .

---

[1] - سليمان أحمد فضل، مرجع سابق.، ص 161.

[2] - راجع المادة 21 من قانون التوقيع الالكتروني المصري .

[3]- هذه الجريمة العمدية يلزم لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة ، وبالتالي ذا وقع السلوك الإجرامي نتيجة الخطأ والإهمال فلا يتحقق الركن المعنوي. للتفصيل راجع سليمان أحمد فضل، مرجع سابق، ص 161.

[4] - اكتفى المشرع المصري بالقصد الجنائي العام دون الخاص في جريمة إساءة استخدام بيانات التوقيع الالكتروني وعليه لا عبرة بالباعث والغرض من ارتكاب هذه الجريمة . فمتى تحقق والركن المعنوي في صورة القصد الجنائي العام إلى جانب الركن المادي ، وجب عقاب الجاني دون النظر إلى الباعث من إساءة استخدام التوقيع الالكتروني.

ب – أتلف أو عيب توقيعا أو وسيطا أو محررا إلكترونيا، أو زور شيئا من ذلك بطريق الاصطناع أو التعديل أو بأي طريق آخر.

ج – استعمل توقيعا أو وسيطا أو محررا إلكترونيا معيبا أو مزورا مع علمه بذلك. د– توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني أو اخترق أو اعترضه أو عطله عن أداء وظيفته، وفي حالة العود تزداد بمقدار مثل العقوبة المقرر لهذه الجرائم .

***جريمة إصدار شهادة التصديق الإلكتروني بدون ترخيص:**

وقد نص المشرع المصري على هذه الجريمة في المادة 23/أ من قانون التوقيع الإلكتروني، ويتطلب لقيامها توافر ركن مادي، ومعنوي.

الركن المادي:

يتمثل السلوك الإجرامي في هذه الجريمة، في انتحال الجاني صفة مزود خدمات التصديق المرخص له بخلاف الحقيقة، و يصدر شهادات تصديق إلكتروني دون ترخيص بذلك من الهيئة العامة لتنمية صنعة تكنولوجيا المعلومات"[1].

وبالتالي تقع هذه الجريمة إذا أصدر الجاني شهادة تصديق الكتروني دون الحصول على ترخيص مخالفة للمادة 19 من قانون التوقيع الالكتروني[2].

---

[1]– عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الأنترنت، دار الفكر الجامعي، الإسكندرية مصر، 2006 ، ص 157. أيمن رمضان أحمد ، مرجع سابق ، ص137.

[2] – تنص المادة 19 من قانون التوقيع الالكتروني على مجموعة من الالتزامات تقع على عاتق من يرغب في مزاولة نشاط إصدار شهادات صديق الكتروني، وهي :

– ضرورة الحصول على ترخيص من هيئة تنمية صناعة تكنولوجيا المعلومات قبل ممارسة النشاط المذكور.

– سداد رسم الهيئة الذكورة مقابل هذا النشاط . – عدم جواز التوقف عن النشاط المرخص به أو الاندماج في جهة أخرى أو التنازل عن الترخيص للغير ، سوى بعد الحصول موافقة كتابية من الهيئة المذكورة .

والسبب في تجريم هذا الفعل هو الآثار الخطيرة المترتبة على شهادة التصديق الإلكترونية في حق الغير[1]، حيث يكون مضمونها التسليم بصحة بيانات التوقيع الإلكتروني، أو بيانات المعاملة المطلوب صدور شهادة التصديق عنها[2].

ويمكن القول أن هذه الجريمة من جرائم الخطر، أو جرائم السلوك المجرد حيث يتكامل قيام الركن المادي فيها بمجرد إتيان الجاني لسلوك إصدار شهادات التصديق الالكتروني بدون ترخيص، دون تطلب حصول ضرر بجهة ما أو شخص ما [3].

الركن المعنوي:

وهذه الجريمة من الجرائم العمدية، لابد فيها من توافر القصد الجنائي العام ، وذلك بأن يعلم الجاني بأن بقوم بإصدار الشهادة دون ترخيص ، وأن تتجه إرادته إلى هذا السلوك[4].

ومن ثمة فلا يتصور وقوع هذه الجريمة بطريق الخطأ بل يجب أن تنصرف الإرادة إلى هذا الفعل، انطلاقا من المادة 1/23.

***إتلاف أوتعييب أو تزوير التوقيع الإلكتروني:**

جرم المشرع المصري هذه الأفعال في المادة 23/ب من قانون التوقيع الإلكتروني، كالآتي :

---

[1] – عرف القانون 15 لسنة 2004 في مادته الأولى شهادة التصديق الالكتروني بأنها " الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع .

[2]– أيمن رضا محمد، مرجع سابق، ص 132.

[3] سليمان أحمد فضل ، مرجع سابق ، ص167.

[4]– عبد الفتاح حجازي، التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية مصر، 2006، ص 540.

جريمة إتلاف أوتعييب التوقيع الإلكتروني:

الركن المادي:

ويتحقق الركن المادي في هذه الجريمة بإتلاف أو تعييب التوقيع الإلكتروني ، ويتحقق فعل الإتلاف بإفقاد البرنامج المعلوماتي الخاص للتوقيع الإلكتروني قدرته على العمل[1]، أما تعيب التوقيع الإلكتروني يكون بفقده القدرة على العمل أو الصلاحية بصورة جزئية، كأن يصدر التوقيع مشوها أو غير واضح[2].

ويتطلب لقيام هذه الجريمة ضرورة توافر الضرر، فالضرر هو النتيجة الإجرامية المترتبة على الاعتداء و ترتبط بالفعل برابطة سببية قانونية حال توافر أركان الجريمة، ويستوي أن يكون الضرر ضرر مادي أو معنوي[3].

الركن المعنوي:

هذه الجريمة من الجرائم العمدية، يتطلب فيها توافر ركن معنوي يتمثل في القصد الجنائي العام بعنصريه العلم و الإرادة، فيجب أن يعلم الجاني بأن فعل الإتلاف أو التعييب للتوقيع الإلكتروني محظور و معاقب عليه قانونا، وأن تتجه إرادته للفعل المجرم[4]، أما إذا كان الإتلاف أوالتعييب ناتج عن حادث غير مقصود كما لو وقع من العامل شيء على الجهاز أدى إلى إتلاف جزء منه فلا تقوم هذه الجريمة .

ولا تتطلب هذه الجريمة قصدا خاصا، و إنما يكتفي بشأنها القصد العام بعنصريه العلم و الإرادة، فتقوم الجريمة بتوافر الركن المادي والقصد الجنائي العام .

---

[1] – لم يحدد القانون المصري في المادة 23 طريقة معينة لإتلاف أو تعييب التوقيع ، وعليه يتحقق الإتلاف بأي وسيلة تؤدي إلى عدم الانتفاع به مثل نشر فيروس أو سكب كوب ماء أو سائل على الوسيط

[2]- عبد الفتاح حجازي، حماية المستهلك عبر شبكة الأنترنت ، مرجع سابق، ص 159.

[3]– أيمن رضا محمد، مرجع سابق، ص 188.

[4]– ناقد ياسين محمد المدهون، مرجع سابق، ص 362.

جريمة تزوير التوقيع الإلكتروني:

الركن المادي :

يتمثل الركن المادي لهذه الجريمة في تزوير التوقيع الالكتروني بتغيير الحقيقة في التوقيع الإلكتروني بطريق الاصطناع أو التعديل أو التحويل، أو بأي طريق على نحو يضر بالغير[1].

ومن أشهر الوسائل التي يمكن الاعتماد عليها في تزوير التوقيع الإلكتروني استخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك ، يتم تصميمها على غرار البرامج والأنظمة المشروعة أو محاولة البعض كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني ، والقيام بنسخها[2].

الركن المعنوي:

يمثل الركن المعنوي في هذه الجريمة في القصد الجنائي العام ، بأن يكون الجاني عالما بأنه ترتكب جريمة و أن تتجه إرادته إلى تزوير التوقيع الإلكتروني ، فمجرد إهماله في تحري الحقيقة مهما كانت درجته لا تتحقق به جريمة التزوير[3].

ويتطلب كذلك توافر القصد الجنائي الخاص لدى الجاني إلى جانب القصد الجنائي العام وهو نية استعمال التوقيع الإلكتروني فيما زور من أجله، على خلاف جريمة الإتلاف التي اكتفى فيها المشرع المصري بالقصد الجنائي العام [4].

---

[1]– يلاحظ أن طرق التزوير لم ترد على سبيل الحصر لكون المشرع أضاف عبارة (أو أي طريق آخر) لأن حصرها غير ممكن، لتعددها و اختلافها و وتجددها ، و لذلك يتحقق تزويره بأي طريقة ووسيلة . للتفصيل راجع عبد الفتاح بيومي حجازي، حماية المستهلك عبر الإنترنت ، مرجع سابق ص 160

[2] – أيمن رضا محمد، مرجع سابق، ص 207.

[3]– سليمان أحمد فضل، مرجع سابق، ص 164.

[4] – عبد الفتاح سومي حجازي، حماية المستهلك عبر الإنترنت ، مرجع سابق ص 161.

***استعمال توقيع إلكتروني معيب أو مزور:**

ورد النص على هذه الجريمة في المادة 23/ج من قانون التوقيع الإلكتروني ، ويقصد باستعمال توقيع الكتروني معيب أو مزور إبراز التوقيع الالكتروني المزور أو المعييب والاحتجاج به على اعتبار أنه صحيح [1]. وتقوم جريمة استعمال توقيع إلكتروني معيب أو مزور بتوافر ركنين مادي و معنوي، على التفصيل الآتي:

الركن المادي:

ويتمثل في استخدام الجاني للتوقيع الإلكتروني المعيب أو المزور مع علمه بذلك ، ولا يشكل

المعاملات بقيمته كما لو كان صحيحا، ويتحقق ذلك بكل سلوك إيجابي [2] .

الركن المعنوي:

جريمة استعمال التوقيع الإلكتروني المعيب أو المزور هي جريمة عمدية، يلزم لقيامها أن يتوافر القصد الجنائي العام بعنصريه العلم و الإرادة، فيجب أن يعلم أو التوقيع الإلكتروني مزورا أو معيبا وفق الاستعمال، ومع ذلك تنصرف إرادته إلى استعماله فيما أعد له.

---

[1] – ومحل جريمة استعمال توقيع إلكتروني معيب أو مزور يتمثل في التوقيع الالكتروني المزور أو المعييب . للتفصيل راجع سليمان أحمد فضل ، مرجع سابق ، ص165.

[2] – وعليه لابد أن يكون السلوك الإجرامي ايجابي بإظهار التوقيع الالكتروني المعيب المزور أو المعيب الغير في المعاملات بقيمته كما لو كان صحيحا، فالعبرة بتقديم المستند الاحتجاج به أو الاستناد إليه في المعاملات كدليل في التمسك بحق أو الحصول على حق معين ، ويستوي أن يكون هذا الاستعمال قد بوشر في مواجهة جهة رسمية أو موظف عام في معاملات الأفراد. للتفصيل راجع جميل عبد الباقي، القانون الجنائي و التكنولوجيا الحديثة، مرجع سابق ، ص 180.

ولا عبرة بالأغراض التي يتوخاها الجاني في الاستعمال، فيعد مرتكبا لهذه الجريمة من يستخدم توقيعا مزورا أو معيبا، وان كان يرمي إلى الوصول إلى حق ثابتا قانونيا[1].

وبالتالي إذا انتفت نية استعمال التوقيع الإلكتروني المعيب أو المزور فيما زور من أجله، انتفت الجريمة، ويجب تحري القصد وقت ارتكاب الجريمة.

وتجدر الإشارة في الأخير إلى أن المشرع المصري عاقب على استعمال توقيع إلكتروني معيب أو مزور، دون الإتلاف، وذلك لأن هذا الأخير لا يعمل و فقاد الصلاحية، و لا أثر له من الناحيتين العملية و القانونية[2].

***جريمة الحصول على التوقيع الإلكتروني أو اختراقه أو اعتراضه أو تعطيله:**

جاء النص على هذه الجريمة في المادة 23/د، ولقيام هذه الجريمة، لابد من توافر ركنين مادي و معنوي، على التفصيل لآتي:

الركن المادي:

ويتخذ السلوك الإجرامي في هذه الجريمة صورة الحصول بغير حق على توقيع إلكتروني بأي وسيلة، ويمكن الاستيلاء على التوقيع الإلكترونين عن طريق السرقة أو النصب أو عن طريق خيانة الأمانة [3].

ويتحقق أيضا باختراق التوقيع الإلكتروني بالدخول غير المشروع أو غير المصرح به للنظام المعلوماتي المتضمن للتوقيع الإلكتروني [4]، أو اعتراضه أو تعطيله عن أداء وظيفته بأي وسيلة تؤدي إلى تباطؤ النظام و جعله غير قادر على الاستعمال دائما أو مؤقتا بشكل متقطع [5].

---

[1] – أيمن رضا محمد، مرجع سابق، ص 219.

[2] – المرجع نفسه، ص. 217 .

[3] – لقد أحسن المشرع المصري صنعا حينما لم يحدد وسيلة على سبيل الحصر لارتكاب الفعل المجرم، لكنه خلافا لبعض التشريعات لم يجرم محاولة الحصول على توقيع أو محرر إلكتروني.

[4] – عبد الحليم رمضان ، مرجع سابق ، ص51. وانظر أيضا:

Gassin(R) op.cit.no88.

[5] – عبد القادر القهوجي، مرجع سابق، ص 140، 141.وانظر أيضا :

الركن المعنوي:

تعتبر هذه الجريمة من الجرائم العمدية ، تتحقق بتوافر القصد الجنائي العام فلابد أن يعلم الجاني بأن حصوله على التوقيع الإلكتروني يعتبر حق، وأنه يخترق التوقيع الإلكتروني أو يعترضه، أو يعطله، و أن تتجه إرادته إلى ذلك الفعل، ولا يتطلب المشرع في هذه الجريمة قصدا جنائيا خاصا، بل اكتفى بالقصد الجنائي العام [1].

لذلك ينتفي القصد الجنائي إذا قام الشخص الذي يتعامل مع النظام بالحصول على التوقيع الالكتروني أو اختراقه أو اعتراضه أو تعطيله نتيجة الخطأ، فهذه الجريمة من الجرائم العمدية لا يتصور وقوعها بطريق الخط [2].

ج- جرائم الاعتداء على التوقيع الالكتروني في التشريع التونسي :

نظر للانتشار الواسع للتوقيع الالكتروني في إطار المعاملات التجارية ، كان لابد من إقرار حماية جزائية ، ضد الاعتداءات التي يتعرض لها التوقيع الالكتروني، لذا نظم المشرع التونسي حماية جنائية خاصة للتوقيع الالكتروني بموجب القانون المؤرخ في 9 أوت 2000 المتعلق بالمبادلات والتجارة الالكترونية [3].

Gassin(R) informatique et liberté répertorie Dalloz de droit pénal ,jzniper.1987.no522.

[1] - أيمن رمضان احمد، مرجع سابق، ص 164. وانظر أيضا عبد الفتاح بيومي حجازي، التوقيع الالكتروني ، مرجع سابق ص133

[2] - عبد الحليم مدحت رمضان، مرجع سابق ، ص54.

[3] - وفر المشرع التونسي حماية جنائية خاصة للتوقيع الالكتروني في الفصول 46-48 من القانون المؤرخ في 9 أوت 2000 المتعلق بالمبادلات والتجارة الالكترونية .

- **جريمة مباشرة خدمات المصادقة بدون ترخيص :**

اقتضى الفصل 46 من نفس القانون "يعاقب كل من يمارس نشاط مزود خدمات المصادقة الالكترونية بدون ترخيص مسبق طبقا للفصل 11 من هذا القانون بالسجن لمدة تتراوح بين شهرين و3 سنوات وبخطية تتراوح بين 1000 و 10000 دينارا أو بإحدى هاتين العقوبتين" [1].

ويتضح بأن المشرع التونسي بتطلب لقيام هذه الجريمة توافر ركن مادي يتمثل في ممارسة نشاط مزود خدمات المصادقة الالكترونية بدون ترخيص [2]، وركن معنوي يتخذ صورة القصد الجنائي العام ، على النحو الآتي :

الركن المادي :

يتحقق الركن المادي في هذه الجريمة بالتعامل في بيانات التجارة الالكترونية دون ترخيص من

، فالجريمة تعتبر جريمة سلوكية[3].

وتشرف الوكالة الوطنية للمصادقة الالكترونية على منح الترخيص اللازم لممارسة نشاط وخدمات المصادقة الالكترونية، وتحقق الوكالة من خلال هذه الصلاحية رقابتها على الأشخاص الذين يمكن أن توكل لهم الوظائف المتعلقة بشهادات المصادقة والإمضاء الالكتروني، والتثبت من مدى توفر الشروط اللازمة للاضطلاع بهذه المهام على الوجه المطلوب ، لذلك كان لابد من زجر

---

[1] – حسب المادة 11 فإنه لا يمكن لمزود خدمات التصديق أن يباشر عمله دون ترخيص من الوكالة الوطنية للمصادقة سواء شخصا طبيعيا أو معنويا، وأن هناك شروط محددة وردت في المادة 1 لمنح الرخصة.

[2] – تتمثل علاقة هذه الجريمة بجرائم الاعتداء على التوقيع الالكتروني ن في أن ممارسة هذه المهنة دون ترخيص ، يؤدي إلى إصدار شهادات غير قانونية ، تحتوي على التوقيع الالكتروني لصحب الشهادة .

[3] – عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص275–276.

كل ممارسة لهذه الوظائف خارج مراقبة الوكالة الوطنية للمصادقة الالكترونية، ودون الحصول على الترخيص المذكور.

الركن المعنوي :

وهذه الجريمة هي جريمة عمدية يكفي لتوافرها توفر القصد الجنائي العام بعنصريه العلم والإرادة، أي أن يكون المزود على علم أنه غير مرخص له في مباشرة النشاط، ومع ذلك تتجه إرادته إلى القيام بذلك[1].

ومتى قامت الجريمة فانه يعاقب الجاني بالسجن لمدة شهرين إلى ثلاث سنوات وبخطية تتراوح بين1000 و10.00دينار أو بإحدى هاتين العقوبتين [2] .

- جريمة التصريح عمدا بمعطيات خاطئة :

ونص عليها المشرع التونسي في المادة 47 بأنه :" يعاقب كل من صرح بمعطيات خاطئة لمورد خدمات التوثيق الالكتروني لكافة الأطراف التي طلب منها أن تثق بإمضائه بالسجن لمدة تتراوح بين 6أشهر و عامين ، وبغرامة تتراوح بين 1000 و 10.000 دينار أو إحدى هاتين العقوبتين [3].

وبالتالي الهدف من تجريم هذا الفعل هو حماية عملية التجارة الالكترونية و أطرافها من استقبال معلومات خاطئة تؤثر على حقوق أطراف التعاقد أو على الثقة المفترضة في هذه التجارة لذلك

---

[1] – هدى قشقوش ، الحماية الجنائية للتجارة الالكترونية عبر الانترنت ، مرجع سابق ، ص43.

[2] – راجع المادة 46 من قانون المبادلات والتجارة الالكترونية التونسي.

[3] – هذا العقاب الجزائي يجد أساسه في الالتزام المحمول على المستعمل بمد مزود خدمات المصادقة الالكترونية إذا كنت غير صحيحة.

فهذه الجريمة من شأن العقاب عليها زيادة الثقة لدى المتعاملين في هذه التجارة و الحفاظ على حقوقهم[1]، و يتطلب لقيام هذه الجريمة ركنين، ركن مادي و ركن معنوي.

الركن المادي :

تتحقق هذه الجريمة بالتصريح بمعطيات خاطئة، أي إعطاء معطيات غير صحيحة سواء كان ذلك من قبل أي شخص ، وسواء أعطيت هذه البيانات إلى مورد خدمات التوثيق الالكتروني أو احد أطراف التعاقد أو طرف آخر كبنك.

هذه الجريمة مثل سابقتها من الجرائم تعد من قبيل جرائم السلوك المجرد وليست من جرائم الضرر ، بمعنى إن المشرع لا يشترط لقيام الركن المادي فيها حلول ضرر معين ، و إنما يكفي تحقق النشاط الإجرامي و هو إعطاء المعطيات غير صحيحة[2].

الركن المعنوي :

جريمة التصريح بمعطيات غير صحيحة هي جريمة عمدية ، حيث تطلب المشرع صراحة توافر القصد الجنائي من خلال عبارة " صرح عمد" و لذلك فصورة القصد هو قصد جنائي عام [3].

وبالتالي يجب أن يعلم أن ذلك الفعل محظورا وفقا للقانون ومع ذلك تنصرف إرادته إلى فعل الإدلاء بالمعطيات غير الصحيحة ، وكذلك إلى قبول النتيجة المترتبة على فعله بوصفها مخالفة للقانون ، ولهذا لا يتصور وقوع الجريمة بطريق الخطأ لأن فعل الإعطاء يجب ناتج عن قصد [4].

---

[1] – عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص290.

[2] – هدى قشقوش،جرائم الحاسب الآلي الالكتروني ، مرجع سابق ، ص45.

[3] – عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص290.

[4] – هدى قشقوش ، الحماية الجنائية للتجارة الالكترونية عبر الانترنت ، مرجع سابق ، ص45.

ولا تتطلب هذه الجريمة لقيامها قصد جنائي خاص أو نية خاصة يتعين توافرها لدى الجاني ذلك أن مجرد الإدلاء بمعلومات خاطئة تقوم به هذه الجريمة [1].

ويعاقب المشرع على هذه الجريمة بالسجن لمدة تتراوح بين 6 أشهر إلى عامين، وبخطية تتراوح من 1000الى 10.000دينار أو بإحدى هاتين العقوبتين[2].

-جريمة فض تشفير إمضاء إلكتروني:

يقتضى الفصل 48 من قانون المبادلات والتجارة الالكترونية يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بإمضاء غيره بالسجن لمدة تتراوح بين 6 أشهر وعامين وبخطية تتراوح بين 1.000 و 10.000 دينار أو بإحدى هاتين العقوبتين.

ولقيام هذه الجريمة يتطلب توافر ركنين مادي ومعنوي ، على النحو الآتي :

الركن المادي:

والركن المادي في هذه الجريمة يتمثل في اختراق التشفير المتعلق بالإمضاء الإلكتروني وبالتالي كل من استعمل عناصر تشفير غيره بصفة غير مشروعة يشكل اختراقا لنظام التشفير يجعله عرضة للمتابعة الجزائية [3].

---

[1] – عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص292.

[2] – راجع المادة 46 من قانون المبادلات والتجارة الالكترونية التونسي.

[3] – ي نظام المبادلات الالكترونية من كل اختراق والذي يجسد الضمانة الأولى والأساسية لتحقيق الأمن.

وهذه الجريمة من جرائم السلوك المجرد لا يتطلب فيها تحقق نتيجة إجرامية بل تقوم بمجرد فض شفرة التوقيع الالكتروني، دون حصول ضرر للمجني عليه[1].

وما يلاحظ أنه بالنظر للصبغة الفنية لهذه الجرائم فقد حرص المشرع أن تكون معاينتها من قبل أشخاص مختصين حتى تتم الإحاطة بهذه الجرائم المعقدة، لكن دون أن يمنع ذلك من إمكانية معاينة أعوان الضابطة العدلية لمثل هذه المخالفات [2].

الركن المعنوي :

هذه الجريمة من الجرائم العمدية التي تتطلب لقيامها القصد الجنائي العام بعنصريه العلم والإرادة ، وبالتالي يجب أن يعلم الجاني أن ذلك الفعل محظورا وفقا للقانون و مع ذلك تنصرف إرادته إلى فعل الاعتداء على البيانات المشفرة .

[1] – وعليه فيتحقق الركن المادي دون ضرورة تحقق النتيجة الإجرامية ، لأنها من جرائم السلوك المجرد لا يتطلب فيها تحقق نتيجة إجرامية بل تقوم بمجرد فض شفرة التوقيع الالكتروني، دون حصول ضرر للمجني عليه .راجع رضا الوسلاتي، جرائم اختراق التشفير الالكتروني. جرائم الإعلامية، ملتقى جهوي بدائرة محكمة الاستئناف بسوسة 2001، ص 88.

[2] – كما أنه بالنظر لميدان تدخل القانون عدد 83 لسنة 2000 وهو ميدان المبادلات والتجارة الالكترونية فقد خول المشرع للإدارة إمكانية إجراء الصلح في بعض المخالفات دون أن يؤثر ذلك على الحقوق المدنية للمتضررين وهو اختيار يتماشى والتوجه التشريعي الذي يخول للإدارة إجراء الصلح في المخالفات الاقتصادية.

المطلب الثاني: الحماية الجنائية للبيانات الشخصية للمستهلك في إطار التجارة الالكترونية

أدى ظهور الانترنت وشيوع استخدامه في كافة مجالات الحياة ، إلى مخاطر على الحياة الخاصة ، لهذا برزت جهود دولية لحماية البيانات الشخصية ، كدليل الأمم المتحدة لعام1990 والمتعلق باستخدام المعالجة الآلية للبنات الشخصية ، ومعاهدة مجلس أوربا الخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات الشخصية في 17 سبتمبر 1980 السارية المفعول في سنة 1985.

واهتمت تشريعات الدول بحماية البيانات الشخصية ، وفي مقدمتها التشريع الفرنسي بموجب القانون رقم 78 /17 الصادر في 06 جانفي 1978 والمتعلق بالمعلوماتية والحريات [1]، واهتمت كذلك التشريعات بعض العربية بحماية البيانات الشخصية، كالتشريع الجزائري والتونسي .

الفرع الأول :جرائم الاعتداء على البيانات الشخصية في التشريع الفرنسي

نص المشرع الفرنسي على جرائم الاعتداء على البيانات الشخصية في المواد 16/226- 226 /24 من قانون العقوبات الفرنسي الجديد [2]. وتمثلت تلك الجرائم في جرائم سلبية كجريمة عدم اتخاذ الإجراءات الأولية ، وجريمة عدم اتخاذ الاحتياطات لحماية البيانات ، وجرائم ايجابية كجريمة المعالجة غير المشروعة للبيانات ، وجريمة معالجة بيانات اسمية لأشخاص مصنفين وجريمة حفظ بيانات اسمية خارج المدة المحددة وجريمة الانحراف عن الغرض من المعالجة الآلية للبيانات الاسمية وجريمة الإفشاء غير المشروع للبيانات الاسمية[3].

---

[1] – قام المشرع الفرنسي بإلغاء قانون 17/78 الصادر في 06 جانفي 1978 (المواد 41-44) بقانون العقوبات الجديد لسنة 1994 المواد 16/226الى 24/226ن لكنه أكد أحكام القانون السابق ، مع بعض التغييرات .

[2] – نص المشرع على جرائم البيانات الاسمية في قانون المعلوماتية والحريات الصادر في 6 جانفي 1978 في المواد41 الى44 والمادة 46 ، لكنه عدلها في إطار قانون العقوبات الجديد لسنة 1994من 226-16الى226-24 من قانون العقوبات الفرنسي الجديد.

[3] – أمين أحمد الشوابكة، مرجع سابق، ص86.

أولا-الجرائم السلبية الواقعة على البيانات الشخصية:

وتمثلت تلك الجرائم السلبية في جريمة عدم اتخاذ الإجراءات الأولية ، وجريمة عدم اتخاذ الاحتياطات لحماية البيانات الشخصية [1]،على النحو الآتي :

1-جريمة عدم اتخاذ الإجراءات الأولية لمعالجة البيانات الشخصية :

نصت المادة 226-16 من قانون العقوبات الفرنسي على أن " كل من قام ولو بإهمال بمعالجة آلية للبيانات الاسمية، أو حاول القيام بمعالجة آلية لمعلومات اسمية دون مراعاة الإجراءات الأولية للقيام بها، يعاقب بالحبس لمدة ثلاث سنوات وبغرامة 300 ألف أورو".

يتضح من خلال المادة 226-16 ، أن هذه الجريمة لها ركنين مادي ومعنوي ، كالآتي :

أ-الركن المادي:

يتحقق الركن المادي لهذه الجريمة توافر عنصرين : يتمثل الأول في السلوك الإجرامي الذي يتخذ شكل المعالجة الآلية للبيانات الاسمية والثاني يتمثل في عدم مراعاة الإجراءات القانونية [2].

-القيام بالمعالجة الآلية للبيانات الشخصية:

طبقا لنص المادة 05 من قانون المعلوماتية والحريات الفرنسي، فإن المعالجة الآلية للبيانات الشخصية تتحقق إما بجمع هذه البيانات أو تسجيلها أو حفظها أو تصنيفها أو تحليلها أو تعديلها أو محوها، وكل مجموعة عمليات تحمل معالجة لهذه البيانات[3]، وعاقب المشرع الفرنسي حتى ولو كانت المعالجة بإهمال من الفاعل بالحبس لمدة ثلاث سنوات وبغرامة 300.000 أورو[4].

---

[1] – وهذه الجرائم سلبية لأنها تنطوي على امتناع عن اتخاذ الإجراءات الأولية ، أو عدم اتخاذ الاحتياطات القانونية.

[2] – عبد الحليم رمضان، مرجع سابق، ص91 وما بعدها.

[3] – راجع المادة 226-16 من قانون العقوبات الفرنسي.

[4] – محمد أمين أحمد الشوابكة، مرجع سابق، ص 86.

-عدم مراعاة الإجراءات الأولية:

لقيام الركن المادي لهذه الجريمة يجب أن تتم المعالجة الآلية للبيانات الشخصية دون اتخاذ الإجراءات القانونية الواردة بالمواد 15، 16 من قانون المعلوماتية والحريات[1].

وطبقا لنص المادة 15 فإنه يتعين بالنسبة لمعالجة البيانات الاسمية لحساب الدولة أو الهيئات العامة أو الهيئات المحلية، أو الأشخاص المعنوية الخاصة التي تقوم بإدارة خدمة عامة تنظيم معالجة البيانات بلائحة، بناءا على موافقة من اللجنة الوطنية للمعلوماتية والحريات [2].

أما المادة 16 من قانون المعلوماتية والحريات، فتنص على أنه عندما يتعلق الأمر بمعالجة البيانات لخلاف الجهات المحددة بالمادة 15، فإنه يتعين إخطار اللجنة الوطنية للمعلوماتية والحريات، قبيل إجراء معالجة البيانات ويجب أن ينطوي هذا الإخطار على إقرار بأن المعالجة تتفق ومتطلبات القانون، وعند استلام الجهة الطالبة ما يفيد العلم بوصول الإخطار للجنة، كان في إمكانها البدء في معالجة البيانات، علما بأن هذا لا يعفيها من مسؤوليتها القانونية[3].

وعليه فالمعالجة لحساب أشخاص القانون العام الواردة في المادة 15 تتطلب ترخيصا أما المعالجة التي تتم لحساب أشخاص القانون الخاص فطبقا للمادة 16 يكفي فيها إخطار اللجنة الوطنية للمعلوماتية والحريات ، وكذلك يكفي إخطار مبسط للجنة طبقا للمادة 17فيما لو كانت المعالجة لحساب أشخاص القانون العام أو الخاص، ولا تنطوي على مساس بالحياة الخاصة أو الحريات، وكانت متسقة مع الضوابط التي وضعتها اللجنة حسب ما جاء في المادة 17 [4].

---

[1] - غير أن جانب من الفقه يرى أن نص المادة 226-16جاء عاما ولم يحيلنا إلى المواد 15و16و17، وبالتالي تمتد لتشمل كل إجراء تطلبه القانون.

[2] -

من الهيئات المحلية ولم توافق اللجنة، فليس من الممكن قانونا إصدار اللائحة إلا بعد قرار من إدارتها يوافق عليه مجلس الدولة . راجع عبد الحليم مدحت رمضان، مرجع سابق، ص91.

[3] - محمد أمين أحمد الشوابكة، مرجع سابق، ص88.

[4] - عبد الحليم مدحت رمضان، مرجع سابق، ص 93.

ويتوافر الركن المادي لهذه الجريمة بمجرد إجراء معالجة آلية للبيانات الشخصية بدون ترخيص، حتى وان لم يترتب على ذلك أي نتيجة إجرامية فالجريمة تعتبر جريمة سلوكية لا تتطلب تحقيق نتيجة معينة[1].

ب- الركن المعنوي :

يتخذ الركن المعنوي لهذه الجريمة صورة القصد الجنائي أو الخطأ الجنائي ويتحقق القصد الجنائي العام بعلم الجاني بالصفة الشخصية للبيانات ، وأنه يقوم بإجراء معالجة لهاته البيانات دون مراعاة الإجراءات المنصوص عليها في القانون، أي دون الحصول على ترخيص من اللجنة الوطنية للمعلوماتية والحريات أو إخطارها، ويتعين أيضا أن تتجه إرادة الجاني إلى إجراء المعالجة الآلية ودون مراعاة للإجراءات الأولية التي نص عليها القانون، ولا عبرة بالبواعث .

ويتخذ الركن المعنوي أيضا صورة الخطأ إذا كان ذلك نتيجة إهمال أو رعونة الفاعل حسب نص المادة 16/226 ، وبالتالي يعاقب المشرع على هذه الجريمة سواء اتخذ الركن المعنوي صورة القصد الجنائي أو الخطأ غير العمدي [2].

يعاقب المشرع الفرنسي على هذه الجريمة بعقوبة أصلية تتمثل في الحبس لمدة ثلاث سنوات وغرامة مالية تقدر بثلاثمائة ألف أورو[3].

---

[1] – هدى حامد قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، مرجع سابق ، ص39.

[2] – عبد الحليم مدحت رمضان، مرجع سابق، ص95.عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الالكترونية ، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق ، ص73

[3] – أصبحت العقوبة الأصلية لهذه الجريمة طبقا للقانون 04-801 المتضمن تعديل قانون العقوبات، السجن خمس سنوات وغرامة تقدر بثلاثمائة ألف أورو ، كما أن الأشخاص المعنوية يمكن أن تقوم مسؤوليتها الجنائية وذلك وفقا للقواعد العامة الواردة في المادة121 من قانون العقوبات الفرنسي، بالإضافة إلى عقوبة تكميلية تتمثل في نشر الحكم الصادر في هذا الشأن وفقا للقواعد العامة الواردة في المادة 131-35 والمادة 226-25 ، ويعاقب على الشروع في هذه الجريمة بنفس العقوبة المقررة لارتكاب الجريمة.

2-جريمة عدم اتخاذ الاحتياطات اللازمة في حماية البيانات المعالجة

نص المشرع الفرنسي على هذه الجريمة في المادة 226-17 من قانون العقوبات الفرنسي على أن " كل من أجرى أو حاول إجراء معالجة آلية لمعلومات اسمية ، دون أن يأخذ كل الاحتياطات المجدية لضمان أمن هذه المعلومات، وعلى وجه الخصوص من تشويهها أو إتلافها أو الوصول إليها من شخص غير مصرح له بذلك، يعاقب بالحبس خمس سنوات وغرامة تقدر بمليوني فرنك فرنسي ".

يتضح أنه يتعين لقيام هذه الجريمة توافر ركنين أحدهما مادي وآخر معنوي.

ا-الركن المادي :

يتحقق الركن المادي لهذه الجريمة بإجراء أو محاولة إجراء المعالجة الآلية للبيانات الاسمية دون أخذ الاحتياطات اللازمة لضمان أمن هذه البيانات[1]، ويهدف المشرع بذلك إلى حماية هذه البيانات، خاصة من تشويهها أو إتلافها أو الوصول إليها من شخص غير مصرح له بذلك[2].

ب- الركن المعنوي :

يتخذ الركن المعنوي لجريمة عدم اتخاذ الاحتياطات اللازمة في حماية البيانات المعالجة صورة القصد الجنائي أو الخطأ، وعليه تقع الجريمة سواء اتخذ الركن المعنوي صورة القصد الجنائي أو الخطأ [3]، وعقوبة الفعل في الصورتين واحدة وان يتوقف الامرعلى السلطة التقديرية للقاضي[4].

---

[1] – انطلاقا من المادة 226-17 من قانون العقوبات الفرنسي ، نلاحظ أن المشرع لم يكتف بالعقاب على إجراء المعالجة الآلية للبيانات الاسمية دون أخذ الاحتياطات اللازمة لضمان أمن هذه البيانات ، بل حتى المحاولة والشروع .

[2] – عبد الحليم مدحت رمضان، مرجع سابق، ص 96.

[3] – وبالتالي عاقب المشرع الفرنسي عن عدم اتخاذ الاحتياطات اللازمة في حماية البيانات المعالجة ، حتى ولو وقع نتيجة خطا أو إهمال ، ولم يكتف بالقصد الجنائي ،. للتفصيل راجع عبد الحليم رمضان ، مرجع سابق ، ص96.

[4] – عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية ، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق ، ص74

ثانيا –الجرائم الايجابية الواقعة على البيانات الشخصية

نص المشرع الفرنسي على الجرائم الايجابية للاعتداء على البيانات الشخصية في المواد 226–18الى المادة 226–22 ، وتمثلت تلك الجرائم في جريمة المعالجة غير المشروعة للبيانات وجريمة معالجة بيانات اسمية لأشخاص مصنفين وجريمة حفظ بيانات اسمية خارج المدة المحددة وجريمة الانحراف عن الغرض من المعالجة الآلية للبيانات الاسمية وجريمة الافشاء [1].

1–جريمة المعالجة غير المشروعة للبيانات :

نصت المادة 226–18من ق ع ف على أن " كل من قام بجمع بيانات مخفية أو بصورة غير مشروعة، أو قام بإجراء معالجة لبيانات اسمية تتعلق بشخص طبيعي رغم معارضة هذا الشخص، متى كانت هذه المعارضة تقوم على أسباب مشروعة، يعاقب بالحبس مدة خمس سنوات وغرامة تقدر بمليوني فرنك فرنسي".

يتضح لنا من خلال هذه المادة أنه يتعين لقيام هذه الجريمة توافر ركنين مادي وآخر معنوي.

أ–الركن المادي :

يتمثل الركن المادي في جمع البيانات الاسمية مخفية أو بصورة غير مشروعة أي بوسيلة غير مشروعة، حيث يمنع جمع البيانات بالغش أو التدليس ، وتعد المواقع الوهمية على الانترنت من أخطر وسائل التدليس والغش في البيانات الاسمية عن طريق الخداع أو التجسس [2].

---

[1] – تعد الجرائم المنصوص عليها في المواد 226–18الى المادة 226–22 من العقوبات ، جرائم ايجابية لأنها تكون بسلوك ايجابي متمثل في المعالجة غير المشروعة للبيانات ، أو وجريمة معالجة بيانات اسمية لأشخاص مصنفين ، أو حفظ بيانات اسمية خارج المدة المحددة أو الانحراف عن الغرض من المعالجة الآلية للبيانات الشخصية أو الإفشاء غير المشروع للبيانات الاسمية .

[2] – أمين أحمد الشوابكة، مرجع سابق، ص86.

ويتحقق أيضا بمعالجة بيانات اسمية رغم معارضة صاحب البيانات، متى كانت تقوم على أسباب مشروعة، وبالتالي تقوم الجريمة بجمع بيانات شخصية تتعلق بشخص طبيعي اعترض على معالجتها وفق مبررات معقولة [1].

ويرى جانب من الفقه الفرنسي أن عبارة أسباب مشروعة، التي استخدمها المشرع مطاطة وغير محددة، ومع ذلك أراد المشرع بهذا القيد تأكيد حماية الحياة الخاصة المقررة في المادة 09 من القانون المدني[2].

ب- الركن المعنوي:

تعد هذه الجريمة من الجرائم العمدية ، يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه بوقائع الجريمة

وانصرفت إرادته إلى جمع البيانات الاسمية بصورة غير مشروعة ، أو معالجة بيانات اسمية رغم معارضة صاحب البيانات [3].

لمدة خمس سنوات والغرامة لمقدرة بمائتي ألف أورو [4].

---

[1] - وبالتالي يتحقق الركن المادي إذا قام شخص بمعالجة بيانات اسمية رغم معارضة صاحب البيانات، متى كانت تقوم على أسباب مشروعة، .

[2] - عبد الحليم مدحت رمضان، مرجع سابق، ص98.

[3] – إن جريمة المعالجة غير المشروعة للبيانات ن جريمة عمدية ، لابد فيها من توافر القصد الجنائي العام ، وبالتالي لاتقوم الجريمة إذا كانت المعالجة غير المشروعة ناتجة عن خطا أو إهمال ، ولم يتطلب المشرع القصد الجنائي الخاص

[4]- وكذلك يعاقب بنفس العقوبات المشار إليها، كل من يقوم بمعالجة البيانات الاسمية في مجال الصحة:

-إذا لم يخطر أصحابها بحقهم في الاطلاع عليها وتصحيحها والاعتراض عليها وبطبيعة البيانات ومتلقيها

-أن يتم هذا التصرف رغم معارضة الشخص المعني، أو حينما يقرر القانون رضا واضح وصريح من الشخص المعني حتى ولو كان هذا الشخص متوفى ما دام عدم رضاه قد ثبت قبل الوفاة وبشكل صريح .

2-جريمة معالجة بيانات اسمية لأشخاص مصنفين :

نصت المادة 226-19 على أنه يعاقب كل من قام في غير الحالات المستثناة قانونا بحفظ بيانات اسمية في ذاكرة الكترونية، دون موافقة صريحة من صاحبها البيانات، متى كانت هذه البيانات تظهر بصورة مباشرة أو غير مباشرة الأحوال العرقية، أو الآراء السياسية أو الفلسفية أو الدينية، أو الانتماءات النقابية أو الأخلاق الشخصية، أو متعلقة بالجرائم أو أحكام الإدانة أو التدابير المتخذة ضده ".

ولقيام هذه الجريمة يجب توافر ركنين أحدهما مادي وآخر معنوي.

ا-الركن المادي:

يتحقق الركن المادي لهذه الجريمة بوضع أو حفظ بيانات شخصية دون موافقة صريحة من قبل صاحبها ، وكانت متعلقة بالمعتقدات الدينية أو الاتجاهات السياسية أو الفلسفية، أو الانتماءات النقابية أو بالأخلاق ، متعلقة بالجرائم التي ارتكبها الشخص أو أحكام الإدانة أو التدابير الصادرة ضده [1]، لأنه لايجوز معالجة البيانات المتعلقة بالجرائم والعقوبات إلا للجهات القضائية والسلطات العامة المختصة بتخزين هذه البيانات [2].

---

[1] – وبالتالي تتمثل عناصر الركن المادي في السلوك الإجرامي في هذه يقي الصورة يعاقب كل من حفظ بيانات اسمية في ذاكرة الكترونية في غير الحالات المستثناة قانونا ، ودون موافقة صريحة من صاحبها البيانات، أما محاها فيكمن في البيانات الشخصية المتعلقة بالأحوال العرقية، أو الآراء السياسية أو الفلسفية أو الدينية، أو الانتماءات النقابية أو الأخلاق الشخصية. للتفصيل راجع نعيم مغبغب، مخاطر المعلوماتية والانترنت، المخاطر على الحياة الخاصة وحمايتها، دراسة مقارنة، بدون ناشر، بيروت لبنان ، 1998، ص 25.

[2] – وعليه يعاقب كل من قام في غير الحالات المستثناة قانونا بحفظ بيانات اسمية في ذاكرة الكترونية، دون موافقة صريحة من صاحبها البيانات، فكل حفظ لتلك البيانات دون رضا صاحبها يشكل هذه الجريمة ، لأنه لايجوز معالجة البيانات المتعلقة بالجرائم والعقوبات إلا للجهات القضائية والسلطات العامة المختصة بتخزين هذه البيانات .

ب-الركن المعنوي:

هذه الجريمة من الجرائم العمدية ، يتحقق الركن المعنوي فيها بتوافر القصد الجنائي العام بعنصريه العلم والإرادة ، فيتعين أن يعلم الجاني بأنه يقوم بجمع بيانات شخصية متعلقة بالمعتقدات الدينية أو الاتجاهات السياسية أو الفلسفية، أو بالجرائم والعقوبات ، وأن تتجه إرادته نحو ارتكاب السلوك الإجرامي [1].

يعاقب المشرع الفرنسي على جريمة معالجة بيانات اسمية لأشخاص مصنفين بالحبس خمس سنوات وبغرامة لاتتجاوز مائتي ألف فرنك فرنسي[2].

3-جريمة حفظ بيانات اسمية خارج المدة المحددة

نصت المادة 226-20 من قانون العقوبات الفرنسي على أن " كل من قام من دون موافقة اللجنة الوطنية للمعلوماتية والحريات بحفظ معلومات اسمية، لمدة أكبر من المدة التي سبق طلبها أوالتي تضمنها الإخطار المسبق، يعاقب بالحبس مدة ثلاث سنوات وغرامة مقدرة بثلاثمائة أورو".

ويتبين أنه لقيام هذه الجريمة لابد من توافر ركنين مادي ومعنوي ، كالآتي :

أ-الركن المادي:

يتحقق الركن المادي لهذه الجريمة بحفظ البيانات الشخصية خارج المدة المحددة في الطلب أو الإخطار، ودون موافقة اللجنة الوطنية للمعلوماتية والحريات [3].

---

[1] - يلاحظ أن المشرع الفرنسي اكتفى بالقصد الجنائي العام دون الخاص ، ولاعبرة بالباعث والغرض من ارتكاب هذه الجريمة ، للتفصيل راجع عبد الحليم مدحت رمضان، مرجع سابق، ص81.

[2] - أصبحت العقوبة الأصلية لهذه الجريمة طبقا للقانون 04-801 المتضمن تعديل قانون العقوبات، السجن خمس سنوات وغرامة تقدر بثلاثمائة ألف أورو .

[3] - عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية ، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق ، ص80.

وبناء على ذلك تقع الجريمة إذا كان حفظ هذه البيانات الشخصية لمدة تتجاوز المدة المطلوبة للحفظ ، حيث أن هذه البيانات لا يمكن أن تحفظ لمدة غير محددة إلا في حالات استثنائية محددة قانونا، ذلك أن من ضوابط حفظ البيانات الشخصية، تأقيت عملية حفظها[1].

وتجدر الإشارة إلى أن مبدأ توقيت حفظ البيانات الشخصية يسرى على كافة أنواع البيانات الشخصية، وأيا كانت طبيعتها كقاعدة عامة، واستثناء على هذه القاعدة فإنه لا يسرى على البيانات الصحيحة التي يحتفظ بها إلى ما لا نهاية كاسم الشخص، تاريخ ميلاده [2].

ب-الركن المعنوي :

تعد جريمة حفظ بيانات اسمية خارج المدة المحددة من الجرائم العمدية، التي يتخذ فيها الركن المعنوي صورة القصد الجنائي العام بعنصريه العلم والإرادة فيتعين أن يكون الجاني عالما بأنه يحتفظ ببيانات شخصية، لمدة أكثر من المدة التي سبق طلبها، أو التي تضمنها الإخطار المسبق، وأن يعلم أيضا أن ذلك الاحتفاظ يتم بغير موافقة اللجنة الوطنية للمعلوماتية والحريات كما يجب أن تتجه إرادة الجاني إلى تحقيق ذلك من خلال الاحتفاظ بهذه البيانات [3].

ولا يتطلب المشرع الفرنسي توافر القصد الجنائي الخاص، فلا عبرة بالبواعث التي دفعت الجاني إلى ارتكاب فعل الحفظ غير المشروع للبيانات الشخصية [4].

---

[1] – وقد نصت المادة 28 من قانون المعلوماتية والحريات، على أنه لا يجوز الاحتفاظ بالبيانات الشخصية إلا للمدة المحددة في طلب إقامة نظم المعلومات، أو لمدة تزيد على المدة اللازمة لتحقيق الغرض من تجميع البيانات واحتياجات البرنامج، في الحالات التي تسمح فيها اللجنة الوطنية للمعلوماتية والحريات، بالاحتفاظ بهذه البيانات أكثر من المدة

[2] – عبد الحليم رمضان، مرجع سابق، ص102.

[3] – وعليه هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائية العام ، ولا يتحقق الركن المعنوي للجريمة، إذا تم الحفظ عن طريق الإهمال أو النسيان عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية ، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق ، ص82.

[4] – أسامة قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، دار النهضة العربية القاهرة مصر 1998، ص91.

يعاقب المشرع الفرنسي على جريمة الحفظ غير المشروع للبيانات الاسمية بعقوبة أصلية حددها في نص المادة 226-20 من قانون العقوبات الفرنسي، وهي الحبس لمدة ثلاث سنوات وغرامة لاتتجاوز ثلاثمائة ألف أورو، ويرجع تقدير عقوبة جريمة حفظ بيانات اسمية خارج المدة المحددة في الطلب أو الإخطار لقاضي الموضوع [1].

4-جريمة تغيير الغرض من المعالجة الآلية للبيانات الاسمية

نصت المادة 226-21 من قانون العقوبات الفرنسي على أن " كل من حاز معلومات اسمية بمناسبة قيامه بتسجيلها أو تصنيفها أو نقلها أو أي إجراء آخر من أوجه المعالجة الآلية، إذا غير من الوجهة النهائية المقررة لهذه البيانات وفقا للقانون، أو القرار الصادر بشأنها، أو في الإخطار المسبق على القيام بمعالجة يعاقب بالحبس مدة خمس سنوات وغرامة مالية تقدر بمليوني فرنك .

يتضح من خلال نص المادة 226-21 أنه يتعين لقيام هذه الجريمة توافر ركنين أحدها مادي، والآخر معنوي, على النحو الآتي :

أ-الركن المادي :

يتحقق الركن المادي لهذه الجريمة بتغيير الغرض من المعالجة الآلية للبيانات الشخصية[2] وهدف المشرع من هذا منع أي استخدام غير مشروع من قبل حائز البيانات الاسمية، وذلك باستخدامها في غير الغرض الذي خصصت له[3].

---

[1] – بالإضافة إلى العقوبة الأصلية المشار إليها في المادة 20/226 قرر المشرع الفرنسي عقوبات تكميلية منصوص عليها في المادة226-24 من قانون العقوبات الفرنسي

[2] – والحقيقة أن معالجة البيانات الاسمية لابد وأن يكون لها هدف أو غرض معين بهدف فرض الرقابة من قبل اللجنة الوطنية لتجنب إساءة استخدام البيانات دون الحد من الإمكانيات المتاحة لاستغلال هذه البيانات ، ولابد أن يكون هناك تناسب ما بين المعلومات المعالجة وغرض معالجتها ، على أن يتم الالتزام بذلك الغرض دون تغيير .

[3] – عبد الحليم مدحت رمضان، مرجع سابق، ص103.

وأناط المشرع الفرنسي في المادة 226-21 باللجنة الوطنية للمعلوماتية والحريات، تحديد ما إذا كان فعل الجاني يشكل انحرافا عن الغرض من المعالجة وذلك بالرجوع إلى الطلب المقدم إليها مسبقا، والمحدد فيه الغاية أو الغرض من المعالجة الآلية للبيانات الاسمية، ويستوي أن يكون الشخص حائزا على هذه المعلومات بغرض تصنيفها أو نقلها أو أي غرض أخر[1].

ب-الركن المعنوي :

يتخذ الركن المعنوي في جريمة تغيير الغرض من المعالجة الآلية للبيانات الاسمية، صورة القصد الجنائي العام، والذي يقوم بتوافر العلم والإرادة؛ فيتعين أن يعلم الجاني بأن من شأن فعله أن يشكل انحرافا عن الغرض من المعالجة الآلية للبيانات الاسمية ، وأن تتجه إرادته نحو ذلك[2].

يعاقب المشرع الفرنسي كل من يرتكب جريمة تغيير الغرض من المعالجة الآلية للبيانات الاسمية ، بالحبس خمس سنوات وبغرامة تقدر بمليوني فرنك فرنسي، وقد شدد المشرع عقوبة الحبس والغرامة لكونها تشكل اعتداء جسيم على خصوصية البيانات الاسمية[3].

5-جريمة الإفشاء غير المشروع للبيانات الاسمية

نصت المادة 226-22 من قانون العقوبات الفرنسي على أن " كل من تلقى بمناسبة التسجيل أو التصنيف أو النقل أو أي إجراء آخر من إجراءات المعالجة الآلية، معلومات اسمية من شأن إفشائها الإضرار باعتبار صاحب البيانات أو حرمة حياته الخاصة، وقام بنقلها من دون موافقة المعني بها إلى من لاحق له في العلم بها يعاقب بالحبس سنة وبغرامة مالية تقدر بمائة ألف أورو" .

---

[1] – أسامة عبد الله قايد، مرجع سابق، ص98.

[2] – ولا عبرة بالبواعث التي تدفع الجاني لارتكاب هذه الجريمة أو غايته، سواء تمثلت في مغنم للجاني أو دفع ضرر عنه، أو تحقيق مصلحة الغير.

[3] –أصبحت عقوبة هذه الجريمة طبقا للقانون 04-801 المتضمن تعديل قانون العقوبات، السجن خمس سنوات وغرامة تقدر بثلاثمائة ألف أورو.

ويعاقب بغرامة تقدر بخمسين ألف أورو، إذا وقع الإفشاء المشار إليه في الفقرة الأولى نتيجة لرعونة أو عدم انتباه ولا تسري الدعوة العمومية وفقا للفقرتين السابق الإشارة إليهما، إلا من خلال شكوى المجني عليه أو ممثله القانوني، أومن له صفة في ذلك " .

أ-الركن المادي:

يلزم لقيام الركن المادي لجريمة الإفشاء غير المشروع للبيانات الشخصية بحيازة بيانات شخصية بمناسبة تصنيفها أو نقلها أو علاجها تحت أي شكل من أشكال المعالجة [1]، وأن يكون من شأن إفشاء هذه المعلومات الإضرار باعتبار صاحب الشأن أو حرمة حياته الخاصة, لا يشترط أن تكون مصادر هذه البيانات صحيحة لكي يتحقق الاعتداء.

كما يجب أن يتم الإفشاء دون رضا صاحب البيانات ، ذلك أن هذا الرضا في حالة وجوده يزيل عن الفعل صفة الاعتداء، ويكون سببا لإباحة فعل الإفشاء للبيانات الاسمية، وأن يتم إفشاء هذه البيانات للغير الذي لا يكون له الحق في الإطلاع عليها[2].

وتختلف جريمة الإفشاء غير المشروع للبيانات الاسمية، عن جريمة إفشاء الأسرار المعاقب عليها بالمادة 13/226 من حيث الأركان والنطاق ، فمن حيث الأركان نجد أن المشرع في جريمة

---

[1] – محمد أمين أحمد الشوابكة، مرجع سابق، ص102.

[2] – حيث اشترط المشرع الفرنسي في قانون المعلوماتية والحريات في المادتين 19 و20 ضرورة إخطار اللجنة الوطنية للمعلوماتية والحريات، بأسماء الأشخاص أو الجهات التي يتم إرسال البيانات إليها، وقد تطلب المشرع وجوب أن يكونوا مختصين أو لديهم أهلية تلقي هذه البيانات تحديدا للمسؤولية.

إفشاء الإسرار المعاقب عليها بالمادة 226-13 لا يتطلب لوقوعها أن يحدث اعتداء على الشرف أو الاعتبار أو الحياة الخاصة للمجني عليه ، بخلاف جريمة إفشاء البيانات الاسمية [1].

ومن حيث موضوع الجريمة فإن جريمة الإفشاء غير المشروع للبيانات الاسمية، تشمل إفشاء البيانات الاسمية السرية وغير السرية، على خلاف جريمة إفشاء الأسرار التي لا تشمل إلا البيانات السرية[2].

ب-الركن المعنوي :

يأخذ الركن المعنوي لجريمة الإفشاء غير المشروع للبيانات الاسمية صورة القصد الجنائي أو الخطأ، ويتحقق القصد الجنائي بتوافر العلم والإرادة، فيتعين أن يكون الجاني عالما بأنه يقوم بإفشاء بيانات اسمية تشكل اعتداءا على الشرف والاعتبار أو الحياة الخاصة للأفراد، ويتعين كذلك أن تتجه إرادته نحو تحقيق ذلك وتتحقق صورة الخطأ إذا كان فعل الإفشاء للغير قد وقع نتيجة لرعونة أو عدم انتباه أو ترك للبيانات الاسمية[3].

شدد المشرع الفرنسي العقاب على فعل الإفشاء غير المشروع للبيانات الاسمية بصورة عمديه، حيث عاقب عليها بالسجن خمس سنوات وغرامة تقدر بثلاثمائة ألف أورو، أما إذا ارتكب فعل الإفشاء غير المشروع للبيانات الاسمية بصورة الخطأ، نتيجة لرعونة أو عدم انتباه أو ترك لهذه البيانات الاسمية، فيعاقب المشرع عليها بالحبس ثلاث سنوات وغرامة تقدر بمائة ألف أورو [4]

---

[1] – كما لا يتصور وقوع جريمة إفشاء الأسرار إلا في صورة عمدية، بخلاف جريمة الإفشاء غير المشروع للبيانات الاسمية المشار إليها في المادة 226-22 من قانون العقوبات الفرنسي ، والتي تتحقق بصورة عمدية كما تتحقق أيضا بصورة الخطأ . انظر محمد أمين أحمد الشوابكة، مرجع ، ص103 .

[2] – أحمد حسام طه تمام، مرجع سابق، ص329.

[3] – عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية ، الكتاب الثاني : الحماية الجنائية للتجارة الالكترونية ، مرجع سابق ، ص92.

[4] – ويشترط المشرع لإيقاع العقاب في صورته المتقدمة (العمد أو الخطأ) أن يأتي الجاني لجريمة الإفشاء غير المشروع للبيانات الاسمية ، أي دون رضا المجني عليه صاحب البيانات الشخصية ن لأن هذا الرضا يزيل عن الفعل صفة الجريمة ، ويكون سببا لإباحة فعل الإفشاء للغير.

الفرع الثاني: الحماية الجنائية البيانات الشخصية في التشريعات العربية

أولت بعض التشريعات العربية أهمية لحماية البيانات الشخصية الالكترونية من أبرزها التشريع الجزائري، والتشريع التونسي، على النحو الآتي:

أولا- الحماية الجنائية للبيانات الشخصية الالكترونية في التشريع الجزائري :

تولى المشرع الجزائري توفير حماية جنائية عامة للبيانات الشخصية الالكترونية في إطار قانون العقوبات ، بموجب قانون رقم 15/04 المؤرخ في 10 نوفمبر عام 2004 المتعلق بالجرائم المعالجة الآلية للمعطيات ، من خلال تجريم التلاعب بالمعطيات في المادة 394 مكرر1 والتعامل بالمعطيات غير المشروعة في المادة في المادة 394 مكرر2[1]، الذي يتخذ صورة التعامل في معطيات متحصلة من جريمة ، أو معطيات صالحة لارتكاب جريمة معلوماتية [2].

وتنطبق أيضا جريمة إفشاء الأسرار المنصوص عليها في المادة 301 من قانون العقوبات الجزائري على البيانات الشخصية [3].

إلا أن الفقه يرى أن المادة 301 لا تصلح لحماية البيانات الشخصية الالكترونية ذلك أن محل جريمة إفشاء الأسرار هو البيانات السرية [4]، والتي يشترط فيها أن تكون إما أسرارا رسمية، أو متعلقة ببعض المهن التي تقوم على الثقة [5].

---

[1] – راجع المادة 394 مكرر2 والمادة 394 مكرر2 من قانون العقوبات الجزائري .

[2] – محمد خليفة ، مرجع سابق، ص 210

[3] – تنص المادة 301 بأنه " يعاقب بالحبس من شهر إلى ستة أشهر،وبغرامة من 500 دج إلى 5.000 دج الأطباء والجراحون والصيادلة والقابلات وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلي بها إليهم وأفشوها في غير الحالات التي يوجب عليهم فيها القانون إفشاءها

[4] – محمد رايس،المسؤولية الأطباء المدنية عن إفشاء السر المهني في ضوء القانون الجزائري ، مجلة جامعة دمشق كلية العلوم الاقتصادية والحقوق، المجلد25 العدد الأول ، 2009،ص262.

[5] – محمد أمين أحمد الشوابكة، مرجع سابق، ص104.

وهي بذلك تختلف عن إفشاء البيانات الشخصية الالكترونية، والتي قد تنطوي على بيانات ذات طبيعة سرية، أو بيانات أخرى لا تعد من قبيل الأسرار فالنصوص العقابية الخاصة بجريمة إفشاء الأسرار لا تصلح لحماية البيانات الشخصية التي تكون محلا للمعالجة الآلية[1]، فهما وان اتفقتا في العلة المتمثلة في حماية بيانات الأفراد إلا أنهما تختلفان في الموضوع والمحل[2] .

لذا جاء المشرع الجزائري بحماية جنائية خاصة للبيانات الالكترونية الشخصية في إطار قانون العقوبات، بموجب المواد303 مكرر إلى المادة 303 مكرر3 من القانون رقم23/06المؤرخ في 20 ديسمبر 2006 [3].

1-جريمة المساس بحرمة الحياة الخاصة :

نص المشرع على هذه الجريمة كجنحة في المادة 303 مكرر ق ع ج[4]، ويتطلب القانون لقيام جنحة المساس بحرمة الحياة الخاصة توافر ركن مادي، ومعنوي .

أ-الركن المادي:

يتمثل في السلوك الإجرامي المتمثل في إلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة سرية ، أو صورة شخص في مكان خاص بغير رضاه[5].

---

[1] – يتمثل الركن المادي لجريمة إفشاء الأسرار في قيام الأمين بحكم وظيفته بإطلاع الغير على بيانات سرية بأي طريقة كانت ، أما الركن المعنوي فيتمثل في القصد الجنائي العام المتمثل في العلم دون نية الإضرار .

[2] – محمد أمين أحمد الشوابكة، مرجع سابق، ص105.

[3] – القانون رقم القانون رقم23/06المؤرخ في 20 ديسمبر2006 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات ج ر عدد 84 صادرة في 23 ديسمبر 2006.

[4] – حيث تعاقب المادة 303 مكرر بالحبس من 6 أشهر والى 3 سنوات وبغرامة من 50.000 إلى 300.000 د ج ، كل من تعمد المساس بحرمة الحياة الخاصة بأي تقنية كانت بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة سرية ، أو إلتقاط أو تسجيل صورة شخص بغير رضا صاحبها.

ويعاقب على الشروع في هذه الجنحة بذات العقوبات ، ويضع الصفح حدا للمتابعة الجزائية .

[5] – راجع الفقرة الأولى من المادة المادة303 مكرر من القانون رقم 22/06.

وعليه يقوم الركن المادي على توافر العنصرين الآتيين :

- إلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة سرية أو صورة شخص:

فبالنسبة لالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة سرية ، فكل من أسترق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة مهما كانت نوعيتها، ومهما كانت نوعية المحادثات جرت في مكان خاص أوعن طريق الهاتف، يعد مرتكبا لهذه الجريمة [1].

ويقصد بالمحادثات والمكالمات كل صوت له دلالة معينة متبادل بين شخصين أو أكثر بأي لغة مستعملة، فالمشرع استعمل عبارة أحاديث والذي يفيد تبادل الحديث بين شخص أو أكثر أي ما يفيد المحادثة [2].

والالتقاط يعني ستراق السمع، أي أن يسمع الجاني الحديث بأذنه بغفلة من الضحية ، فوضع الأذن خلف الباب والضحية يتحدث ، أو يختفي وراء شيء معين ، أما تسجيل الحديث فيعني التقاطه لسماعه فيما بعد ، أما نقله [3].

إلى جانب ذلك جرم المشرع إلتقاط أو تسجيل أو نقل صورة شخص في مكان خاص بغير إذن صاحبها أو رضاه ، ويعني إلتقاط الصورة تثبيتها في أجهزة التصوير أو إرسالها إلى مكان آخر ولو كان عاما.

---

[1] – فالجريمة محلها مكالمات أو أحاديث خاصة سرية ، أو صورة شخص. بينما تقع الجريمة وبالخصوص إذا تمت في مكان سري أو خاص لكنه تنتفي في مكان عام .

[2] – وبالتالي إن لم يكن الصوت حديثا أو مكالمة فلا تقع الجريمة ، ويمتد نص المادة إلى إلتقاط حديث فردي كأن ينطق به شخص فسجله لنفسه فيلتقطه الغير.

[3] – وتقع الجريمة بأي وسيلة وتقنية كانت، انطلاقا من عبارة (بأي تقنية كانت) وعليه فقد تتم هذه الجنحة عن طريق أجهزة خاصة أو جهاز الإرسال أو الهاتف، وكل جهاز يكشف عنه التطور العلمي يسمح بالنقل والالتقاط أو التسجيل للمكالمات والأحاديث والصور .

-انعدام الرضا والإذن :

لقد اشترط المشرع الجزائري لقيام هذه الجريمة عدم رضا صاحب الحديث أو الصورة ، فإذا رضي بذلك تنتفي الجريمة ، كما أن المشرع أعتبر أن هاتين الجريمتين جنحة قرر لهما عقوبة الحبس من6أشهر إلى 3 سنوات وغرامة مالية من 50ألف إلى 300ألف دينار ، وعاقب أيضا على الشروع في إركاب هذه الجريمة ، غير أن صفح الضحية يضع حدا للمتابعة الجنائية [1].

ب-الركن المعنوي:

جريمة المساس بحرمة الحياة الخاصة جريمة عمدية ، تتخذ صورة القصد الجنائي العام المتمثل في العلم و الإرادة .

وبالتالي يجب أن يعلم الجاني بأن من شأن فعله أن يشكل إلتقاط أو تسجيل أو نقل مكالمات أو الأحاديث أو صور الأشخاص في أماكن خاصة ، وأن تتجه إرادته نحو ذلك، ولا عبرة بالبواعث التي تدفع الجاني لارتكاب هذه الجريمة أو الغاية.

2- جريمة التعامل بالأشياء المتحصل عليها من الجرائم السابقة :

ينص المشرع الجزائري على هذه الجريمة في المادة 303 مكرر 1 [2] ، ولقيام هذه الجريمة لابد من توافر ركنين مادي يتمثل في التعامل المتحصل عليها من الجرائم السابقة بالإيداع أو الاستعمال أو الاحتفاظ وركن معنوي يتخذ صورة القصد الجنائي ، على التفصيل الآتي:

---

[1] - راجع الفقرات 2، 3 من المادة 303 مكرر من القانون رقم 22/06.

[2] - تعاقب المادة 303 مكرر 1/1 بالعقوبات المنصوص علبها في المادة السابقة كل نمن احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير ، أو استخدم بأي وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها المادة 303 مكرر من هذا القانون . وعندما ترتكب الجريمة عن طريق الصحافة فتخضع للجرائم المحددة في قانون الإعلام . ويعاقب على الشروع في ارتكاب هذه الجنحة بالعقوبات المقررة للجريمة التامة .

أ-الركن المادي:

يتحقق الركن المادي عن طريق الإيداع ، أو الاستعمال أو الاحتفاظ ، فكل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير ،أو أستخدم بأية وسيلة التسجيلات أو الصور أو الوثائق المتحصل عليها فيعاقب بـ 6أشهر إلى 3 سنوات ، وعندما ترتكب الجريمة عن طريق الصحافة فتخضع للجرائم المحددة في قانون الإعلام .

عاقب المشرع عليها بنفس العقوبات المبينة في المادة 303 مكرر، وصفح الضحية يضع حدا

العمل مؤسسة فيخضع هذا الشخص المعنوي لعقوبة الغرامة المحددة في المادة 18 مكرر[1].

يلاحظ أن المشرع قد أورد استثناءات بشأن بعض الجرائم كجرائم الفساد وجرائم تبييض الأموال، والمخدرات ، بحيث سمح قانون مكافحة الفساد بالتصنت واستعمال الأجهزة الإلكترونية لسماع المحادثات الدائرة بين الموظف والأشخاص الآخرين دون علم هذا الموظف ، إضافة إلى هذا سمح المشرع باللجوء إلى إجراء التسرب بالمواد 65 مكرر 11 إلى 65 مكرر 18 بالقانون[2].

عرف المشرع الجزائري التسرب في المادة 65 مكرر 12 بأنه قيام ضابط أو عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة ، بإيهامهم أنه فاعل معهم أو شريك معهم أو كخاف [3].

---

[1] – طبقا للمادة 18 مكرر والمادة 18 مكرر 1 من قانون العقوبات تتمثل في عقوبة الشخص المعنوي في الغرامة مرة إلى5 مرات الغرامة المحددة للشخص الطبيعي ، بالإضافة إلى عقوبات تكميلية ت الجنايات

[2] – كما تناوله المشرع الجزائري كأسلوب للتحري الخاص وأطلق عليه مصطلح الاختراق في المادة 56 من القانون رقم 01/06 المتعلق بالوقاية من الفساد ومكافحته، وكذلك نص قانون الإجراءات الجنائية الفرنسي على هذا الإجراء في المواد 81/706إلى 87/706, و المادتين 7/694 و 9/ 694 .

[3] – راجع المادة 65 مكرر 12 من القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر 155/66 المتضمن قانون الإجراءات الجنائية ، ج ر عدد 84 صادرة في ديسمبر 2006.

ب-الركن المعنوي:

إن جريمة إيداع واستعمال واحتفاظ الصور والوثائق المتحصل عليها جريمة عمدية تتخذ صورة القصد الجنائي العام المتمثل في العلم و الإرادة ، يجب أن يعلم الجاني بأن من شأن فعله أن يشكل جريمة إيداع واستعمال وتسجيل الصور والوثائق المتحصل عليها ، وأن تتجه إرادته نحو تلك الأفعال الإجرامية .

وبالتالي إذا كان إيداع واستعمال واحتفاظ بالصور والوثائق المتحصل عليها كان نتيجة الخطأ دون تعمده ، لاتقوم هذه الجريمة لانتفاء القصد الجنائي .

ثانيا- الحماية الجنائية للبيانات الشخصية في التشريع التونسي :

وفر المشرع التونسي حماية للمعطيات الشخصية في إطار قانون حماية المعطيات الشخصية المؤرخ في 27 جويلية 2004 ، وفي إطار قانون المبادلات والتجارة الالكترونية الصادر في 17أوت 2000.

1- في إطار قانون حماية المعطيات الشخصية:

لقد تضمن القانون المؤرخ في 27 جويلية 2004 المتعلق بحماية المعطيات الشخصية جملة من الأحكام الجزائية ، وتتعلق هذه الجرائم بإحالة المعطيات الشخصية المعالجة إلكترونيا، أو بعدم أخذ التدابير الحماية اللازمة عند معالجتها، كالآتي:

أ- جريمة إحالة المعطيات الشخصية المعالجة إلكترونيا:

اقتضى الفصل 90 من قانون 27 جويلية 2004 أنه "يعاقب بالسجن مدة عام والخطية خمسة آلاف دينار كل من يتولى إحالة المعطيات الشخصية دون موافقة المعني بالأمر أو موافقة الهيئة الوطنية لحماية المعطيات الشخصية في الصور المنصوص عليها بالقانون".

لقيام هذه الجريمة لابد من توافر ركنين مادي ، ومعنوي ، على النحو الآتي :

-الركن المادي:

يتمثل الركن المادي لهذه الجريمة في إحالة المعطيات الشخصية دون موافقة المعني بالأمر أو موافقة الهيئة الوطنية لحماية المعطيات الشخصية.

ولم يشترط المشرع لقيام الجريمة ضرورة حصول ضرر للمعني بالأمر، فمجرد إحالة المعطيات الشخصية المتعلقة به، دون احترام الضوابط القانونية، يعد فعلا غير مشروع، ويرتب المسؤولية الجزائية للجاني.

كما يعاقب الفصل 89 بالسجن مدة عام وبخطية قدرها خمسة آلاف دينار كل من تعمد إحالة المعطيات الشخصية لغاية تحقيق منفعة خاصة أو إلحاق ضرر[1].

وقد يتجسد الاستعمال غير الشرعي للمعطيات الشخصية من جهة أخرى، في نشرها بطريقة تسئ لصاحبها أو لحياته الخاصة ، ويعاقب مرتكبها بالسجن لمدة ثلاثة أشهر وبخطية قدرها ثلاثة آلاف دينار حسب ما أقتضى ذلك الفصل 93 من قانون27 جويلية 2004 [2] . فيمكن إذا أن يشمل العقاب مختلف الأشخاص، الذين قد تتاح لهم فرصة الاطلاع على المعطيات الشخصية بمناسبة أداء مهامهم، بدءا من الممارس الفعلي لنشاط المعالجة إلى أعضاء الهيئة الوطنية لحماية المعطيات الشخصية.

---

[1] – وتختلف الجريمة المنصوص عليها في الفصل 89 عن جريمة الفصل 90 من حيث أنها تقتضي ضرورة توفر قصد جنائي خاص، وهو إرادة تحقيق منفعة خاصة للمخالف أو لغيره أو إرادة إلحاق الضرر بالمعني بالأمر.

[2] – والملاحظ أن الصبغة غير الشرعية للفعل تتأتى من طريقة النشر لا من عملية النشر في حد ذاته، أي أن الأمر هنا

97 الذي اقتضى انطباق الفصل 254 من المجلة الجزائية على المسؤول عن المعالجة والمناول وأعوانهما ورئيس الهيئة الوطنية لحماية المعطيات الشخصية وأعضاءها، الذين يتعمدون إفشاء محتوى المعطيات الشخصية.

-الركن المعنوي:

إن جريمة إحالة المعطيات الشخصية المعالجة إلكترونيا من الجرائم العمدية تأخذ صورة القصد الجنائي العام ، يجب أن يعلم الجاني بأن من شأن فعله أن يشكل جريمة إحالة المعطيات الشخصية الالكترونية، وأن تتجه إرادته نحو ذلك.

ولا تقتضي هذه الجريمة ضرورة توفر قصد جنائي خاص، على خلاف الجريمة المنصوص عليها في المادة 89، متمثل في تحقيق منفعة أو إلحاق ضرر بالمجني عليه، حيث ينص الفصل 89 على معاقبة كل من تعمد الإحالة لتحقيق منفعة خاصة أو إلحاق ضرربالمعني.

ب – مخالفة تدابير حماية المعطيات الشخصية:

تقتضي معالجة المعطيات الشخصية توفير الوسائل الفنية والتقنية اللازمة لحمايتها من مختلف أشكال الاعتداء ، وقد حدد الفصلين 18 و 19 من قانون 27 جويلية 2004 التزامات المشرف على عملية المعالجة في هذا الإطار.

-الركن المادي :

يتمثل الركن المادي لهذه الجريمة في مخالفة الالتزامات والاحتياطات التي يتخذها الشخص الذي سيقوم بمعالجة المعطيات [1].

---

[1] – وقد اقتضى الفصل 19 أنه يجب أن تضمن احتياطات معالجة المعطيات :

– عدم وضع المعدات المستعملة في ظروف أو أما كن تمكن من الوصول إليها من غير مأذون لهم.

–عدم إمكانية قراءة السندات أو نسخها أو تعديلها أو نقلها من قبل شخص غير مأذون له بذلك.

–عدم إمكانية إقحام أي معطيات في نظام المعلومات دون إذن في ذلك وعدم إمكانية الاطلاع على المعطيات المسجلة أو محوها أو التشطيب عليها .

–عدم إمكانية استعمال نظام معالجة المعلومات من قبل أشخاص غير مأذون لهم.

–إمكانية التثبت اللاحق من هوية الأشخاص الذين نفذوا إلى نظام المعلومات التي تم إقحامها وزمن ذلك ومن تولى ذلك.

وتتعلق هذه الالتزامات في غالبها بضرورة تأمين نظام المعالجة المعلوماتية للمعطيات الشخصية لدرء خطر الاطلاع عليها من أشخاص غير مخول لهم ذلك وفي حالة عدم احترام هذه الالتزامات فإن المسؤول عن المعالجة يكون عرضة للعقاب بالسجن مدة ثلاثة أشهر وبخطية قدرها ألف دينار حسب الفصل 94 من قانون 27 جويلية 2004.

-الركن المعنوي:

يتمثل الركن المعنوي لهذه الجريمة في القصد الجنائي العام بعنصريه العلم والإرادة، يجب أن يعلم الجاني بأن من شأن فعله أن يشكل جريمة مخالفة تدابير الحماية ، وأن تتجه إرادته نحو تحقيق ذلك الفعل المجرم[1].

ولا تتطلب هذه الجريمة على غرار الجريمة السابقة، قصد جنائي خاص ، بل يكتفي فيها بالقصد الجنائي العام لقيام الجريمة[2].

2- في إطار قانون المبادلات والتجارة الالكترونية :

نص المشرع التونسي على حماية البيانات في إطار قانون المبادلات والتجارة الالكترونية الصادر في 17 أوت 2000 في الباب السادس , وذلك بتجريم السلوكيات الآتية:

أ- جريمة معالجة البيانات الشخصية بدون إذن صاحب الشهادة :

ينص الفصل 38 من قانون المبادلات والتجارة الالكترونية التونسي على أنه لايمكن لمزود خدمات المصادقة الالكترونية معالجة المعطيات الشخصية إلا بعد موافقة صاحب الشهادة [3].

يتضح من خلال الفصل 38 أن جريمة معالجة البيانات الشخصية بدون إذن صاحب الشهادة تقوم بتوافر ركن مادي، ومعنوي.

---

[1] – هدى قشقوش ، الحماية الجنائية للتجارة الالكترونية غبر الانترنت ، مرجع سابق ، ص 42.

[2] – راجع الفصل 94 من قانون 27 جويلية 2004.

[3] – ويعاقب الفصل 51 كل مخالف لأحكام الفصل 38 هذا بغرامة تتراوح بين1000و10000دينار.

-الركن المادي:

يتحقق النشاط المادي لهذه الجريمة بمعالجة البيانات الاسمية من قبل مزود خدمات المصادقة الالكترونية، دون الحصول على موافقة صاحب الشهادة المعني. إذن يلزم لقيامها توافر عنصرين[1]، يتمثل العنصر الأول في السلوك الإجرامي الذي يتخذ شكل المعالجة للبيانات الاسمية ولم يحدد المشرع التونسي شكل المعالجة [2].

أما العنصر الثاني يتمثل في عدم موافقة صاحب الشهادة المعنية ، أما بالنسبة للقانون الفرنسي ، فيجب أن تتم المعالجة الآلية دون إذن من اللجنة الوطنية للمعلوماتية والحريات، وفقا للمادتين 15 و16 من قانون المعلوماتية والحريات[3].

وبالنسبة لمعالجة البيانات الاسمية لحساب الدولة أو الهيئات العامة أو الهيئات المحلية، أو الأشخاص المعنوية الخاصة التي تقوم بإدارة خدمة عامة، يتم تنظيم معالجة البيانات بلائحة، بناءا على موافقة من اللجنة الوطنية للمعلوماتية والحريات،[4].

والركن المادي لهذه الجريمة يتوافر بمجرد معالجة البيانات بدون موافقة صاحب الشهادة المعنية ، وحتى وان لم يترتب على ذلك أي نتيجة إجرامية فالجريمة من جرائم السلوك المجرد لاتتطلب تحقيق نتيجة إجرامية معينة .

---

[1] -عبد الفتاح حجازي، مقدمة في التجارة الالكترونية العربية ، دار الفكر ،الإسكندرية ، 2006، ص277.

[2] وطبقا لنص المادة 05 من قانون المعلوماتية والحريات الفرنسي، فإن المعالجة للبيانات الشخصية تتحقق إما بجمع هذه البيانات أو تسجيلها أو حفظها أو تصنيفها أو تحليلها أو تعديلها أو محوها، وكذلك كل مجموعة من العمليات من ذات الطبيعة تحمل معالجة لهذه البيانات، بقصد الربط بينهما.راجع للتفصيل الحليم رمضان، مرجع سابق، ص97 وما بعدها.

[3] راجع المادة 15 و16 من قانون المعلوماتية والحريات .

[4] - وفي حالة رفض اللجنة فإنه لا يمكن إصدار اللائحة إلا بناءا على رأي من مجلس الدولة بالهيئات المحلية ولم توافق اللجنة، فلا يمكن إصدار اللائحة إلا بعد قرار من إدارتها يوافق عليه مجلس الدولة.

-الركن المعنوي :

يتخذ الركن المعنوي لهذه الجريمة في صورة القصد الجنائي العام بعلم الجاني بالصفة الاسمية للبيانات، وأن يعلم أيضا بمعالجته بيانات شخصية دون الحصول على إذن من صاحب الشهادة المعني , ويتعين أيضا أن تتجه إرادة الجاني إلى إجراء المعالجة الآلية في أي صورة من صورها المختلفة ودون مراعاة للإجراءات الأولية التي نص عليها القانون[1].

وتتحقق أيضا هذه الجريمة بالخطأ ، حين يخطئ الشخص في تدول البيانات و إجراء المعالجة الآلية للبيانات الشخصية بدون إذن، نتيجة إهماله أو رعونته[2].

ب-جريمة الجمع غير المشروع للمعطيات الشخصية :

نصت عليها الفقرة الأولى من الفصل 39 بقولها لايمكن لمزود خدمات المصادقة الالكترونية أواحد أو أعوان جمع المعلومات الخاصة بصاحب الشهادة إلا إذا كانت ضرورية لإبرام العقد إلا

بعد الرجوع لصاحبها [3] .

ويتضح لنا من خلال الفصل 39 أنه يتعين لقيام جريمة الجمع غير المشروع للبيانات الشخصية توافر ركنين أحدهما مادي والأخر معنوي، على التفصيل الآتي :

---

[1] – هدى قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، مرجع سابق ، ص 40.

[2] – يتخذ الركن المعنوي لهذه الجريمة في صورة القصد الجنائي العام بعنصريه العلم والإرادة . وتتحقق أيضا هذه الجريمة بالخطأ ، حين يخطئ الشخص في تدول البيانات و
رعونته . لكن المشرع لم يتطلب القصد الجنائي الخص ، فلا عبرة بالبعث من ارتكاب هذه الجريمة للتفصيل راجع عبد الفتاح حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني :الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص277 .

[3] –وعاقب الفصل 51 كل مخالف للفصل 39 بغرامة تتراوح بين 1000و10000دينار.

-الركن المادي:

يتحقق الركن المادي لهذه الجريمة بجمع البيانات الشخصية من قبل مزود خدمات المصادقة الالكترونية أواحد أعوانه لغير إبرام العقد أو تحديد محتواه أو تنفيذه أو إعداد أو إصدار الوثيقة .

ولا يمكن استعمال المعطيات المجمعة لغير الغاية المذكورة أعلاه من قبل المزود أو غيره إلا إذا تم إعلام صاحب الشهادة بذلك ولم يعارض [1].

حيث يمنع جمع البيانات عن طريق الغش أو التدليس، كما تمنع المعالجة عند معارضة صاحب البيانات، متى كانت تقوم على أسباب مشروعة [2].

-الركن المعنوي :

يأخذ الركن المعنوي في جريمة الجمع غير المشروع للبيانات الشخصية صورة القصد الجنائي العام، بعنصريه العلم والإرادة، فيتعين أن يعلم الجاني بأنه يقوم بجمع غير مشروع البيانات الشخصية وأن تتجه إرادته إلى تحقيق ذلك [3].

و لم يشترط المشرع التونسي قصد جنائي خاص، لذا فإن الجريمة تقوم بتوافر القصد الجنائي العام إلى جانب الركن المادي [4].

---

[1] – عبد الفتاح بيومي حجازي ، مقدمة في التجارة الالكترونية العربية ، مرجع سابق ، ص277

[2] – عبد الحليم مدحت رمضان، مرجع سابق، ص100-101.

[3] _

هذه الجريمة .

[4] – وعليه اكتفى المشرع التونسي بالقصد الجنائي العام دون القصد الجنائي الخاص ، إذن لم يهتم بالباعث والغرض من ارتكاب هذه الجريمة عبد الفتاح بيومي حجازي ، مقدمة في التجارة الالكترونية العربية ، مرجع سابق، ص271 وما بعدها .

ج-جريمة إفشاء البيانات الشخصية :

ينص الفصل 52 من القانون على أنه " يعاقب طبقا لأحكام الفصل 254 من المجلة الجنائية مزود خدمات المصادقة الالكترونية وأعوانه الذين يفشون أو يحثون أو يشاركون في إفشاء المعلومات التي عهدت إليهم ، في إطار تعاطي نشاطاتهم باستثناء تلك التي رخص صاحب الشهادة كتابيا أو الكترونيا في نشرها أو الإعلام بها ، أو في المجالات المنصوص عليها في التشريع الجاري العمل به. ويتضح لنا أنه يتعين لقيام هده الجريمة توافر ركنين هما :

-الركن المادي :

يتمثل الركن المادي في إفشاء مزود خدمات المصادقة الالكترونية أو أحد أعوانه للمعلومات التي عهدت إليهم في إطار نشاطاتهم, سواء، باستثناء تلك التي رخص صاحب الشهادة كتابيا أو الكترونيا في نشرها أو الإعلام بها أو في الحالات المنصوص عليها في التشريع الحالي[1].

ولم يكتف المشرع التونسي كنظيره الفرنسي بتجريم إفشاء البيانات الشخصية بل جرم المشاركة في عملية الإفشاء أو التحريض عليها، وهوما يعني رغبة المشرع في تحقيق حماية فاعلة [2].

-الركن المعنوي :

يأخذ الركن المعنوي لجريمة الإفشاء غير المشروع للبيانات الاسمية صورة العمد بتوافر القصد الجنائي العام الذي يقوم بتوافر العلم والإرادة، فيتعين أن يكون الجاني عالما بأنه يقوم بإفشاء بيانات اسمية ، وأن تتجه إرادته نحو ذلك [3].

---

[1] -عبد الحليم رمضان، مرجع سابق، ص105.

[2] - وجدير بالذكر إن المشرع التونسي لم يحدد عقوبة لهذه الجريمة, بل أحال على عقوبة جريمة إفشاء الأسرار بالفصل 254 من المجلة الجنائية . راجع عبد الفتاح حجازي، مقدمة في التجارة الالكترونية العربية ، مرجع سابق ، ص273

[2] - عبد الفتاح حجازي، النظام القانوني للتجارة الالكترونية،الحماية الجنائية للتجارة الالكترونية ،مرجع سابق ، ص319.

د-جريمة الاعتداء على بيانات مشفرة :

ينص عليها المشرع التونسي في الفصل 48 بقولها يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية، والمتعلقة بإمضاء غيره بالسجن من6أشهر إلى عامين وبغرامة بين 1000و10000دينار، أو بإحدى هاتين العقوبتين. ولهذه الجريمة ركنان مادي ومعنوي يتمثلان في مايلي :

-الركن المادي :

يتمثل الركن المادي لهذه الجريمة في فض مفاتيح التشفير المتعلقة بالتوقيع الالكتروني، أي كشف البرامج الخاصة بتشفير التوقيع الالكتروني, وذلك بنقل التوقيع من صورة مكتوبة إلى صورة رقمية [1].

وهذه الجريمة من جرائم السلوك المجرد لا يتطلب فيها تحقق نتيجة إجرامية معينة ، بل تقوم بمجرد فض الشفرة المتعلقة بالتوقيع الالكتروني , دون انتظار حصول ضرر بالمجني عليه[2].

_الركن المعنوي :

هذه الجريمة من الجرائم العمدية التي تتطلب لقيامها القصد الجنائي العام بعنصريه العلم والإرادة ، وبالتالي يجب أن يعلم الجاني أن ذلك الفعل محظورا وفقا للقانون و مع ذلك تتصرف إرادته إلى فعل الاعتداء على البيانات المشفرة , وكذلك إلى قبول النتيجة المترتبة على فعله بوصفها مخالفة للقانون [3].

---

[1] -هدى قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، مرجع سابق ، ص 64.

[2] - عبد الفتاح حجازي، مقدمة في التجارة الالكترونية العربية مرجع سابق ، ص276 .

[3] - لا يتصور وقوع جريمة الاعتداء على بيانات مشفرة بطريق الخطأ لأن فض تشفير التوقيع الالكتروني يجب أن يكون عن علم و إرادة دون تطلب نية أو قصد جنائي خاص، فهي من الجرائم العمدية يجب فيها توافر القصد العام .

الباب الثاني

الحماية الجنائية الإجرائية للتجارة الالكترونية

الباب الثاني

مدى كفاية الحماية الجنائية الإجرائية للتجارة الالكترونية

أثارت الجرائم الإلكترونية لاسيما جرائم التجارة الالكترونية بعض المشكلات فيما يتعلق بالقانون الجنائي الموضوعي بحثا عن إمكانية تطبيق نصوصه التقليدية على الجرائم الالكترونية، و كذلك أثارت العديد من الإشكالات في نطاق القواعد الإجرائية التقليدية تعرقل عمل أجهزة العدالة في مواجهتها [1]

جنائي ومدى سلطة المحكمة في قبول تقدير الدليل لالكتروني .

إن الطبيعة الخاصة لجرائم التجارة الالكترونية لابد أن تنعكس على قانون الإجراءات الجزائية فيلزم على الدول أن تنشئ قواعد إجرائية حديثة تتمشى مع طبيعة هذه الجرائم ، ولهذا اتجهت بعض التشريعات كالتشريع الإنجليزي والأمريكي والجزائري [2]، إلى تعديل بعض قواعدها الإجرائية

ا .

وعليه سنبحث هذه الحماية الإجرائية للتجارة الالكترونية قبل مرحلة المحاكمة (الفصل الأول) وفي مرحلة المحاكمة (الفصل الثاني).

---

[1] –حيث وضعت نصوص قانون الإجراءات الجنائية لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجميع الأدلة مع خضوعها لمبدأ حرية الاقتناع الشخصي . على خلاف الجريمة المعلوماتية وجرائم ة عالية للتعامل معها.

[2] – عدل المشرع الجزائري القواعد الإجرائية لتتلاءم مع الجريمة المعلوماتية بالقانون رقم 14/04 الموافق 10نوفمبر 2004 المعدل والمتمم للأمر رقم 66 /155 الموافق 8يونيو سنة 1966م المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية للجمهورية الجزائرية العدد 71 الموافق لـ 10 نوفمبر 2004 ، وبالقانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 155/66 الموافق ل 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية.

الفصل الأول

الحماية الجنائية الإجرائية للتجارة الالكترونية قبل مرحلة المحاكمة

رأينا أن جرائم التجارة الالكترونية أثارت العديد من الإشكالات الإشكاليات القانونية والعملية في نطاق القواعد الإجرائية التقليدية من أهمها تلك المتعلقة بإجراءات البحث والتحري ، والتحقيق الابتدائي .

إذ يواجه أجهزة الضبط القضائي صعوبات ومشاكل عملية في مواجهة هذه الجرائم الالكترونية ترجع إلى ن ضعف خبرتهم في هذا المجال، وهذا ما جعل أغلب الدول الأجنبية ، وبعض الدول العربية تنشئ ضبطية قضائية متخصصة في الجرائم المعلوماتية بما فيها جرائم التجارة الالكترونية وتخويلها اختصاصات وسلطات معينة عادية واستثنائية ، كما تم إنشاء على المستوى الدولي والأوربي بالانتربول الاوربول على التوالي .

كما تثير جرائم التجارة الالكترونية إشكاليات قانونية في مرحلة التحقيق الابتدائي متعلقة بمدى قابلية نظم الحاسوب والانترنت للتفتيش والضبط ، كما أن إجراءات جمع الأدلة تتم في كثير من الدول في إطار النصوص التقليدية ، مما بترتب عليه الكثير من المشكلات بالنسبة لضبط أدلة هذه الجرائم ، والتي قد تتعدد أماكن ارتكابها داخل الدولة الواحدة، أو يمتد نطاقها لشمل الكثير من الدول فيتعذر بذلك اتخاذ إجراءات جمع الدليل بشأنها.

وعليه سنبحث الحماية الجنائية للتجارة الالكترونية في مرحلة البحث التمهيدي من خلال الضبطية القضائية المختصة بمكافحة جرائم التجارة الالكترونية واختصاصاتها (المبحث الأول) ثم نبحث الحماية الجنائية للتجارة الالكترونية في مرحلة التحقيق الابتدائي من خلال التفتيش والضبط (المبحث الثاني).

المبحث الأول

الحماية الجنائية للتجارة الالكترونية في مرحلة البحث والتحري

خول القانون مهمة البحث التمهيدي (جمع الاستدلالات)لأجهزة الضبط القضائي ومن أجل ذلك خولهم اختصاصات وسلطات متنوعة وعديدة ، حيث يقوم هؤلاء بدور فعال في ضبط أدلة الجريمة ومرتكبيها ، وذلك بهدف مساعدة أجهزة التحقيق القضائي في الوصول إلى أدلة الجريمة[1].

ويواجه أجهزة الضبط القضائي صعوبات ومشاكل عملية في مواجهة هذه الجرائم الالكترونية إذ أصبح ن
ضعف خبرتهم في هذا المجال [2] . ولذلك تطلب الأمر إنشاء ضبطية قضائية متخصصة في الجرائم المعلوماتية (المطلب الأول)، وتخويلها اختصاصات وسلطات معينة(المطلب الثاني) .

المطلب الأول: الضبطية القضائية المختصة بمكافحة جرائم التجارة الالكترونية

نظرا لظهور وانتشار جرائم الانترنت، قررت الدول مواجهتها بإنشاء أجهزة متخصصة ومنها إنشاء شرطة متخصصة سواء على المستوى الوطني أو الدولي [3]، وهذا ما دعت إليه الاتفاقية الأوربية لجرائم الانترنت ، وكذلك المؤتمر المنعقد في السوريون بباريس بتاريخ 19/1/ 2005 تحت عنوان الشرطة والانترنت[4].

---

[1] – بشأن أجهزة واختصاصات الضبط القضائي راجع الفصل الأول المعنون بالضبط القضائي من الباب الأول المعنون بالحث والتحري من المواد 12 إلى 28 من قانون الإجراءات الجنائية الجزائري .

[2] – نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، دار الفكر الجامعي، الإسكندرية ، 2007 ، ص 97.

[3] – تعرف هذه الأجهزة بشرطة الانترنت (police de net) أو (cyber policet) ، وهي عبارة عن ضبطية قضائية تتولى مهمة جمع الاستدلالات والتحري في العالم الافتراضي، ولا تعتمد على التدريبات المادية أو الفيزيو
على قوة تكوين البناء العلمي والتكنولوجي لإفرادها. راجع جميل عبد الباقي ، الجوانب الإجرائية لجرائم الانترنت ، دار النهضة العربية ، القاهرة مصر 2002، ص77.

[4] – نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية ، 2007 ،ص107.

الفرع الأول: على المستوى الوطني

نظرا للتزايد المستمر لجرائم الانترنت وخاصة جرائم التجارة الالكترونية، قررت بعض الدول سواء الأجنبية أو العربية وضع شرطة متخصصة لمكافحتها [1].

أولا-التشريعات الأجنبية:

ومن أبرز الدول الأجنبية التي بادرت إلى إنشاء شرطة متخصصة في مكافحة جرائم الانترنت الولايات المتحدة الأمريكية وبريطانيا وفرنسا [2]، كالآتي:

1-في الولايات المتحدة الأمريكية :

بسبب تزايد ظاهرة جرائم الانترنت والتجارة الالكترونية في الولايات المتحدة الأمريكية سارعت إلى إنشاء أجهزة ضبط قضائي متخصصة في مكافحة الانترنت تتمثل فيما يلي:

أ- قسم جرائم الحاسوب وجرائم حقوق الملكية الفكرية:

وتم إنشاء قسم جرائم الحاسوب وجرائم حقوق الملكية الفكرية سنة 1991[3]، ويختص بالكشف عن جرائم الكمبيوتر وحقوق الملكية الفكرية وملاحقة مرتكبيها.

ب- وحدة جرائم الإنترنت:

وهي وحدة متخصصة بالتحقيق في جرائم الملكية الفكرية وجرائم الانترنت ويترأسها مدير مساعد مكتب التحقيقات الفيدرالي ولها ذات مرتبة وحدة التفتيش [4].

---

[1] - نافذ ياسين، مرجع سابق، ص456.

[2]- المرجع نفسه ، ص456.

[3] - حيث كان هذا القسم تابعا لوزارة العدل الأمريكية وفي عام 1996 ثم أصبح قسما مستقلا نتيجة لتضخم أعماله للتفصيل راجع عم بن يونس الجرائم الناشئة عن استخدام الانترنت ، دار النهضة العربية القاهرة مصر ، 2004، ص814.

[4] - نبيلة هبة هروال ، مرجع سابق ، ص108-109.

ج- مكتب رئيس التكنولوجيا:

ويختص بتسيير مختلف المشروعات التكنولوجية وملاحقة مرتكبي جرائم الحاسوب كالملاحقة الشهيرة المسماة بكارنيفور وأيضا تلك المسماة بالمصباح العجيب [1]، وهو مكتب تابع مباشرة لمدير مكتب التحقيقات الفيدرالي.

د- المركز الوطني لحماية البنية التحتية:

وهو تابع للمباحث الفيدرالية الأمريكية، والذي يتقاسم مهامه مع وزارة الدفاع الأمريكية ويتكون من فريق سري يصل أعضائه إلى 125 رجلا حكوميا [2].

هـ- مركز تلقي شكاوى الاحتيال عبر الانترنت:

ويدار من طرف مكتب التحقيقات الفيدرالي الأمريكي بالاشتراك مع المركز الوطني لجرائم الياقات البيضاء، حيث يقوم بالربط بين معلومات يتلقاها من ضحايا جرائم الانترنت فيعد منها ملف يسلمها لجهات تطبيق القانون [3].

و- وكالة مكافحة القرصنة المعلوماتية :

ومهمتها مكافحة القرصنة المعلوماتية بالتنسيق مع المركز الوطني لحماية البنية التحتية والتابع للمباحث الفيدرالية الأمريكية والتي تقوم بدور مهم في مواجهة جرائم الانترنت [4].

---

[1] – نبيلة هبة هروال ، مرجع سابق ، ص109.

[2] – تعود نشأة هذا المركز إلى تقرير جمعية العمل حول جرائم الانترنت والمقدم إلى الرئيس "بيل كلينتون والذي حددت من خلاله البن التحتية التي تعتبر هدفا للهجمات والاعتداء عبر الانترنت وهي الاتصالات والكهرباء والغاز والبترول ووسائل النقل والبنوك والمؤسسات الاقتصادية والمياه النقية ومصالح الاستعجال والمصالح الإدارية والاجتماعية .

[3] –حسن بن سعيد بين سيف الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت (دراسة مقارنة) ، رسالة مقدمة لنيل درجة الدكتوراه ، جامعة عين شمس كلية الحقوق ، 2007، ص350.

[4] – عمر محمد أبو بكر بن يونس مرجع سابق، ص815.

2- في بريطانيا:

خصصت بريطانيا وحدة تجمع نخبة من رجال الشرطة المتخصصين في البحث والتنقيب عن الجرائم المرتبطة بالإنترنت، كالجرائم الجنسية وخاصة الواقعة على الإحداث.

وتضم هذه الوحدة 80 مفتشا، 40 منهم متمركزين في لندن ضمن الوحدة الوطنية لمكافحة جرائم التقنية العالية، و40 موزعين على الوحدات المحلية الأخرى.

وتتلخص مهام هذه الوحدة في متابعة مرتكبي الجرائم الجنسية غبر الانترنت خصوصا تلك الواقعة على الأحداث، وكذلك قراصنة المعلومات، وجرائم نشر الفيروسات [1].

3- في فرنسا :

لعبت فرنسا دورا هاما على المستوى الوطني والدولي في مكافحة جرائم الانترنت لاسيما جرائم التجارة الالكترونية، حيث أنشأت فرنسا عدة وحدات ومراكز متخصصة وغير متخصصة ضمن الشرطة [2]، والدرك الوطني لمكافحة جرائم الانترنت بجميع صورها ، كالآتي :

أ- على مستوى مصالح الشرطة :

وتشمل المراكز المتخصصة على مستوى الشرطة الفرنسية على مايلي :

- القسم الوطني لقمع جرائم المساس بالأموال والأشخاص :

بدأ هذا القسم مهامه سنة 1997 وتلقى حوالي 3000 بلاغ خلال عام 2004، ويتألف من 6 محققين مختصين في التحقيق في الجريمة المعلوماتية، ويقوم هذا القسم بمعالجة الجرائم مع إحالة القضايا الأخرى التي يكون المشتبه فيه معروفا إلى الجهات القضائية المختصة [3].

---

[1] - نبيلة هبة هروال، مرجع سابق ، ص 111.

[2]- إلى جانب المراكز المتخصصة في مكافحة جرائم الانترنت، توجد مراكز غير متخصصة، من أهمها الإدارات الإقليمية للشرطة القضائية، وفريق حماية الأحداث من جرائم الانترنت.

[3] - نافذ ياسين، مرجع سابق، ص460. نبيلة هبة هروال ، مرجع سابق ، ص122.

-المركز الوطني لمكافحة جرائم تكنولوجيا المعلومات والاتصالات:

تم إنشاء هذا المركز الوطني بموجب مرسوم وزاري رقم 405/2000 في 15/5/ 2000 على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية، ويتمتع باختصاص وطني لمكافحة هذه الجرائم المستحدثة، ويمارس هذا المكتب من خلال وحدة العمليات ووحدة المساعدة التقنية ووحدة التحليل والتوثيق العملي[1].

ويكلف هذا المركز الوطني وفقا للمادة 03 من المرسوم السابق بملاحقة مرتكبي الجرائم المرتبة بتكنولوجيا المعلومات والاتصالات إضافة إلى تقديم يد المساعدة للشرطة القضائية في إجراءات التحقيق في جرائم تكنولوجيا المعلومات والاتصالات [2].

ب- على مستوى مصالح الدرك الوطني :

وينعقد الاختصاص لرجال الدرك الوطني في مكافحة جرائم الانترنت على مستويين : على مستوى الاختصاص الوطني ، على مستوى الاختصاص الإقليمي ، على النحو الآتي :

-على مستوى الاختصاص الوطني :

ونجد على مستوى الاختصاص الوطني المراكز الآتية :

---

[1] – نافذ ياسين، المرجع السابق، ص460

[2] - تنص المادة 03 من المرسوم 405/2000 المتعلق بالمركز الوطني لمكافحة جرائم تكنولوجيا المعلومات والاتصالات على مايلي :

L'office est chargé":

1-D'animer etdecooronner .au niveau national lamiseen œuvre opérationnelle de l'alute contre les auteurs et complices d'infractions et spécifique a la criminalité liteaux technologies l'information et de communication.

2- De procéder a la demande de l'autorité judiciaire atours actes d'enquête et de travaux techniques" .

*** قسم الانترنت التابع للمصلحة التقنية للبحوث القانونية والوثائقية :**

وتم إنشاؤه عام 1998، ويختص بجمع الأدلة الرقمية(preuve numériques) ويصل عدد أفراده إلى 14 شخص مختصين ي مجال تقنية المعلومات فيهم 8 مهندسين و 6 تقنيين.

***المركز الوطني لتحليل الصور الإباحية :**

ولقد تم إنشاؤه في أكتوبر 2003 ، ويختص بجمع وترتيب الصور التي يتم ضبطها أثناء .[1]

***القسم المعلوماتي الالكتروني التابع لمعهد البحوث الجنائية للدرك الوطني :**

ولقد تم إنشاؤه عام 1992 ، ويختص بتحليل بيانات الحاسوب في إطار التحقيقات القضائية المتعلقة بالأعمال الاقتصادية والمالية ، وبالتالي يقوم بتقديم المساعدة التقنية للدرك الوطني .

***على مستوى الاختصاص الإقليمي:**

وعلى مستوى الاختصاص الإقليمي نجد المراكز الآتية[2]:

-الوحدات الإقليمية ووحدات البحوث:

إذ تساهم الوحدات الإقليمية ووحدات البحوث إلى جانب الوحدات المركزية السابقة في مكافحة جرائم الانترنت على المستوى الإقليمي.

-وحدات أقسام الاستعلامات والتحقيقات القضائية :

وتتركز أعمال هذه الوحدات على تبادل الخبرات التقنية وتبادل الاختصاصات بين رجال الدرك

---

[1] – نافذ ياسين، مرجع سابق، ص461

[2] – المرجع نفسه ، ص138-139.

والى جانب وحدات الشرطة والدرك المختصة بمكافحة جرائم الانترنت، توجد خلية استقبال وتحليل الانترنت والتي تم إنشاؤها سنة 1998 من قبل المديرية العامة للجمارك [1].

ثانيا– بعض التشريعات العربية:

للحد من خطورة جرائم الانترنت أوجدت بعض الدول العربية أجهزة ضبط قضائي لمكافحتها، ومن أبرزها الجزائر والإمارات العربية المتحدة، ومصر على النحو الآتي :

1– في الجزائر والإمارات العربية المتحدة:

لمكافحة جرائم الانترنت لاسيما جرائم التجارة الالكترونية والحد من خطورتها، طبقت الإمارات العربية المتحدة نظام الرقيب (proxy) من اجل إحكام الرقابة على شبكة الإنترنت، عن طريق القيام بمراجعة نوعية الخدمات المقدمة لمنع ظهور أي من تلك الخدمات المحظورة [2].

أما في الجزائر فاستحدث المشرع الجزائري الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بموجب قانون رقم 09–04 المتعلق بالوقاية من جرائم الاتصال والمعلومات ومكافحتها [3]، في المواد 13 و14 من هذا القانون .

وتتولى هذه الهيئة وفقا للمادة 14 تنشيط وتنسيق عمليات بالوقاية من جرائم الاتصال والمعلومات ومكافحتها ، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية ، وأيضا وتبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم .

---

[1] – تختص هذه الخلية بتأمين الرقابة على الانترنت والبحث عن الاحتيال في ميدان التجارة الالكترونية ومكافحة غسيل الأموال عبر الانترنت وكذا تجارة الممنوعات عبر شبكة الانترنت .

[2] – جميل عبدالباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002 ص78.

[3] – وفقا للمادة 2/13 من قانون 09–04تحدد تشكيلة هذه الهيئة الوطنية وتنظيمها وكيفيات سرها عن طريق التنظيم.

كما أنشأت الجزائر مركز لمكافحة جرائم الانترنت على مستوى الدرك الوطني في إطار مسايرتها للتطور التكنولوجي وما يصاحبه من أنواع جرائم الانترنت[1].

2- في مصر:

في إطار مكافحة جرائم الانترنت استحدثت مصر أيضا الإنترنت كالإدارة العامة لمباحث الأموال العامة ، والإدارة العامة للتوثيق والمعلومات، وكذلك الإدارة العامة للمصنفات الفنية وكذلك الإدارة العامة لمكافحة جرائم الحاسب وشبكات المعلومات [2].

وتعد الإدارة العامة لمكافحة جرائم الحاسب وشبكات المعلومات من أهم الأجهزة المتخصصة التي تم إنشاؤها القرار رقم 13507 لسنة2002، وهي تابعة الإدارة العامة للتوثيق والمعلومات وتتكون من ضباط متخصصين في تكنولوجيا الحاسبات والانترنت [3].

وتقسم هذه الإدارة العامة لمكافحة جرائم الحاسب وشبكات المعلومات إلى: قسم العمليات قسم وقسم البحوث والمساعدات الفنية ، على النحو الآتي :

أ- قسم العمليات :

وهو قسم يختص بالاشتراك مع الأجهزة المختصة بمكافحة جرائم الحاسوب والانترنت والتنسيق مع الجهات المختصة لإجراء التحريات وأعمال الضبط [4].

---

[1] - أيمن عبد الحفيظ عبد الحميد، إستراتيجية مكافحة جرائم الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه، أكاديمية الشرطة، بدون سنة طبع، ص 455.

[2] - نافذ ياسين، المرجع السابق، ص452 وما بعدها.

[3] - وهي تابعة للإدارة العامة للمعلومات والتوثيق، وتخضع للإشراف المباشر لمدير الإدارة العمة وتشرف عليها فنيا مصلحة الأمن العام ، وتقوم بوضع خطة تأمين ورقابة الشبكات المعلوماتية لمنع وقوع هذه الجرائم واتخاذ الإجراءات.

[4] - نبيلة هبة هروال، مرجع سابق ، ص 143.

ب-قسم البحوث والمساعدات الفنية :

ويقوم بإعداد البحوث الفنية والقانونية في مجال تأمين نظم وشبكات المعلومات ودراسة الظواهر الإجرامية المتعلقة بجرائم الحاسوب والانترنت ، ويقوم بتقديم الدعم الفني في القضايا المرتبطة بجرائم الحاسوب والانترنت [1].

الفرع الثاني: على المستوى الأوربي والدولي

ولما كانت جرائم التجارة الالكترونية عابرة للحدود، كانت الحماية الوطنية غير كافية، لذا وجب مكافحتها على المستوى الولي ، فالتعاون الدولي أصبح ضرورة لمكافحة هذه الجرائم الخطيرة، ولقد ظهر هذا التعاون في أجهزة أوربية ودولية لمكافحة جرائم الانترنت [2].

ومن صور هذا التعاون القضائي ،ومن أهم صوره التعاون الدولي الشرطي في مجال البحث وتبادل المعلومات بين سلطات التحقيق ، فالتعاون الدولي يحقق أهداف لايمكن للشرطة الإقليمية تحقيقها في مكافحة جرائم الانترنت.

أولا-أجهزة الضبط القضائي على المستوى الدولي:

[1] – أيمن عبد الحفيظ عبد الحميد، مرجع سابق، ص 455.

[2] – لم يعد ينظر إلى التعاون باعتباره خرق لسيادة الدول بقدر ما أصبح يعني التعاون بين سيادات الدول ترمي جميعها إلى تشديد وتفعيل حلقات مكافحة الجريمة العابرة للحدود بصفة خاصة .

من أهم الأجهزة المكلفة بمكافحة الإجرام
"المنظمة الدولية للشرطة الجنائية" أو ما تسمى بالانتربول التي مقرها باريس[1].

وتهدف هذه المنظمة إلى تأكيد وتشجيع التعاون المتبادل بين سلطات البوليس في الدول الأطراف أن تسهم على
نحو فعال في منع ومكافحة جرائم القانون العام[2].

وتقوم هذه المنظمة الدولية بتجميع كافة البيانات والمعلومات المتعلقة بالجريمة والمجرم من خلال المكاتب المركزية الوطنية للشرطة الجنائية الدولية المتواجدة في أقاليم الدول الأعضاء كما أنها تعمل على ضبط وملاحقة المجرمين الهاربين وتسليمهم إلى الدولة التي تطلب تسليمهم، وهي بذلك متخصصة بمكافحة الجرائم ذات الطابع الدولي، وخاصة تلك المتعلقة بالعنف ضد الأشخاص والجرائم الواقعة على الأموال، وهي كذلك تختص بمكافحة الإجرام المنظم العابر للحدود كجرائم الإنترنت وخاصة المتعلق بالاستغلال الجنسي للأطفال[3].

ومن بين الانجازات التي قامت بها المنظمة الدولية للشرطة الجنائية (بالانتربول) العملية التي قامت بها بالاشتراك مع المباحث الفيدرالية الأمريكية وكذا الشرطة الانكليزية، والتي أحرزت فيها انجازات كبيرة عام 1998، إذ حققت من خلالها تفكيك موقع منشور عليه أكثر من (75000) صورة سلبية لدعارة الأطفال، وكذا القبض على عشرات الأشخاص[4]، وكذا تلك العملية التي يتم

---

[1] – تم إنشاء هذه المنظمة سنة 1923 تحت اسم اللجنة الدولية للشرطة الجنائية وذلك للتنسيق بين أجهزة الشرطة في الدول الأوربية في مجال مكافحة الجريمة، وتم إيقاف نشاطها أبان الحرب العالمية الثانية، ثم أعيد فتحها خلال مؤتمر فينا تحت اسم "منظمة الشرطة الجنائية الدولية" سنة 1956، وهي تظم 177 أجهزة هي ، الجمعية العامة، اللجنة التنفيذية، الأمانة العامة، وجهاز المستشارين والمكاتب المركزية الوطنية. ولمزيد من التفاصيل راجع د. علاء الدين شحاتة، التعاون الدولي في مجال مكافحة الجريمة، القاهرة، 2000، ص174 وما بعدها. عبد الواحد محمد الفار، الجرائم الدولية وسلطة العقاب عليها، دار النهضة العربية، القاهرة، 1996، ص569 وما بعدها.

[2] – أنظر المادة 02 من ميثاق المنظمة الدولية للشرطة الجنائية .

[3] – جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار الفكر العربي، القاهرة 2001، ص 76.

[4] – نبيلة هبة هروال، ، مرجع سابق، ص155.

القبض فيها على شاب ألماني بتهمة توزيع احد الفيروسات، من خلال تنسيق بالانتربول بين المباحث الفيدرالية الأمريكية والشرطة الألمانية[1].

ويبدو لنا أهمية (الانتربول) باعتباره من أجهزة الضبط القضائي على المستوى الدولي من خلال الإحصاءات الصادرة عن الأمانة العامة لها، وذلك عن قيامها بجهود كبيرة في مجال نشر أوصاف المجرمين وكشف كثير من القضايا الدولية وضبط مرتكبيها،[2].

والى جانب بالانتربول، هنالك منظمات لها دور فعال في مواجهة جرائم الانترنت على المستوى الدولي، كمنظمة التعاون الاقتصادي والتنمية (OECD) ومجموعة الثمانية الاقتصادية والتي قامت بإعداد ملتقى دولي مع منظمات دولية وبعض الدول (كمصر والصين) ، وذلك لتكوين قوة دولية تضطلع بالتحقيق أمن تكنولوجيا المعلومات[3].

ثانيا –على المستوى الأوربي :

وبالإضافة إلى الانتربول كذلك هنالك يوجد على المستوى الأوربي مكاتب متخصصة في جرائم الإنترنت خاصة، فهنالك مركز الشرطة الأوربية (الاوربول) وله دور فعال في مكافحة جرائم الإنترنت، إذ نجده يقوم بتسهيل التحقيقات المرتبطة بوقائع بث أو امتلاك محتويات إباحية عبر الإنترنت بين الدول الأوربية [4].

---

[1] – وتجدر الإشارة إلى أن الاختصاص المكاني للأنتربول يشمل كل الدول باستثناء الدول التي لاتنتمي للاتحاد الأوربي لانعقاد الاختصاص فيه لوحدات الاوربول وقوات شنجن . راجع عمر محمد أبو بكر بن يونس ، مرجع سابق ، ص816.

[2] – وقد نوه المجلس الاقتصادي والاجتماعي بجهودها وانجازها في مجال التعاون الدولي الأمني لمكافحة الجريمة وضبط المجرمين وظهر ذلك في توصياته بهذا الشأن، ولا شك أن قيام المنظمة بنشاطاتها في إطار القواعد القانونية الدولية و احترامها للسيادة الوطنية، بالإضافة إلى خبرتها في مجال التعاون الدولي الأمني ، هو السبب الحقيقي وراء نجاحها. راجع جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت ، مرجع سابق، ص 80.

[3] – نافذ ياسين مدهون ، مرجع سابق، 162.

[4] – حسنين المحمدي بوادي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر الجامعي، الإسكندرية، 2004، ص164.

وكذلك إلى جانب الاوربول يتواجد على المستوى الأوربي (الاورجست) كجهاز يساعد على التعاون القضائي والشرطي في مواجهة ومكافحة جميع أنواع الجرائم الخطيرة، والى جانب هاتين المنظمتين في أوربا تم إنشاء فضاء جماعي من غير حدود يسمى (شنجن) [1]، وذلك لمواجهة التحديات الأمنية ومنها جرائم الإنترنت، وتعمل على مراقبة المشتبه بهم عبر الحدود وملاحقة المجرمين [2].

المطلب الثاني: اختصاصات الضبطية القضائية في مكافحة جرائم التجارة الالكترونية

تتمثل مهام أجهزة الضبط القضائي في البحث عن الجرائم ومعرفة فاعليها وجمع المعلومات التي تفيد التحقيق، وتبدأ عملية البحث والتحري وجمع الأدلة ضرورية ولازمة بعد تلقي عضو

[1] – تم إنشاء شنجن من خلال التوقيع على معاهدة شنجن سنة 1985 وعلى اتفاقية تطبيقها سنة 19990، ولتعزيز التعاون استحدثت وسيلتين لمواجهة التحديات الأمنية وهي مراقبة المشتبه فيهم عبر الحدود وملاحقة المجرمين خارج الحدود الوطنية .

[2] – محمد فتحي عيد،الإنترنت ودوره في انتشار المخدرات، أكاديمية نايف العربية للعلوم الأمنية، الرياض 2003،ص202.

الضبط القضائي بلاغا عن وقوع جريمة أو مشاهدته الجريمة بنفسه [1]، وبعد ذلك على عضو الضبط القضائي القيام بإجراءات منها عادية واستثنائية على سبيل الاستثناء[2]. ولما كانت جرائم التجارة الالكترونية كغيرها تهدد الصالح العام، فقد كان من المنطقي أن تتخذ بشأنها نفس الإجراءات مع نوع من الخصوصية[3].

الفرع الأول:اختصاصات شرطة الانترنت في الظروف العادية

يقصد بالظروف العادية هنا الأحوال التي يمارس فيها عضو الضبط القضائي اختصاصه نتيجة لتلقيه شكوى عن وقوع الجريمة بأي طريقة من الطرق عدا حالة التلبس [4]، وتتمثل في تلقي البلاغات والشكاوى ومن ثم قيامه بالتحري وجمع الأدلة.

أولا- تلقي البلاغات أوالشكاوى :

ويقصد بالبلاغ إخبار السلطات المختصة عن وقوع جريمة سواء كانت الجريمة واقعة على شخص المخبر أو ماله أو شرفه أو على شخص الغير أو ماله أو شرفه وقد تكون الدولة أو مصالحها أو الملكية الاشتراكية هي محل الاعتداء [5].

ويعرف كذلك بأنه إخبار السلطات المختصة عن وقوع جريمة أو أنها على وشك الوقوع، أو أن أو قرائن أو أو وجود شك أو أنها ارتكبت[1].

---

[1] - نبيلة هبة هروال، مرجع سابق، ص161.

[2] - بينت المواد 12 ،13، 17، 18 41 ، 44 إلى 47، و138 من قانون الإجراءات الجنائية الجزائري واجبات عضو الضبط القضائي في الظروف العادية وفي الظروف الاستثنائية.

[3] نافذ ياسين المدهون ، مرجع سابق ، ص163.

[4] - راجع المادة 41 من قانون الإجراءات الجنائية الجزائري بشأن حالات التلبس.

[5] - سليم حربة وعبد الأمير العكيلي، شرح قانون أصول المحاكمات الجزائية، الجزء الأول، المكتبة الوطنية، بغداد، 1988، ص100.

والبلاغ عادة يكون إما شفوي أو

تفاصيل الجريمة كاسم الجاني والمجني عليه وأسباب الجريمة وقد يجهل بعض التفاصيل كأن يكون الجاني مجهول الهوية أو يجهل شخص المجني عليه، وكذلك قد يقدم الإخبار عن طريق الإنترنت وهو ما يسمى بالإخبار الرقمي[2].

والبلاغ الرقمي قد يتم عن طريق إرسال رسالة الكترونية إلى البريد الالكتروني للجهات المختصة بالتحقيق والتحري، أو عن طريق ملء استمارات رقمية متواجدة في المواقع المخصصة لتلقي البلاغات والشكاوى كالموقع الرسمي الفرنسي المركزي لانترنت الأحداث [3].

إلا أن

عدم خبرة أعضاء الضبط القضائي وعدم معرفتهم بالأمور الفنية

يصعب تحديد الجاني في جرائم الإنترنت في تلك الاخبارات، وان كان يمكن معرفة الحاسوب الذي ارتكبت من خلاله الجريمة.

لذا كان على الدولة استحداث أجهزة أو مكاتب متخصصة تعمل على تلقي الاخبارات في مثل هذا النوع من الجرائم وبواسطة محققين متخصصين في المعلومات وكذا في الإجراءات الجنائية[4].

وعند تلقي عضو الضبط القضائي بلاغا يشير والى وقوع جريمة كقيام شخص بنشر فيروسات تخريبية عبر شبكة الإنترنت أو بث صور إباحية عبر تلك الشبكة أو عن وجود مواقع أو صفحات خادعة أعدت للاحتيال على الناس، فعلى عضو الضبط القضائي تسجيل

---

[1] – لمزيد من التعاريف انظر سعد احمد محمود سلامة، التبليغ عن الجرائم، دراسة مقارنة، رسالة دكتوراه،أكاديمية الشرطة، القاهرة، 2003، ص 32 وما بعدها. Gaston Stefani, Georges levasseur, Bernard Bouloc procedure penal , 15 eme ed, dalloz.1993? p.296.

[2] – عمر أبوبكربن يونس ، الجرائم الناشئة عن استخدام الانترنت ، رسالة دكتوراه، جامعة عين شمس ن 1992 ص827 .

[3] – نبيلة هبة هروال ، مرجع سابق ،118.

[4] – لذلك أنشأت بعض الدول كفرنسا وحدات ومراكز متخصصة كالمكتب المركزي لمكافحة جرائم تكنولوجيا المعلومات والاتصالات ، ومن بين اختصاصاته تلقي البلاغات وتحليلها ودراستها للتأكد من صحتها. لمزيد من التفصيل راجع عمر أبوبكر يونس ، المرجع السابق ، ص805 .

البلاغ الذي ورد إليه، وعليه تقديم المساعدة لقضاة التحقيق والمحققين وضباط الشرطة ومفوضيها وتزويدهم بما يصل إليه من معلومات ،وضبط مرتكبيها وتسليمهم إلى السلطات المختصة [1].

وكما يختص عضو الضبط القضائي بقبول البلاغات عن الجرائم الواقعة ومنها جرائم الإنترنت، فأنه كذلك يتلقى الشكاوى عن بعض الجرائم التي حددها المشرع على سبيل الحصر والتي لا يمكن تحريك الدعوى الجزائية فيها إلا بعد تقديم شكوى من قبل المجني عليه أووكيله [2].

ولا تختلف أحكام الشكوى في الجرائم التقليدية عن تلك التي ترتكب عبر الإنترنت كجرائم النشر والسب والقذف عبر الانترنت ، إذ لا يجوز للجهات المختصة تحريك الدعوى العمومية في تلك الجرائم إلا بعد تقديم شكوى من طرف المجني عليه أو المتضرر منها أو [3].

وكما ذكرنا في موضوع البلاغ أو
هذا النوع من الجرائم، وهذا ما يجعل موضوع الشكوى في هذه الجرائم محل نقاش قانوني، وخاصة إذا علمنا إن تقديم الشكوى من قبل المجني عليه ضد مزودي الخدمات، دون حاجة إلى متابعة التحريات لمعرفة الجاني[4].

ولقد خصصت بعض التشريعات مراكز لمعالجة الشكاوى ، كمركز تلقي الشكاوى عن جرائم الاحتيال عبر الانترنت والدي تم تأسيسه في فرجينيا الغربية بالولايات المتحدة الأمريكية من طرف

---

[1] – حسين سعيد بمن سيف الغافري ، مرجع سابق ، ص353. نبيلة هبة هروال ، مرجع سابق ، ص187.

[2] – الشكاوى هي الطلبات التي يتقدم بها المتضررون من الجريمة مطالبين بالتعويض أو تحريك الدعوى العمومية. راجع حسن صادق المرصفاوي ، أصول الإجراءات الجنائية ، منشأة المعارف الإسكندرية 1996، ص70.
Gaston Stefani, Georges Levasseur Bernard Bouloc opcitp297

[3] – نبيلة هبة هروال ، مرجع السابق ،192.

[4] – عمر أبوبكر يونس ، مرجع السابق ، ص536.

مكتب التحقيقات الفيدرالي ، وكذلك مركز معالجة الشكاوى المتعلقة بجرائم الانترنت الذي يختص بتلقي الشكاوى وتحليلها[1].

- التحري وجمع الأدلة:

تبدأ مرحلة التحري وجمع الأدلة بعد الإبلاغ أو شكوى عن وقوع الجريمة إلى الجهات المختصة، حيث تبدأ دور الضبطية القضائية ، بجمع المعلومات التي تفيد التحقيق، فمرحلة التحري إذن هي مرحلة تحضير تسبق مرحلة التحقيق التي هي مرحلة تمحيص وتدقيق الأدلة للوصول إلى القرار المناسب[2].

الأدلة هي من الإجراءات الضرورية في جرائم التجارة الالكترونية كغيرها من الجرائم، وهي "مجموعة من الإجراءات التي يقوم بها المتحري عبر شبكة الإنترنت بواسطة التقنية الالكترونية الرقمية للحصول على معلومات توضيحية عن الأشخاص أو الأماكن .

فهذه الإجراءات وسيلة لجمع المعلومات والأدلة عن الجرائم بصفة عامة وجريمة الإنترنت بصفة خاصة، ولعضو الضبط القضائي في ذلك سلطة تقديرية واسعة في اختيار وسائل إجراء التحري التي يراها مناسبة ولازمة لإتمام عمله بصورة ايجابية في جمع المعلومات التي يستفيد منها لضبط الجريمة أو للحد منها، وهناك العديد من وسائل التحريات ، أبرزها نظام الإرشاد الجنائي عبر الإنترنت وكذلك مراقبة شبكة الاتصالات[3].

---

[1] – نبيلة هبة هروال ، مرجع سابق ،ص193 .

[2] – يختلف الضبط القضائي عن الضبط الإداري، فالضبط الإداري يستهدف صيانة النظام العام دون تتجه إرادة القائم بعملية الضبط إلى الكشف عن جريمة ما. أما الضبط القضائي فيرمي إلى تحري الجرائم وتعقب مرتكبيها وتوقيع العقوبات عليهم.

[3] – مصطفى محمد موسى، دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، 2005، ص22.

حيث يعد الإرشاد الجنائي من أهم المصادر التي يعتمد عليها عضو الضبط القضائي في تحرياته وجمع الأدلة إذ نجد العديد من الدول تقوم باستخدامه [1].

كما أن المراقبة الالكترونية هي الأخرى وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه بهم، حيث يقوم بها مراقب الكتروني، يتمثل في عضو ضبط قضائي ذو كفاءة تقنية عالية كأن يراقب احد الأشخاص ممن قام باختراق الحاسب الآلي الخاص بالمجني عليه، أو يقوم بإعداد صندوق بريد الكتروني مستنسخ لمراقبة المشتبه به عند إرساله[2].

الفرع الأول:اختصاصات شرطة الانترنت في الظروف الاستثنائية

يتمثل الاختصاص الأصيل للضبطية القضائية في البحث والتحري ، إلا أن هنالك من الظروف ما يستدعي التدخل المباشر والسريع بإجراء من إجراءات والمحافظة على أدلة الجريمة، لذا يقر المشرع لأعضاء الضبط القضائي سلطة اتخاذ بعض إجراءات التحقيق كالقبض على المتهم وتفتيشه وتفتيش منزله وذلك في حالة الجريمة المشهودة، وكذلك في حالة صدور أمر إليه من قاضي التحقيق أو المحقق.

وتكون الجريمة مشهودة إذا شوهدت حال ارتكابها أو عقب ارتكابها ببرهة يسيرة أو إذا تبع المجني عليه مرتكبها اثر وقوعها أو تبعه الجمهور مع الصياح أو إذا وجد مرتكبها بوقت قريب ألآت أو أسلحة أو أمتعة أو أوراقا أو أشياء أخرى يستدل منه على انه فاعل أو شريك فيها أو إذا وجدت به في ذلك الوقت أثارا أو علامات تدل على ذلك[3].

---

[1] – وذلك عن طريق تجنيد عناصرها أو الغير للدخول إلى العالم الافتراضي وبالأخص عبر قاعات الدردشة والاتصال المباشر مستخدمين في ذلك أسماء وصفات مستعارة بقصد البحث عن الجرائم ومرتكبيها .

[2] - نبيلة هبة هروال، مرجع سابق ، ص197وما بعدها . و لمزيد من التفاصيل انظر عمر محمد بن يونس الإجراءات الجنائية عبر الانترنت في القانون الأمريكي ، ط 1، 20005 ، ص 372 و مابعدها .

[3] – راجع المادة 41 من قانون الإجراءات الجنائية الجزائري بشأن حالات التلبس.

فالتلبس على هذا النحو حالة تتعلق باكتشاف الجريمة وتعتمد إما على مشاهدة الجريمة حال ارتكابها أو عقب ارتكابها ببرهة يسيرة، ذلك انه وصف ينصب على الجريمة دون فاعلها فقد تشاهد الجريمة ولا يشاهد الفاعل ذلك أن مناط حالة التلبس هو التقارب الزمني بين لحظة وقوع الجريمة ولحظة اكتشافها[1].

ونلاحظ بأن المشرع الجزائري ونظيريه المصري والفرنسي نص على حالات التلبس على سبيل الحصر لا المثال، وبالتالي لا يجوز التوسع في تفسيرها بطريق القياس أو التقريب.

أولا-المعاينة:

يجب على عضو الضبط القضائي في حدود اختصاصه إذا اخبر عن جريمة مشهودة أو اتصل علمه بها أن إلى مكان الجريمة لمعاينته، ويدون إفادة المجني عليه ويسأل المتهم عن التهمة المسندة إليه بط كل ما يظهر انه استعمل في ارتكاب الجريمة ويعاين أثارها المادية ويحافظ عليها ويثبت حالة الأشخاص والأماكن وكل ما يفيد في اكتشاف الجريمة ويسمع أقوال أو من يمكن الحصول منه على إيضاحات قضائي عند انتقاله إلى محل الجريمة المشهودة أن يمنع الحاضرين من مبارحة محل الواقعة أو الابتعاد عنه ، وله أن يحضر في الحال كل شخص يمكن الحصول منه على إيضاحات بشأنها[2].

عليها خوفا من إتلافها، أو محوها أو تعديلها [3].

---

[1] – أحمد شوقي الشلقاني ، مبادئ الإجراءات الجزائية في التشريع الجزائري (الجزء الثاني) ديوان المطبوعات ، 1999، ص178. محمد زكي أبو عامر، الإجراءات الجنائية ، دار منشأة المعارف ، الإسكندرية 2002، ص139.

[2] – راجع المادة 42 و43 من قانون الإجراءات الجنائية الجزائري . ولمزيد من التفصيل انظر عبد الفتاح بيومي حجازي، المبادئ الاجرءات الجنائية في جرائم الكومبيوتر والإنترنت، دار الكتب القانونية، القاهرة ، 2007، ص247.

[3] – محمد زكي أبو عامر، الإجراءات الجنائية المرجع السابق، ص233.

ويعرفها البعض بأنها رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة [1].

والمعاينة من إجراءات التحقيق الابتدائي، ويجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق، والأصل أن يحضر المعاينة أطراف الدعوى وقد يقرر المحقق أن يجريها في غيبتهم، ولا يلتزم المحقق بدعوة محامي المتهم للحضور ومجرد غياب المتهم عند إجراء المعاينة ليس من شأنه أن يبطلها.

أهمية المعاينة عقب وقوع جريمة من الجرائم التقليدية، حيث يوجب مسرح فعلي للجريمة يحتوي على آثار مادية فعلية، يهدف القائم بالمعاينة إلى التحفظ عليها تمهيدا لفحصها لبيان مدى صحتها في الإثبات، فليس الحال كذلك بالنسبة للجرائم الإلكترونية، حيث تطول الفترة الزمنية بين وقوع الجريمة واكتشافها، مما يعرض آثارها إلى المحو أو التلف أو العبث به[2].

فيرى جانب من الفقه الجنائي

ضرورة إتباع بعض القواعد والإرشادات الفنية عند معاينة مسرح الجرائم المعلوماتية ، على التفصيل الآتي [3]:

---

[1] – ومن الاختصاصات التي يمارسها عضو الضبط القضائي أيضا عند علمه بجريمة مشهودة من جرائم الإنترنت، الانتقال إلى محل الواقعة الإجرامية، والانتقال هنا لا يكون إلى العالم المادي، إلى العالم الافتراضي لمعاينته، وذلك من خلال مكتبة أو اللجوء إلى مقهى الإنترنت أو إلى مقر مزود الإنترنت .

ولمزيد من التفاصيل انظر إلى عمر محمد يونس، ، مرجع سابق ، ص 809. وانظر هشام فريد ، الجوانب الإجرائية للجرائم المعلوماتية ، (دراسة مقارنة) ، مكتبة الآلات الحديثة أسيوط مصر 19994، ص59.

[2]– عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير ي جرائم الكمبيوتر ، المرجع السابق ، ص 44 وما بعدها وانظر نبيلة هبة هروال ، مرجع سابق ، ص217 .

[3] – عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت ،المرجع السابق ، ص 185 وانظر أيضا هشام فريد ، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق ، ص60-61- وهبة هروال ، المرجع السابق، ص220. محمد الأمين البشري، التحقيق في الجرائم المستحثة ، جامعة نايف للعلوم الأمنية ، الرياض 2004 ص113

– تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

–العناية بملاحظة الطريقة التي تم بها إعداد النظام ، و
والكابلات المتصلة بكل مكونات النظام .

–عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يمحو البيانات المسجلة.

–التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة، وفحصها، ورفع البصمات ذات الصلة بالجريمة.
–التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات .

- ضرورة قصر عملية المعاينة على أعضاء الضبط القضائي ممن تتوافر فيهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات واسترجاع المعلومات.

وتجدر الإشارة إلى أن المشرع الجزائري أجاز المعاينة في الجرائم المعلوماتية المتلبس فيها في المادة 3/47 ، والتي تنص على أنه عندما يتعلق الأمر بجرائم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإنه يجوز إجراء المعاينة في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص [1].

[1] – يلاحظ أن المشرع الجزائر يخرج على الأصل المنصوص عليه في الفقرة 01 من المادة 47 من قانون الإجراءات الجنائية ، وهي أنه لا يجوز البدء في تفتيش المساكن و معاينتها قبل الساعة الخامسة (5) صباحا، و لا بعد الساعة الثامنة (8) مساء غلا إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل أو في الأحول الاستثنائية .
وطبقا للمادة 6/47 لا تمس هذه الأحكام بالحفاظ على السر المهني المنصوص عليه في الفقرة الثالثة من 45 من قانون الإجراءات الجنائية .

ثانيا-التفتيش:

بالإضافة إلى المعاينة من الجائز لعضو الضبط القضائي أثناء التلبس بجرائم الإنترنت أن يقوم بتفتيش شخص المشبه به وما يحمله من حاسوب نقال أو هاتف نقال أو حاسوب صغير أو مسكنه وما يتضمنه من موجودات ومن بينها الحاسوب ، والتفتيش إجراء من إجراءات التحقيق يهدف إلى البحث عن أشياء تتعلق بالجريمة، وكل ما يفيد بصفة عامة في كشف الحقيقة [1].

وقد عرف المجلس الأوروبي التفتيش المعلوماتي بأنه إجراء يسمح بجمع الأدلة المخزنة باستخدام الوسائل الإلكترونية في أ . ويشترط في التفتيش وقوع جريمة بالفعل تعد جناية أو جنحة، وأن يوجه اتهام إلى الشخص المراد تفتيشه آو تفتيش مسكنه، وأن يكون الأمر بالتفتيش مسبب حضور المتهم أو من ينيبه أو الغير أو من ينيبه التفتيش، و تحرير محضر بالتفتيش، كما [2].

ويثير امتداد الإذن بالتفتيش إلى أماكن أو أنظمة أخرى، غير الواردة في الإذن الأول بعض المشكلات، يتعلق أولها برفض صاحب المكان أو النظام الأخر مباشرة التفتيش لديه، لهذا يرى البعض في هذه الحالة عدم استمرار أوامتداد البحث لديه إلا في حالتي التلبس،أورضائه بالتفتيش[3].

---

[1] -هلالي عبد الله احمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، دراسة مقارنة ، دار النهضة العربية القاهرة 2006، ، ص45 وما بعدها .أحمد فتحي سرور ، الوسيط في قانون الإجراءات الجنائية ، الطبعة السابعة ، دار النهضة العربية ، القاهرة مصر 1993، ص544.

[2] - إلا أن هذا الشرط يحمل بعض المخاطر أحيانا وذلك في حالة ما إذا كان التفتيش في مكان آخر غير الذي صدر بشأنه الإذن المكتوب وتتمثل المخاطر في إمكانية قيام الجاني بتدمير، أو محو البيانات، أو نقلها، أو تعديلها ولمواجهة هذه المخاطر، يرى البعض أن الإذن المكتوب بالتفتيش في مكان ما يجب أن يتضمن الإذن بتفتيش أي نظام معلوماتي أخر يوجد في أي مكان غير مكان البحث . راجع عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت مرجع سابق ، ص3565 و مابعدها . هبة هروال ، مرجع سابق ، ص228 وما بعدها .

[3] - نبيلة هبة هروال ، مرجع سابق ، ص240. هشام فريد ، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق ص70-71.

وتضيف المادة 2/23 و مكررا/2 من قانون تحقيق الجنايات البلجيكي إن الإذن يتجاوز حدود الاختصاص المحلي، من اجل البحث عن أدلة الجريمة، لكن يشترط لصحته فضلا عن صدوره من الجهة المختصة أن يتم إبلاغ ممثل النيابة الداخل في نطاق اختصاصه الموضع الجديد.

وقد أدى هذا إلى إدخال المادة 88 من قانون تحقيق الجنايات بمقتضى القانون الصادر 23 نوفمبر 2000، التي تنص على أنه "إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي، أو في جزء منه، فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان أخر غير مكان البحث الأصلي، ويتم هذا الامتداد إذا كان ضروريا لكشف الحقيقة ، أو إذا وجدت مخاطر تتعلق بضياع بعض الأدلة، نظرا لسهولة عملية محو أو إتلاف، أو نقل البيانات محل البحث [1] .

ويرى البعض أنه في حالة امتداد الاختصاص، فيمكن أن يصدر الأمر بالامتداد شفويا من قاضي التحقيق، تحقيقا للسرعة المطلوبة، ثم يصدر فيما بعد الإذن المكتوب، وفي جميع الأحوال يجب أن يكون الإذن مسببا، لتتمكن الجهة القضائية من مراقبة مدى مشروعيته [2].

والمشكلة الثانية التي تثور في حالة امتداد الإذن بالتفتيش إلى خارج إقليم للدولة التي صدر منها الإذن، ودخوله في مجال دولة أخرى، حيث يعد انتهاكا لسيادة الدولة الأخرى في غياب اتفاقية بين الدولتين تجيز هذا الامتداد، أو على الأقل الحصول على إذن الدولة الأخرى[3].

---

[1]- Meunier (C.): La loi du 28 Nov. 2000 relative a la criminalité informatique. Rev. Dr. Pen. Crime. 2002, p. 665

[2] - Meunier (C.) : art. Perec. P. 668

3- ومع ذلك فقد أجازت المادة 32 من الاتفاقية الأوروبية التي أعدها المجلس الأوروبي في صيغتها النهائية في 25 مايو سنة2001 إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها، وذلك في حالة إذا تعلق بمعلومات أو بيانات متاحة للجمهور إذا رضي صاحب هذه البيانات. للتفصيل راجع :

Podovo(Y.) : un aperçu de la lutte contre la cybercriminalité en France. R.S.C. 2002, p. 765. spec. p.777

ومع ذلك فإن تطبيق هذا النص يمكن أن يثير مشكلات جمة ، وبالتالي لامناص من التعاون الدولي في هذا المجال بمقتضى اتفاقية ثنائية أو متعددة الأطراف، أو على الأقل الحصول على إذن الدولة التي يتم التفتيش في مجالها الإقليمي[1].

ويثور السؤال عن إمكانية التفتيش وفقا للضوابط السابقة في مجال الجرائم الإلكترونية؟

على الرغم من أن التفتيش بالمعنى التقليدي بهدف إلى حفظ أشياء مادية تتعلق بالجريمة وتفيد في كشف الحقيقة، بينما البيانات الإلكترونية ليس لها بحسب جوهرها مظهر مادي ملموس في العالم الخارجي، ومع ذلك فيمكن أن يرد التفتيش على هذه البيانات غير المحسوسة عن طريق الوسائط الإلكترونية لحفظها وتخزينها كالأسطوانات والأقراص الممغنطة، ومخرجات الحاسب[2].

وعليه يمكن القول بإمكانية أن يكون محل التفتيش البيانات المعالجة آليا والمخزنة بالحاسب الآلي، ثم ضبطها والتحفظ عليها، أو ضبط الوسائط الإلكترونية التي سجلت عليها هذه البيانات والتفتيش في هذه الحالة يخضع لما يخضع له التفتيش بمعناه التقليدي من ضوابط وأحكام[3].

ولقد أجاز المشرع الجزائري التفتيش في الجرائم المعلوماتية المتلبس فيها في المادة 3/47 حيث يجوز إجراء المعاينة في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص [4].

---

[1] - Padovo (Y.): art. Prec, P.778.

[2] - عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت ، مرجع سابق ، ص 378 379. وانظر أيضا هشام فريد، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق ، ص68.

[3] – نبيلة هبة هروال ، مرجع سابق ، ص226.

[4] – يلاحظ أن المشرع الجزائر خرج في التفتيش على الأصل المنصوص عليه في الفقرة 01 من المادة 47 من قانون الإجراءات الجنائية ، وهي أنه لا يجوز البدء في تفتيش المساكن و معاينتها قبل الساعة الخامسة (5) صباحا، و لا بعد الساعة الثامنة (8) مساء غلا إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل أو في الأحول الاستثنائية وطبقا للمادة 6/47 لا تمس هذه الأحكام بالحفاظ على السر المهني المنصوص عليه في الفقرة الثالثة من 45 .

وبالتالي فان التفتيش يقع على مكونات الحاسب الآلي المادية والمعنوية ، كما يقع التفتيش على الشبكة وما تتضمنه من مكوناتها[1]، وبعد إجراء التفتيش يجب على القائم بالتفتيش أن يحرر محضر يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي أثبتت وان يحمل تاريخ تحريره وتوقيع محرره ، كما ينبغي أن يكون هناك شخص متخصص في أمور الحاسوب والإنترنت يرافق عضو الضبط القضائي القائم بالتفتيش للاستعانة به في مجال الخبرة الفنية الضرورية [2].

ثالثا-الضبط:

يهدف التفتيش إلى ضبط أشياء تتعلق بالجريمة ويفيد في التحقيق الجاري بشأنها، سواء أكان هذا الشيء أدوات استعملت في ارتكاب الجريمة أو شيئا نتج عنها أو مما يفيد في كشف الحقيقة .

والضبط هو وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها، و من حيث محله لا يرد إلا على الأشياء المادية[3].

ونظرا لكون الضبط محله في مجال الجرائم الإلكترونية، البيانات المعالجة إلكترونيا، فقد اختلف الفقه وانقسم إلى اتجاهين:

فيرى الاتجاه الأول أن بيانات الحاسب لا تصلح لأن تكون محلا للضبط، لانتفاء الكيان المادي عنها، ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس، عن طريق التصوير الفوتوغرافي، أو بنقلها على دعامة أو غيرها من الوسائل المادية ويستند هذا الرأي إلى أن النصوص التشريعية المتعلقة بالضبط محل تطبيقها الأشياء المادية الملموسة [4].

---

[1] – عبد الله حسين محمود، مرجع سابق، ص372.

[2] – نبيلة هبة هروال ، مرجع سابق ، ص250. هشام فريد ، الجوانب الإجرائية للجرائم المعلوماتية ، مرجع سابق ، ص75

[3] - kaspersen (H.W.K) : Computer crimes and others crimes against information technology in the Netherlands. Rev. int. dr. pen. 1993. p. 474. spec. p. 502- Mothernc blager (M.), Rapp. Prec. Rev. int. dr. pen.1993. p.349. spec. p.350

[4] – عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت ،مرجع سابق ، ص 395.عبد الله حسين محمود، مرجع سابق ، ص397

ويرى الاتجاه الثاني أن البيانات المعالجة إلكترونيا إن هي إلا ذبذبات إلكترونية، أو موجات كهرومغناطيسية، مسجلة على وسائط مادية، وبالإمكان نقلها وبثها واستقبالها [1].

وهذا الخلاف دعا المشرع في بعض الدول إلى تطوير النصوص التشريعية المتعلقة بمحل التفتيش والضبط ليشمل فضلا عن الأشياء المادية البيانات المعالجة إلكترونيا، وهو ما نصت عليه المادة 39 من قانون تحقيق الجنايات البلجيكي [2].

كما أجاز المشرع الجزائري الضبط والحجز في الجرائم المعلوماتية المتلبس فيها في المادة 3/47 ، إذ يجوز إجراء المعاينة في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص .

وتواجه عملية الضبط للبيانات المعلوماتية صعوبات منها حجم شبكة المعلومات مثال ذلك البحث في نظام الكتروني لشركة متعددة الجنسيات، وكذلك وجود هذه البيانات في شبكات أو أجهزة تابعة لدولة أجنبية، مما يستدعي تعاونها مع جهات الشرطة والتحقيق في عملية الضبط [3].

أن الضبط القضائي في جرائم الإنترنت ينطوي على تحديات كثيرة، أهمها الحاجة إلى سرعة الكشف عن الجريمة خشية ضياع الدليل، وقانونية وحجية أدلة جرائم الإنترنت ومشكلات الاختصاص القضائي والقانون الواجب التطبيق، والحاجة إلى تعاون دولي شامل في حقل امتداد إجراءات التحقيق والملاحقة خارج الحدود [4].

---

[1] – تنص كالمادة 7/29 من قانون الإثبات في كندا التي تنص على أن تفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة مالية، يقتصر على تفتيش المكان بغرض تفقده واخذ نسخة من المواد المكتوبة، سواء مكتوبة ورقيا إلكترونيا .

[2] – عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت ، مرجع سابق ، ص 220 أيضا هشام فريد ، الجوانب الإجرائية للجريمة المعلوماتية مرجع سابق ، ص96.

[3] – ولتفادي ذلك، فقد منحت المادة 88 من قانون تحقيق الجنايات البلجيكي لقاضي التحقيق سلطة الأمر بالتحفظ عليها، إن وجدت على الأرض البلجيكية، أو أن يطلب من السلطات الأجنبية نسخة من هذه البيانات محل الجريمة، إن وجدت لدى دولة أجنبية وخشية من محو أو إتلاف أو نقل أو ضياع الأدلة الناتجة عن عملية التفتيش .

[4] – يونس عرب، جرائم الكومبيوتر والإنترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002، أبو ظبي، ص 43.

المبحث الثاني

الحماية الجنائية الإجرائية للتجارة الالكترونية في مرحلة التحقيق الابتدائي

إجراءات التحقيق الابتدائي هي مجموعة من الأعمال التي تباشرها سلطة مختصة للتحقيق في مدى صحة الاتهام الموجه من طرف النيابة العامة بشأن واقعة جنائية معروضة عليها وذلك بالبحث عن الأدلة المثبتة لذلك ، والتحقيق مرحلة لاحقة لإجراءات جمع الاستدلال وتسبق مرحلة المحاكمة التي تقوم بها جهة الحكم وعليه فإن التحقيق يهدف إلى تمهيد الطريق أمام قضاء الحكم باتخاذ جميع الإجراءات الضرورية للكشف عن الحقيقة[1]

يهدف التحقيق الابتدائي إلى كشف الحقيقة وللوصول إلى هذا الغرض يلجأ المحقق إلى مجموعة إجراءات بعضها يهدف للحصول على الدليل، وتسمى إجراءات جمع الدليل كالتفتيش والضبط والمعاينة والشهادة والخبرة ، وبعضها الآخر يمهد للدليل ويؤدي إليه وتعرف بالإجراءات الاحتياطية ضد المتهم كالقبض والحبس المؤقت[2].

وسوف نقتصر على أهم إجراءات جمع الأدلة المادية وهي التفتيش (المطلب الأول) والضبط (المطلب الثاني) كأهم التحديات الإجرائية لجرائم الانترنت ولاسيما جرائم التجارة الالكترونية .

---

[1] – إسحاق إبراهيم منصور ، المبادئ الأساسية ي قانون الإجراءات الجزائية الجزائري ، ديوان المطبوعات الجامعية ، الجزائر 1995، ص100 وما بعدها وانظر أحمد شوقي الشلقاني ن مبادئ الإجراءات الجزائية في التشريع الجزائري ، الجزء الثاني ، ديوان المطبوعات الجامعية ، الجزائر ، 1999 ، ص210.

[2] – رغم أن المعاينة تعد من الأدلة المادية التي تؤثر في اقتناع القاضي بحكم العقل والمنطق إلا أنها لا تؤدي ذات الدور في كشف غموض الجريمة المعلوماتية ويرجع ذلك إلى سببين : أولهما أن هذه الجرائم لا تترك أثر مادي في مسرح الجريمة وثانيهما أن مرتكبها تكون له القدرة على إتلاف أو تشويه الدليل في فترة قصيرة وهذا ما يورث الشك في الأدلة المستقاة من المعاينة ، أما بالنسبة للخبرة فإن الجريمة المعلوماتية تكاد تنطبق عليها قواعد الخبرة المعمول بها في الجرائم التقليدية ، أما عن الأدلة القولية الأخرى من شهادة واستجواب واعتراف فهي أقل مفعولا وأثرا لأنها لا تعتمد على العقل والمنطق .

المطلب الأول: التفتيش في مجال جرائم التجارة الالكترونية

ترتب على ثورة الاتصالات عن بعد ظهور هذا النوع الجديد من الجرائم الذي قد يرتكب بالوسائل الإلكترونية أو قد تكون هذه الوسائل محلا له، ولأجل ضبط هذه الجرائم وجمع الأدلة بشأنها فإن سلطة التحقيق قد تلجأ إلى التفتيش لضبط الأدلة المادية التي قد تساعدها في إثبات

.

لقد تعددت التعريفات التي أضفاها الفقه على التفتيش, إلى أنها تجتمع على أن التفتيش عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل وذالك من أجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات القانونية المقررة , وقد أحاط القانون التفتيش بضمانات عديدة لأنه قد يقتضي البحث في محل له حرمة خاصة[1].

والتفتيش في مدلوله القانوني بالنسبة للجرائم الإلكترونية لا يختلف عن مدلوله السائد في فقه الإجراءات الجنائية فيقصد به أنه إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بإركابها[2].

ويثير موضوع التفتيش الذي يقع على نظم الوسائل الإلكترونية مسائل عديدة للبحث، أبرزها مدى صلاحية الكيانات المعنوية في هذه الوسائل كمحل يرد عليه التفتيش، و ضوابط تفتيش نظم الحاسوب والانترنت.

---

[1] – نبيلة هبة هروال ، مرجع سابق ، ص222–223 – هلالي عبد الله ، مرجع سابق ، ص45 وما بعدها .

[2] –علي حمودة ، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي مؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر:اكادمية شرطة دبي ، مركز البحوث والدراسات ، رقم العدد : 1 ، بتاريخ 26 نيسان 2003 ، دبي – الإمارات العربية المتحدة.

الفرع الأول: مدى قابلية نظم الحاسوب والانترنت للتفتيش

أولا- موقف الفقه :

أشرنا سابقا إلى أن الحاسوب يتكون من مكونات مادية ومكونات معنوية ولا تثار أدنى صعوبة إذا كان محل جرائم الحاسوب مكونات مادية حيث ينطبق يصددها القواعد تقليدية دون صعوبة [1] بمعنى أن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه وهل هو من الأماكن العامة أم من الأماكن الخاصة ، إذ أن لصفة المكان أهمية خاصة في مجال التفتيش فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش منزله وبنفس الضمانات المقررة قانونا في التشريعات المختلفة [2] .

أما إذا كان محل جرائم الحاسب الآلي مكونات غير مادية كبرامج الحاسب أو بياناته فقد ثار خلاف كبير في الفقه بين مؤيد ومعارض .

1- الاتجاه المؤيد:

حيث يذهب هذا الرأي أنه إذا كان هد التفتيش هو جمع الأدلة فان هذا المفهوم يتسع ليشمل البيانات والمعلومات والبرامج [3].

---

[1] - فالواقع أن ولوج المكونات المادية للحاسب بأوعيتها المختلفة بحثا عن شيء يتصل بجريمة معلوماتية قد وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها لا خلاف بين الفقهاء في أنه يدخل في نطاق التفتيش طالما تم وفقا للإجراءات القانونية المقررة .

[2] - وبالنسبة للاماكن العامة سواء كانت بطبيعتها كالطرق العامة والشوارع أو كانت بالتخصيص كالمقاهي والمطاعم والسيارات العامة فإن الشخص إذا وجد في هذه الأماكن وهو يحمل مكونات مادية للحاسب الآلي أو كان مسيطرا أو حائزا لها فإن التفتيش لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود . راجع هلالي عبد الإله ، التفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع السابق ص74.

[3] - هشام فريد، مرجع سابق، ص67. وانظر هبة هروال ، مرجع سابق ، ص227. كامل عفيفي مرجع سابق، ص366.

وقد لجأ الفقه في العديد من الدول استنادا إلى عمومية نصوص التفتيش إلى التوسع في تفسيرها وذلك بمد حكمها إلى البرامج والبيانات المخزنة في أنظمة المعالجة الآلية للمعلومات ، وأبرز مثال لذلك الفقه الكندي عندما وسع من تفسير المادة 487 من قانون العقوبات الكندي والتي تسمح بضبط وتفتيش بيانات وبرامج الحاسب الآلي والانترنت [1].

وفي هذا المعنى نجد المادة 251 من قانون الإجراءات الجزائية اليوناني تعطي سلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع وحماية الدليل ويفسر الفقه اليوناني أن عبارة أي شيء تشمل تفتيش البرامج والبيانات المعالجة الالكترونية[2].

2- الاتجاه المعارض:

وعلى النقيض يرى أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم المادي لا ينطبق على برامج وبيانات الحاسوب غير المحسوسة ، ويقترح هذا الرأي في مواجهة هذا القصور التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة (مواد معالجة الكترونية) ، ولذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هي البحث عن الأدلة أو أي مادة معالجة بواسطة الحاسب الآلي[3].

والحقيقة أن الحاجة ماسة لتدخل تشريعي لتقرير الضوابط القانونية الكفيلة للتغلب على الصعوبات الإجرائية التي تثار عند تفتيش الأنظمة المعلوماتية سواء بتعديل النصوص القائمة أو استحداث نصوص خاصة.

---

[1] - تنص المادة 487 على إمكانية إصدار أمر قضائي لتفتيش أي شيء تتوافر بشأنه أسس أو مبررات معقولة تدعوا للاعتقاد بأن الجريمة قد وقعة أو يشتبه في وقوعها أو أن هناك نية لاستخدامه في ارتكاب جريمة أو أنه سيتيح دليلا على ارتكاب جريمة ، وهكذا فإن هذا النص يفسر على أنه يسمح بضبط بتفتيش بيانات وبرامج الحاسب الآلي . راجع هشام فريد مرجع سابق، ص67 .

[2] -حسن عبد الله محمود، مرجع سابق، ص372.

[3] -هشام فريد ، الجوانب الإجرائية للجريمة المعلوماتية ، مرجع سابق ، ص65. هبة هروال ، مرجع السابق ، ص226. كامل عفيفي عفيفي، مرجع سابق، ص366.

ثانيا – موقف التشريعات:

إذا كان التفتيش كوسيلة إجرائية يستهدف الحصول على دليل مادي يساعد في إثبات الجريمة، فإن البعض قد تشكك في مدى صلاحيته للبحث عن أدلة الجريمة في الكيانات المعنوية للحاسبات الآلية، وهو ما حدا ببعض التشريعات بأن تنص صراحة على أن التفتيش يتم بالنسبة لجميع أنظمة الحاسب الآلي، ومثال ذلك قانون إساءة استخدام الحاسوب في إنجلترا الصادر في سنة1990[1].

إذ نص المشرع الإنجليزي في قانون إساءة استخدام الكمبيوتر الصادر عام 1990 على تفتيش نظم الحاسب الآلي في جرائم الولوج غير المشروع على أنظمة الحاسوب ، والتعديل غير المرخص به في نظام الحاسوب بدون إذن طالما كان هدف هذا الولوج ارتكاب جرائم ، أما إذا كان الولوج مجرد دون نية لارتكاب أفعال غير مشروعة فإن التفتيش ممكن دون إذن قضائي [2].

وفي الولايات المتحدة الأمريكية تم تعديل المادة 34 من قانون الإجراءات الجنائية الفيدرالي عام 1970 لتسمح بتفتيش الحاسوب والكشف عن الوسائط الالكترونية[3]. كذلك أجاز التشريع الهولندي تسجيل البيانات الموجودة في النهاية الطرفية في المادة 25/أ من قانون الإجراءات الجنائية ، وقرر أيضا بعض القواعد القانونية بغية التغلب على الصعوبات التي قد تثار عند تفتيش الأنظمة [4].

---

[1] – عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت ،مرجع سابق، ص378 .
Wasik (martin) , computer crimes and other crimes agains Information technology in the United Kingdom- rev, inter, De, Dr, Penal 1993,P,64

[2] – أسامة محمد المناعسة ، مرجع سابق ، ص266.

[3] – عبد الله حسين محمود، مرجع سابق، ص372.

[4] – أجاز في المادة 25/أ منه للقائم بالتفتيش سلطة تسجيل البيانات الموجودة في النهاية الطرفية التي يتصل بها النظام المعلوماتي دون التقيد بالحصول على إذن مسبق بذلك من قاضي التحقيق وهذا لتذليل الصعوبة الخاصة بوجود النهاية الطرفية للنظام المعلوماتي في منزل أخر غير منزل المتهم كما أجاز بموجب المادة 25 منه إلزام غير المتهم كالشاهد والشخص القائم بالتشغيل بتقديم كافة البيانات للولوج نظام الحاسب الآلي والتعامل مع سلطة التحقيق . للتفصيل راجع هشام فريد رستم ، مرجع سابق ، ص 100.

كما أجاز المشرع الجزائري تفتيش المنظومة المعلوماتية بموجب المادتين45 و47 من القانون رقم 22/06المعدل والمتمم لقانون الإجراءات الجنائية [1] ، إذ تنص المادة 45 على أنه لا يشترط حضور المشتبه فيه صاحب المسكن إذا تعلق الأمر بالتفتيش عن الجرائم المعلوماتية ، باستثناء الأحكام المتعلقة بالحفاظ على السر المهني و كذا جرد الأشياء و حجز المستندات [2].

كما تنص المادة 3/47 من قانون العقوبات عندما يتعلق الأمر بجرائم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإنه يجوز إجراء التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل و ذلك بناء على إذن مسبق من وكيل الجمهورية المختص [3].

كذلك سمح المشرع الجزائري في المادة 05 من قانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها [4] ، بالدخول في منظومة معلوماتية بغرض التفتيش ولوعن بعد ، وذلك في الحالات المنصوص عليها في المادة 04 [5].

---

[1] – راجع المادتين 45 و47 من القانون رقم 22/06 المؤرخ في 20ديسمبر 2006 المتضمن قانون الإجراءات الجنائية ج ر . عدد84 مؤرخة في 20 ديسمبر 2006.

[2] –وعليه سمح المشرع بالتفتيش عن الجرائم المعلوماتية، لكنه لم يشترط حضور المشتبه فيه صاحب المسكن، لكن دون المساس باستثناء الأحكام المتعلقة بالحفاظ على السر المهني و كذا جرد الأشياء و حجز المستندات.

[3] – بالتالي سمح المشرع بالتفتيش عن الجرائم المعلوماتية في أي محل ، وفي أي وقت لكنهه اشترط إذن مسبق من وكيل الجمهورية المختص، وعدم المساس بالسر المهني .

[4] – راجع المادة05 من القانون رقم 04/0 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها.

[5] – تتمثل الحالات المنصوص عليها في للمادة 04 في الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة ، وأيضا في حالة توفير معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني ، وكذلك لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية ، وكذا في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة .

الحصول عليها بمساعدة السلطات المختصة طبق للاتفاقيات الدولية ووفقا لمبدأ المعاملة بالمثل [1].

ونصت أيضا اتفاقية بودابست للجريمة المعلوماتية لسنة 2001 في المادة 19 على أنه يجب على الدول الإطراف أن تتبنى الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية من اجل تخويل سلطاته المختصة سلطة التفتيش [2].

الفرع الثاني: ضوابط التفتيش المعلوماتي

إذا كان الوصول إلى الحقيقة يمثل الغاية من الإجراءات ، بيد أن تحقيق تلك الغاية لا يكون بأي ثمن , ففي كل الحالات فإن الغاية لا تبرر الوسيلة , فالبحث عن الحقيقة القضائية لا ينبغي أن يكون طليقا من كل قيد ، بل إن ذلك يخضع لضوابط معينة ، ومن هذا المنطلق يجب أن يخضع التفتيش في النظم المعلوماتية لضوابط يمكن تقسيمها إلى ضوابط موضوعية وشكلية [3].

أولا- الضوابط الموضوعية :

تنحصر هذه الضوابط الموضوعية للتفتيش المعلوماتي ، في الآتي :

أ- سبب التفتيش :

يتمثل سبب التفتيش في وقوع جريمة معلوماتية: اتهام شخص أو أشخاص معينين بارتكابها أو المشاركة فيها ، و توافر أمرات قوية أو قرائن تفيد في كشف الحقيقة [4]، على التفصيل الآتي :

---

[1] – راجع المادة 03/05 من القانون رقم 04/0 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها.

[2] – انظر عبد الإله هلالي الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مرجع سابق ، ص 225 وما بعدها.

[3] – نبيلة هبة هروال ، مرجع سابق ، ص229.

[4] – علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت (دراسة مقارنة)، عالم الكتب الحديث 2004، ص 62. حسين بن سعيد بن سيف الغافري، مرجع سابق، ص379-380.نبيلة هبة هروال ، مرجع سابق ص230.

أ-وقوع جريمة معلوماتية:

والجريمة المعلوماتية هي كما سبق القول كل فعل غير مشروع يكون الحاسوب الآلي وسيلته أو محله وذلك لتحقيق أغراض غير مشروعة [1]، وهناك العديد من التشريعات التي حرصت على استحداث نص خاص بالجريمة المعلوماتية، كما هو الحال بالنسبة لانجلترا التي أصدرت قانون إساءة استخدام الكمبيوتر في 29 يونيو 1990 ، وفي فرنسا صدر قانون رقم 88 /19 في 05 يناير 1988 الخاص بالغش المعلوماتي الملغى بقانون العقوبات الفرنسي الجديد الذي بدأ العمل به اعتبارا من أول مارس 1994 [2].

ومن أمثلة هذه الجرائم، الغش المرتبط بالحاسوب الإدخال، الإتلاف والمحو لبيانات أو برامج الحاسوب، التزوير المعلوماتي ، الدخول أو الاعتراض غير المشروع لنظام معلوماتي وأخطرها جرائم التجارة الالكترونية الواقعة على مواقع التجارة وبطاقات الائتمان والتوقيع الالكتروني .

وبالنظر إلى الطبيعة الفنية للجرائم المعلوماتية فإنه يمكن الاستعانة في ذلك بمأموري الضبط ذوي الخبرة الفنية بما يساعد في جمع الدليل ، لكن يحتاج التفتيش عن هذه الجرائم إلى معرفة كلمات السر أو مفاتيح الشفرة التي تمكن من الدخول إلى نظمها والإطلاع على محتوياتها [3].

---

[1] - علي حسن محمد الطوالبة ،مرجع سابق ، ص63 وما بعدها . راجع أيضا نائلة عادل قورة ، مرجع سابق 10

[2] - كما صدر بعض الدول العربية تشريعات للجريمة المعلوماتية ، من أبرزها :

-في الجزائر صدر القانون رقم 15/04 الموافق لـ 10نوفمبر 2004 المتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المعدل والمتمم لقانون العقوبات ، والقانون رقم 09-04 المتعلق والوقاية من جرائم الاتصال والمعلومات ومكافحتها -في مصر صدر القانون 15 رقم لسنة 2004

تكنولوجيا المعلومات.

--في تونس صدر القانون عدد 89 لسنة 1999 المؤرخ في 2 أوت 1999المتعلق بجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و المعدل لقانون العقوبات التونسي ، والقانون عدد 83 لسنة 2000 المؤرخ في 9 أوت 2000 المتعلق بالمبادلات والتجارة الالكترونية . الالكترونية التونسي .

[3] - شيماء عبد الغني عطاء الله ، مرجع سابق ، ص363 -هشام فريد ، مرجع سابق ، ص81-82.

ب- اتهام شخص أو أشخاص معينين بارتكابها أو المشاركة فيها :

فيشترط لجواز إصدار أمر بتفتيش نظم الحاسوب والانترنت أن يكون هناك اتهام موجه ضد شخص ،ولا يكفي توجيه التهمة إلى الشخص لإجراء التفتيش، بل ينبغي أن يتوفر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية ، سواء بوصفه فاعلا أو شريكا ، بحيث انه إذا لم تتوفر هذه الدلائل كان على قاضي التحقيق أن يصدر أمرا بأن لا وجه لإقامة الدعوى وهذا ما تؤكده المادة 163 من قانون الإجراءات الجزائية الجزائري والمادة 177 من قانون الإجراءات الجزائية الفرنسي[1].

ويقصد بتعبير الدلائل الكافية المظاهر والدلائل التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة وكذلك على خبرة القائم بالتفتيش والتي تنسب الجريمة المعلوماتية إلى شخص معين سواء بوصفه فاعلا أو شريك [2] .

يتمتع المتهم مبدأ وجوب افتراض براءته إلا أن يثبت العكس بالحكم الجنائي البات، وذلك عبر مراحل الدعوى الجنائية بالحماية المقررة له ، ويترتب على ذلك أنه لا يجوز إجباره على تقديم دليل يدين به نفسه، بل له الحق في الصمت إلا إذا كان كلامه دفاعا عنه. ويجب ألا يفسر صمته بأنه إقرار منه بصحة الاتهام المنسوب إليه [3] .

---

[1] – عبد الله هلالي ، التفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص120. وانظر أيضا:

Jean larguier,procedure pénale , Dalloz,1991. P.91.

[2] – هلالي عبد الله ، التفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص121. عبد الله حسين محمود، مرجع سابق، ص379.

[3] – ويترتب على الحق في الصمت ذلك أنه لا يجوز إجبار المتهم على كشف مفاتيح الدخول إلى نظم الوسائل الإلكترونية أو طباعة ملفات بيانات مخزنة ، تطبيقا لمبد البراءة

ج- توافر أمرات قوية أو قرائن تفيد في كشف الحقيقة :

فلا يكفي مجرد وقوع جناية أو جنحة بل يجب أن تتوافر أمارات وقرائن قوية على وجود أشياء تفيد في كشف الحقيقة ، ويستوي أن تكون هذه الأشياء المعلوماتية موجودة في حيازة الشخص أو في منزله [1].

وهكذا فإن التفتيش لا يجرى إلا إذا توفرت لذا المحقق أسباب كافية على أنه يوجد في المكان أو لدى الشخص المراد تفتيشه أدوات استعملت في الجريمة المعلوماتية أو أشياء المتحصلة منها أو أية أشياء أو مستندات الكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم المعلوماتي أو غيره [2].

وتقدير هذه الدلائل هو من المسائل الموضوعية متروكة لسلطة التحقيق ، فيجب أن يكون تقديرها منطقيا ومتفقا مع الواقع[3]، تحت رقابة محكمة الموضوع ، ومن ثمة إذا أراد المتهم أن يدفع ببطلان التفتيش لعدم الجدية عليه أن يتقدم به إلى محكمة الموضوع وليس محكمة النقض .

ويلاحظ أن الأشخاص الذين يتعاملون مع الوسائل الإلكترونية بحكم طبيعة عملهم لا يعتبرون شهودا وفقا لمدلول الشهادة كدليل إثبات في المواد الجنائية ، أما الشاهد بالنسبة للجرائم التي تقع في محيط الوسائل الإلكترونية فيقصد به صاحب الخبرة والتخصص في تقنية وعلوم الحاسب والذي تكون لديه معلومات جوهرية لازمة لإمكان الدخول في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة ويعد من هؤلاء الشهود مشغلو الحاسبات وخبراء البرمجة، المحللون، مهندسو الصيانة والاتصالات ومديرو النظم المعلوماتية [4].

---

[1] - عبد الله هلالي ، التفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص122. انظر أيضا حسين بن سعيد بن سيف الغافري، مرجع سابق ، ص381.

[2] - حسين عبد الله محمود، مرجع سابق، ص372.

Merle (roger) traite de droit tome procedure penale4 édition Cujas 1989 P.757.

[4] - شيماء عبد الغني عطاء الله ، مرجع سابق ، ص363.

وتفرض بعض التشريعات المقارنة التزاما قانونيا بالإدلاء أو بالإفصاح عن الشفرات وكلمات السر أو المرور للدخول إلى نظم الحاسبات الآلية وذلك من خلال التزامه بالإجابة على الأسئلة التي تتعلق بها، وما تستلزمه مصلحة التحقيق من طبع ملفات بيانات مخزنة[1].

وعلى ضوء ذلك يمكن القول بأن الشاهد يلتزم بالنسبة للجرائم الإلكترونية بطبع ملفات البيانات المخزنة في ذاكرة الحاسب أو حاملات البيانات الثانوية، وأن يفصح عن كلمات المرور السرية وعن أرقام الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة.

ولا شك في أن وجود الالتزام القانوني الذي بموجبه يمكن مطالبة المهنيين والحرفيين من الشهود ومستخدمي الوسائل الإلكترونية بالإعلام عن المعلومات والبيانات الجوهرية التي في حوزتهم، ليمثل أهمية كبيرة في إمكانية جمع الأدلة التي ترتكب على هذه الوسائل، وأنه يلعب دورا وقائيا هاما إذ أن تطبيقه يمنع من ضبط النظام الشبكي بأكمله وعدم عزله عن البيئة المعلوماتية.

2-محل التفتيش :

يتمثل الهدف من التفتيش في ضبط مكونات الحاسوب المادية والمعنوية والتي قد توجد في حوزة الشخص أو في مسكنه [2]، وبالتالي قد يكون الشخص محلا للتفتيش ، كمشغل الحاسوب أو من خبراء البرامج أومن المحللين أو مهندسي الصيانة والاتصالات أو أشخاص في حوزتهم معدات معلوماتية ، كما قد كون منزل الشخص محل للتفتيش أي مقر إقامته الدائم أو المؤقت [3].

---

[1] – فالمشرع الإجرائي الفرنسي يلزم الشهود الذين يقع عليهم التزام قانوني بأداء الشهادة بالكشف عن كلمات السر بالنسبة للحاسبات الآلية، ولا يعفيهم من هذا الالتزام إلا التمسك باحترام السر المهني[1]. للتفصيل راجع هلالي عبد الله ، التفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص123. وانظر أيضا هشام محمد فريد،الجوانب الإجرائية للجريمة المعلوماتية ، مرجع سابق ، ص89 .

[2] – حسين بن سعيد بن سيف الغافري، مرجع سابق ، ص382. عبد الله هلالي ، التفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص126.

[3] – يقصد بالمنازل كل محال الإقامة أو المأوى وكذلك الملحقات المخصصة لمنافعها والتي يشغلها الشخص بصفة مؤقتة أو دائمة وساء كانت ثابتة أو متنقلة ، وأيا كانت المادة المصنوعة منها .

ثانيا- الضوابط الشكلية:

بالإضافة إلى تلك الشروط الموضوعية للتفتيش المعلوماتي، توجد شروط شكلية يجب مراعاتها عند ممارسة هذا الإجراء صونا للحريات الفردية من التعسف أو الانحراف من استخدام السلطة [1]:

1- إجراء التفتيش من قبل سلطة مختصة بالتحقيق :

يجب أن يقوم بتفتيش نظم الحاسوب سلطة مختصة بالتحقيق ، وقد جعل المشرع المصري الاختصاص بالتفتيش كإجراء تحقيق في الجرائم التقليدية للنيابة العامة بصفة أصلية ولقاضي التحقيق في حالات خاصة ، وذلك على خلاف القانون الفرنسي والجزائري الذين أناطا الاختصاص الأصيل بقاضي التحقيق ، أما النيابة العامة فلا تختص بالتفتيش إلا في حالات معينة كالتلبس ، أما في انجلترا فإن معظم الإجراءات منوط بالشرطة ما عدا بعض الجرائم التي تناط بالمدعي العام[2].

2-الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش:

والهدف من ذلك ضمان الاطمئنان إلى سلامة الأجراء وصحة الضبط ، وقد استوجب المشرع الجزائري في المادة 1/45 أن يتم التفتيش في حضور صاحب المسكن الذي يجرى فيه التفتيش تحت طائلة البطلان [3] . وكذلك استلزم المشرع الفرنسي في الفقرة الأولى من المادة 57 من قانون الإجراءات الجنائية حضور صاحب المسكن الذي يجرى فيه التفتيش ، و إذا لم يتم حضوره يترتب على التفتيش البطلان [4].

---

[1] – عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت ، مرجع سابق ، ص389.

[2] – هلالي عبد الله ، التفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص125 . راجع عبد الفتاح بيومي حجازي، مبادئ لإجراءات الجنائية في جرائم الكومبيوتر والإنترنت ، مرجع سابق ، ص378 وما بعدها.

[3] – راجع المادة 45 من قانون الإجراءات الجنائية الجزائري .

[4] – نبيلة هبة هروال ، مرجع سابق ، ص225 . محمد الأمين البشري، مرجع سابق ، ص30.

غير أن المشرع الجزائري بموجب المادة 45 من القانون رقم 22/06 استثنى إجراء الحضور لبعض الأشخاص، إذا تعلق الأمر بالتفتيش في مجال الجرائم المعلوماتية [1]، لكن إذا تعلق التفتيش بمسكن موقوف صاحبه للنظر أو محبوس في مكان آخر أو الحال يقتضي عدم نقله بسبب مخاطر جسيمة تمس بالنظام العام أو احتمال فراره أو اختفاء الأدلة خلال المدة اللازمة لنقله ، أوجب المشرع بموجب المادة 47 حضور شاهدين مسخرين أو بحضور ممثل يعينه صاحب المسكن محل التفتيش[2].

3- تحرير محضر التفتيش:

بما أن التفتيش من أعمال التحقيق فينبغي تحرير محضر به يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة ، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، وبالتالي فإنه لا يشترط لصحته سواء ما تستوجبه القواعد العامة في المحاضر والتي تقضي بأن يكون المحضر مكتوب باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره وأن يتضمن كافة [3].

4- الميقات الزمني لإجراء التفتيش:

فحرصا على عدم التضييق من نطاق الاعتداء على الحرية الفردية وحرمة المسكن حرصت التشريعات الإجرائية على حضر القيام بتفتيش المنازل وما في حكمها في وقت معين، فالقانون الفرنسي ينص في المادة 59 من قانون الإجراءات الجزائية على أن التفتيش لا يمكن أن يبدأ قبل الساعة السادسة صباحا وبعد التاسعة مساءا، ولقد أخذت بعض التشريعات العربية بهذا كالقانون التونسي ، أما بالنسبة لتشريعات الدول الانجلوساكسونية كالقانون الإنجليزي والأمريكي فإنها لا تقيد التفتيش بوقت معين[4].

---

[1] – تنص المادة 7/45 من قانون الإجراءات الجنائية الجزائري على أنه لانطبق هذه الإحكام إذا تعلق الأمر بالجرائم المعلوماتية باستثناء الحفاظ على السر المهني وجرد الأشياء وحجز المستندات .

[2] – راجع المادة 47 من القانون رقم 22/06 المعدل والمتمم لقانون الإجراءات الجنائية الجزائري .

[3] –هلالي عبد الله ، التفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص167.

[4] – نبيلة هبة هروال ، مرجع سابق ، ص258 .

لكن المشرع الجزائري بموجب المادة 47 فقرة 03 قرر إجراء التفتيش والمعاينة والحجز في الجرائم المعلوماتية في كل ساعة من ساعات النهار أو الليل، وفي كل محل سكني أو غير سكني، بناء على إذن مسبق من وكيل الجمهورية المختص، إلا أنه أوجب الحفاظ على السر المهني[1].

5-الإذن بالتفتيش:

إذ نصت المادة 44 من قانون الإجراءات الجزائية الجزائري على ضرورة أن يكون التفتيش بناء على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا إذن قبل الدخول إلى المكان والشروع في التفتيش [2].

إن تفتيش نظم الحاسوب والانترنت يتطلب إذن قضائي خاصة في ظل ما يتقرر من قواعد تحمي الخصوصية وتحمي حقوق الأفراد، ويجب أن تكون المذكرة واضحة في تحديد النظام محل التفتيش، ويشترط في الإذن مايلي [3]:

أ- ضرورة أن يكون الإذن الصادر مكتوبا ومحددا التاريخ وموقعا ممن أصدره، وان يكون صريحا في الدلالة على التفويض في مباشرة التفتيش، وان يتضمن من البيانات ما يحدد نوع الجريمة المطلوب جمع الأدلة عنها، وتحديد محل التفتيش ، وتحديد المدة الزمنية[4].

ب - لكي يكون الإذن بالتفتيش صحيحا يجب أن يكون من أصدر الإذن مختصا بالتحقيق في الجريمة التي يصدر الإذن بشأنها.[5]

---

[1] - راجع المادة 3/47 من قانون الإجراءات الجنائية الجزائري .

[2] - راجع المادة 44 من قانون الإجراءات الجنائية الجزائري .

[3] - هلالي عبد الله ، التفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق ، ص138.

[4] - شيماء عبد الغني عطاء الله، مرجع سابق، ص281.

[5] - وهذا الاختصاص قد يتحدد بمحل الواقعة أو المكان الذي ضبط فيه الجاني أو بمحل إقامته، ويجوز أن تمتد بعض الإجراءات خارج هذا الاختصاص إذا تطلبت ظروف التحقيق ذلك بشرط أن يكون المحقق قد بدأ إجراءات التحقيق بدائرة اختصاصه المكاني.

ج- ويلزم كذلك أن يكون المحقق مختصا بالإجراء الذي يتخذه، فلا يجوز له ندب مأمور الضبط القضائي لتفتيش غير المتهم أو غير منزله لأن هذا التفتيش يخرج عن اختصاصه.

د- ويجب أن يكون من صدر له الإذن بالتفتيش من الضبطية القضائية المختصين بذلك وظيفيا ومكانيا ونوعيا، وينبغي أن تتوفر فيه أيضا خبرة معينة ، لكي يتمكن من تأدية عمله وفي ذات الوقت يحافظ على سلامة الأدلة الالكترونية.

المطلب الثاني : الضبط في مجال جرائم التجارة الالكترونية

حتى يحقق التفتيش غايته في جمع الأدلة، لابد من وسيلة التقاط تلك الأدلة وهذه الوسيلة هي الضبط، والضبط في معظم الأحيان يكون هو غرض التفتيش، وقد يحصل الضبط نتيجة لأسباب أخرى مثل المعاينة [1].

ويقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها ومن حيث طبيعته يعد من إجراءات الاستدلال والتحقيق[2].

اقعة على المكونات المادية للحاسوب لا يثير صعوبة للتقرير بصلاحية هذه الجرائم لضبط أدلتها ، ذلك أن الضبط لا يرد بحسب الأصل إلا على أشياء لكن بالنسبة للجرائم الواقعة على المكونات المعنوية يثير مشاكل بالنسبة لضبط أدلتها[3].

وعليه سنبحث موقف الفقه والتشريعات من مسألة صلاحية المكونات المعنوية من بيانات ومعلومات وبرامج للضبط والحجز، على النحو الآتي :

---

[1] - هشام فريد ، الجوانب الإجرائية للجريمة المعلوماتية ، مرجع سابق ، ص93.

[2] - وتتحدد طبيعته بحسب طريقة وضع اليد على الشيء المضبوط ، فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضى الأمر تجريده من حيازته كان الضبط بمثابة إجراء تحقيق ،أما إذا كان الاستيلاء عليها دون الاعتداء على حيازة قائمة فيكون بمثابة استدلال.

[3] - هلالي عبد الله ، التفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص197.

الفرع الأول: موقف الفقه من ضبط الأدلة الرقمية

ثار خلاف فقهي كبير حول مدى قابلية الأدلة الرقمية للضبط بين معارض ومؤيد ، كالآتي:

أولا –الرأي المؤيد:

يرى هذا الاتجاه إلى أنه إذا كان الضبط يهدف إلى كشف الحقيقة فإنه يمكن ضبط المكونات المعنوية كالبرامج والمعلومات، لأنها ذبذبات إلكترونية، أو موجات كهرومغناطيسية، تقبل التسجيل والحفظ والتخزين على وسائط مادية، وبالإمكان نقلها وبثها واستقبالها المادي لا يمكن إنكاره[1].

حيث يري الفقه الكندي إلى أنه يمكن ضبط المكونات المعنوية استنادا إلى نص المادة 487 التي تمنح سلطة الضبط لأي شيء طالما تتوافر أسس معقولة للاعتقاد بأن الجريمة ارتكبت أو يشتبه في ارتكابها أوان هناك نية في أن يستخدم في ارتكاب الجريمة أو أنه سوف ينتج دليلا على وقوع الجريمة [2].

وكذا يرى الفقه في لكسمبورغ انه يمكن ضبط مكونات الحاسب الآلي المعنوية لأن النص يشمل كل الأشياء التي تفيد في إظهار الحقيقة [3].

ثانيا– الرأي المعارض :

وفي المقابل هناك رأي آخر يرى انه لا يتصور ضبط الأدلة الرقمية من بيانات وبرامج ومعلومات إلا اتخذت شكلا ماديا، فالأدلة التي يتصور ضبطها يجب أن تكون أشياء مادية [4].

---

[1] – هشام محمد فريد ، الجوانب الإجرائية للجريمة المعلوماتية مرجع سابق، ص95.

[2] – ويستند الفقه الكندي أيضا إلى المادة 7/29 من قانون الإثبات الكندي التي تنص على أن تفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة مالية، يقتصر على تفتيش المكان بغرض تفقده وأخذ نسخة من المواد المكتوبة ، سواء كانت السجلات مكتوبة أم في شكل إلكتروني .

[3] – كامل عفيفي عفيفي ، مرجع سابق، ص378. نبيلة هبة هروال مرجع سابق، ص264.

[4] – هلالي عبد الله ، التفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق،ص218.

لذلك فإن هذه الأشياء المعنوية غير قابلة للضبط فهي تنقصها الخاصية المادية ، ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس عن طريق التصوير الفوتوغرافي، أو بنقلها على دعامة أو غيرها من الوسائل المادية ويستند هذا الرأي إلى أن النصوص التشريعية المتعلقة بالضبط محل تطبيقها الأشياء المادية الملموسة [1].

وفي هذا الإطار يرى الفقه الفرنسي أن النبضات الالكترونية أو الإشارات الالكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة، فهي لا تعتبر شيئا ماديا بالمعنى المألوف للمصطلح، لذلك لا يمكن ضبطها [2].

الفرع الثاني: موقف التشريعات من ضبط الأدلة الرقمية

النصوص التقليدية للضبط لتطبيقها بصدد البيانات والمعلومات والبرامج مجردة عن دعامتها المادية ، بل لابد من تدخل تشريعي يوسع من نطاق الأشياء الممكن ضبطها [3].

ولقد تدخل المشرع الفرنسي بإصدار القانون رقم 91 – 649 في 10 يوليه 1991 بشأن المراقبة القضائية للاتصالات الالكترونية ، واشترطت المادة 2/100 في الجريمة المراد ضبطها بهذه الوسيلة أن تكون جناية أو جنحة معاقب عليها بالحبس الذي يزيد عن سنتين وكذلك حدد ميعادا زمنيا للمراقبة مدته أربعة أشهر في حدها الأقصى وتكون قابلة للتجديد في حدها الأقصى وأنه يتعين أن يتم التسجيل وتفريغ التسجيل تحت سلطة القاضي[4].

---

[1] – هلالي عبد الله ، التفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص202. كامل عفيفي عفيفي ، مرجع سابق، ص378. نبيلة هبة هروال، مرجع سابق، ص265.

[2] – عفيفي كامل، لمرجع سابق، ص379. هلالي عبد الله ، التفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع السابق ، ص202. كامل عفيفي عفيفي ، مرجع سابق، ص378.

[3] – هشام محمد فريد ، الجوانب الإجرائية للجريمة المعلوماتية ، مرجع سابق، ص96.

[4] – راجع المادة 2/100 من قانون رقم 91 – 649 المؤرخ في 10 يوليه19991 المتعلق بالمراقبة القضائية للاتصالات الالكترونية.

كما نص المشرع الإنجليزي على صلاحيتها أيضا للضبط في قانون إساءة استخدام الكمبيوتر الصادر 1990، وقد ساير هذا الاتجاه مشروع قانون الحاسب الآلي الإسرائيلي[1] ، كما نص المشرع البلجيكي على قابلية المكونات المعنوية للضبط بموجب المادة 39 من قانون تحقيق الجنايات البلجيكي، المدخلة في التقنين بمقتضى القانون الصادر في 23 نوفمبر سنة 2000، حيث يشمل الحجز وفقا لهذا النص على الأشياء المادية، وعلى البيانات المعالجة إلكترونيا[2].

وخشية من محو أو إتلاف أو نقل أو ضياع الأدلة التي يتم الحصول عليها بطريق التفتيش، فقد أعطت المادة 88 من قانون تحقيق الجنايات البلجيكي لقاضي التحقيق سلطة الأمر بالتحفظ عليها، إن وجدت على الأرض البلجيكية، أو أن يطلب من السلطات الأجنبية نسخة من هذه البيانات إن وجدت لدى دولة أجنبية .

ولضمان الحفاظ على البيانات محل البحث ومقارنتها بالنسخة المخرجة من الجهاز في حالة نفيها من المتهم، فقد أعطى القانون البلجيكي بموجب المادة 39 مكرر 3 للنيابة العامة سلطة الأمر بسحب البيانات التي سبق أخذ نسخة منها، من الجهاز في حالة ما إذا كانت محلا للجريمة أو ناتجة عنها إذا كانت مخالفة للنظام العام أو الآداب ، إذا كانت خطرا على الأنظمة الإلكترونية ، أوكانت تمثل خطرا بالنسبة للمعلومات المخزنة أو المعالجة أو المرسلة بهذه الأنظمة [3].

وأيضا أجاز المشرع الجزائري بموجب المادة 47 الضبط أو الحجز في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في محل سكني أو غير سكني، و في ساعة من ساعات النهار أو الليل بإذن مسبق من وكيل الجمهورية [4].

---

[1] – هشام محمد فريد ، الجوانب الإجرائية للجريمة المعلوماتية مرجع سابق، ص96.

[2] – هلالي عبد الله ، التفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص202.

[3] – نبيلة هبة هروال ، مرجع سابق، ص265. محمد أبوبكر يونس ، مرجع سابق ، ص87 .

[4] – تنص المادة 47 من قانون الإجراءات الجنائية على أنه "عندما يتعلق الأمر.... الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .. فإنه يجوز إجراء التفتيش و المعاينة و الحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل و ذلك بناء على إذن مسبق من وكيل الجمهورية المختص ".

وقرر المشرع الجزائري أيضا حجز المعطيات المعلوماتية في المادة 06 من القانون 04/09 المتعلق بالوقاية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

فوفقا للمادة 06 عندما تكشف السلطة التي تباشر التفتيش معطيات تفيد في كشف الجرائم أو مرتكبيها يتم نسخ المعطيات محل البحث على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية ، ويجب على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة التي تجري بها العملية [1].

التقنيات المناسبة لمنع الوصول إلى المعطيات أو نسخها[2].

ويجب على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية [3].

ولا يجوز للسلطات استعمال المعلومات المتحصل علبها عن طريق المراقبة الافي الحدود الضرورية للتحريات أو التحقيقات تحت طائلة قانون العقوبات[4].

ومن أجل ضبط أدلة الجريمة فإن المشرع الجزائري بموجب المواد 65 مكرر إلى 65 مكرر10 ، أجاز اعتراض المراسلات وتسجيل الأصوات والتقاط الصور إذا اقتضت ذلك ضرورة التحقيق الابتدائي بإذن من قاضي التحقيق لمدة أربعة أشهر قابلة للتجديد، وتنفذ العمليات المأذون بها تحت مراقبة مباشرة لقاضي التحقيق، و دون المساس بالسر المهني المنصوص عليه في المادة 45 من قانون الإجراءات الجنائية [5].وبالتالي تنفذ العمليات المأذون بها على هذا الأساس وفقا

---

[1] – راجع المادة 1/6 من قانون 04/09 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها.

[2]- راجع المادة 07 من نفس القانون .

[3] – يمكن للسلطات التي تباشر التفتيش لأن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة ، لاسيما عن طرق تكلف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك .

[4] – راجع المادة 09 من قانون 04/09 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها.

[5] – راجع المواد 65 مكرر إلى 65 مكرر10 من قانون الإجراءات الجنائية الجزائري

للمادة 65 مكرر 4 ، والمادة 65 مكرر05 تحت المراقبة المباشرة لوكيل الجمهورية المختص ، وفي حالة فتح تحقيق قضائي تتم العمليات المأذون بها تحت المراقبة المباشرة لقاضي التحقيق [1].

أجاز المشرع أيضا لقاضي التحقيق الإذن بمباشرة عملية التسرب في إحدى الجرائم المنصوص عليها في المادة 65 مكرر5، إذا اقتضت ذلك ضرورة التحقيق الابتدائي بعد إخطار وكيل الجمهورية ضمن الشروط المنصوص عليها في المواد65 مكرر11 إلى المواد 65 مكرر 18 من قانون الإجراءات الجنائية الجزائري [2]. كما تناول المشرع الجزائري التسرب وسماه بالاختراق في المادة 56 من قانون رقم 01/06 المؤرخ في 2006 المتعلق بالوقاية من الفساد مكافحته [3].

ويقصد التسرب وفقا للمادة 65 مكرر 12 بأنه قيام ضابط أو عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك معهم أو كخاف [4].

---

[1] – ويراقب القضاء العمليات المأذون بها رقابة المشروعية، بمراقبة مدى مطابقة عمليات الاعتراض والالتقاط والتسجيل للقانون ، كوجوب الحصول على إذن قضائي ، وعدم تجاوزه مدة الإذن وعدم المساس بالسر المهني ، كما يراقب القضاء تلك العمليات رقابة موضوعية، من خلال تقدير مدى قيمة وكفاية أدلة الإثبات الموجودة في محاضر الضبطية القضائية .

وعليه يقتصر دور القضاء على الجوانب القانونية والموضوعية، بينما تعود الرقابة التقنية لضباط الشرطة القضائية أو الأعوان المسخرين لهذا الغرض، باعتبارهم أكثر معرفة و دراية بتقنيات التحري والتحقيق .

[2] –راجع المواد65 مكرر11 إلى المواد 65 مكرر 18 من قانون 22/06 المؤرخ في 20 ديسمبر 2006 .

[3] – راجع المادة 56 من قانون رقم 01/06 المؤرخ في 20 فيفري2006 المتعلق بالوقاية من الفساد مكافحته ج . ر 14 صادرة في 8 مارس 2006 .

[4] – يشترط قانون الإجراءات الجزائية في التسرب : الإذن القضائي وفقا للمادة 65 مكرر 15 ، وتقرير عملية التسرب طبقا للمادة 65 مكرر 13 ، وأن تمارسه جهة مختصة وفقا للمادة 65 مكرر 12 وهي ضابط الشرطة القضائية أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، أو الأشخاص المسخرين لهذا الغرض من قبل ضابط الشرطة القضائية المكلف بتنسيق العملية حسب المادة 65 مكرر 14 .

الفصل الثاني

الحماية الجنائية الإجرائية للتجارة الالكترونية في مرحلة المحاكمة

تخطى مدى الجريمة المعلوماتية لاسيما جرائم التجارة الالكترونية حدود الدول بل والقارات ولم يعد خطرها أو آثارها محصورة في النطاق الإقليمي لدولة بعينها ، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام أجهزة العدالة الجنائية المعنية بمكافحة الجريمة .

أبرزها مسألة تحديد المحكمة الجنائية المختصة في مجال جرائم التجارة الالكترونية، لأنه يترتب على ذلك تحديد القانون الواجب التطبيق في حالة تنازع القوانين ، ذلك أن ملاحقة الجناة وكشف جرائمهم عبر الحدود يقتضي من الناحية العملية أن يتم في نطاق إقليم دولة أخرى ، وهو

تنازع الاختصاص القضائي بسبب صعوبة تحديد مكان وقوع الجريمة المعلوماتية عبر الوطنية .

كما تثير هذه الجرائم ومسألة سلطة المحكمة الجنائية في قبول وتقدير الأدلة الرقمية والالكترونية فلقد تركت ثورة تقنية المعلومات انعكاسات واضحة على إثبات الجريمة المعلوماتية عبر الوطنية بخلاف الجرائم التقليدية ، بالنظر إلى طبيعة هذا النوع من الجرائم وما تتسم به من خصائص وسمات،
والتصدي لها ، وتكمن المشكلات المتعلقة بالإثبات في أن هذه الجرائم باعتبارها تقع في
ة.

وعليه سنبحث تحديد المحكمة الجنائية المختصة في جرائم التجارة الالكترونية (المبحث الأول) وسلطة تلك المحكمة الجنائية في تقدير الأدلة الرقمية (المبحث الثاني).

المبحث الأول

تحديد المحكمة الجنائية المختصة في جرائم التجارة الالكترونية

إن قواعد القانون الجنائي تخضع في تطبيقها من حيث المكان لمبدأ الإقليمية الذي يعني خضوع الجرائم التي تقع في إقليم دولة معينة لقانونها الجنائي النافذ بحيث تصبح محاكمها هي صاحبة الولاية بنظر الدعوى الناشئة عنها[1].

ويتحدد اختصاص المحكمة بمكان وقوع الجريمة أو إقامة المتهم أو القبض عليه ، ولا تخضع من حيث الأصل لسلطان أي قانون أجنبي، وفي المقابل لا يمتد سريان قانون الدولة الجنائي خارج .[2]

بيد أن الجرائم المعلوماتية لاسيما جرائم التجارة الالكترونية لا يكتمل الركن المادي للجريمة في مكان واحد اوز مداها حدود الدولة ، حينما يتوزع ركنها المادي على أكثر من مكان إذ يقع السلوك في مكان ، في حين تتحقق النتيجة الإجرامية الضارة في نطاق إقليم دولة أخرى .

وهذا ما أدى إلى اختلا فقهي وقضائي حول المحكمة الجنائية المختصة، لكن بعض التشريعات تجاوزت ذلك الاختلاف بتدخل تشريعي حدد معاييراختصاص المحكمة الجنائية في الجرائم الالكترونية كالتشريع الجزائري .

---

[1] – والقانون الجزائري على غرار القانون المصري والفرنسي أخذ بمبدأ إقليمية القوانين إذ نص المادة 3 من قانون العقوبات على أنه " يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية، كما تطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية الجزائرية طبقا لأحكام قانون الإجراءات الجزائية".

[2] – تنص المادة 329من قانون الإجراءات الجنائية الجزائري : "تختص محليا بالنظر في الجنحة محكمة محل الجريمة أو محل إقامة أحد المتهمين أو شركائهم أو محل القبض عليهم ولو كان هذا القبض قد وقع لسبب آخر.... وتختص المحكمة التي ارتكبت في نطاق دائرتها المخالفة أو المحكمة الموجودة في بلد إقامة مرتكب المخالفة بالنظر في تلك المخالفة.

وعليه سنبحث الاختصاص الجنائي في الجرائم المعلوماتية لاسيما في جرائم التجارة الالكترونية في الفقه والقضاء (المطلب الأول) وفي تشريعات الدول (المطلب الثاني).

المطلب الأول: موقف الفقه والقضاء من تنازع الاختصاص الجنائي المعلوماتي

ثار خلاف فقهي وقضائي كبير حول تحديد المحكمة الجنائية المختصة في الجرائم المعلوماتية بما فيها جرائم التجارة الالكترونية ،على التفصيل الآتي :

الفرع الأول: موقف الفقه من تنازع الاختصاص الجنائي المعلوماتي

حاول الفقه حل مشكلة تنازع الاختصاص، وانقسم إلى ثلاثة اتجاهات وهي : مذهب النشاط الإجرامي ، مذهب مكان تحقق النتيجة ، والمذهب المختلط ، على النحو الآتي:

أولا- مذهب السلوك أو النشاط الإجرامي :

التي يقع في نطاقها النشاط الإجرامي، وليس مكان حصول النتيجة أو الآثار المترتبة عليه؛ بدعوى أن اتخاذ آثار الفعل كمناط لتحديد مكان وقوع الجريمة تكتنفه بعض الصعوبات؛ يمكن إجمالها في أنه معيار مرن و فضفاض [1].

في الغالب أسباب لا إرادة لمقترف السلوك فيها ، وأن من شأن تطبيق قانون الدولة التي تحقق في

.[2]

---

[1] _

تكون قريبة من مسرح الجريمة، ناهيك أن الحكم يكون أكثر فعالية. للتفصيل انظر أسامة المناعسة ، مرجع سابق ص210.

[2] – وقد حظي هذا الاتجاه بتأييد جانب كبير من الفقه سواء في فرنسا أو مصر، ليس هذا فحسب، بل اتجهت بعض التشريعات المقارنة إلى تبنيه، ومنها القانون النمساوي والمجري.

لكن يؤخذ على هذا الاتجاه عدة انتقادات ، أبرزها أن بعض الأفعال قد لاتجرمه الدولة التي وقع النشاط الإجرامي فيها مما يساعد الجناة على التهرب من العقاب[1].

ثانيا- مذهب مكان تحقق النتيجة :

على الرغم من الحجج التي ساقها مؤيدو المذهب الأول، فإن هذا الاتجاه تعرض لجملة من

فيه الضرر الذي كان الجاني يسعى إلى تحقيقه.

والآثار الضارة هي التي تبعث الفزع في نفوس الناس ، في حين أن مكان وقوع السلوك لا يعدو

آثارها الضارة التي كان الجاني يقصدها[2].

يضاف إلى ذلك أن تقادم الجريمة يتم احتسابه من الوقت الذي تحققت فيه النتيجة ، كما يؤخذ في الحسبان جسامة الضرر كأساس لتقدير التعويض ولا عبرة بخطورة الفعل أو درجة الخطأ المدنية ، فتنفى بانتفاء الضرر.

لكن يؤخذ على هذا الاتجاه أنه لا يراعي مصلحة المتهم بجره إلى أماكن بعيدة للمحاكمة مما يزيد ي تكالي التقاضي ويطيل الخصومة.

ثالثا- المذهب المختلط :

أمام الانتقادات التي تعرض لها كلا الاتجاهين السابقين ، برز اتجاه ثالث يرى أن ينعقد الاختصاص للمحكمة الجنائية التي يقع في نطاقها النشاط الإجرامي أي مكان حصول الفعل وكذا المكان الذي تحققت فيه النتيجة أو الذي من المتوقع أو المنتظر تحققها فيه وهذا الراجح[3].

---

[1] – أسامة المناعسة ، مرجع سابق، ص210.

[2] – أسامة المناعسة ، مرجع سابق، ص211.

[3] – ومن المبررات التي سيقت لتعزيز هذا الاتجاه أن الأخذ به يحقق وحدة الجريمة وعدم الفصل بين عناصرها ، كذلك يمتاز هذا الاتجاه في نظر المدافعين عنه بأنه أكثر و

وهذا الاتجاه أخذت به بعض التشريعات المقارنة، ومنها قانون العقوبات النرويجي وكذلك الدانمركي ، والصيني والألماني والإيطالي ، كما تبنته بعض محاكم الدول ومنها فرنسا [1].

بالوقوف على المبررات التي استند إليها كل اتجاه، نرى أن الرأي الأخير هو الراجح، لكونه تجاوز المآخذ التي اعترت المذهبين الآخرين، وفي الوقت ذاته استجمع ميزات كل منهما ، فهو يوسع من نطاق الحماية الجنائية ويتيح مرونة أكثر في مد نطاق الاختصاص لاسيما وأن بعض

دول أخرى غير التي وقع فيها النشاط ، الأمر الذي يهدد مصالحها الحيوية .

و

الاختصاص التي يفترض عدم تضييق نطاقها ، بحيث يكون من الملائم أن ينعقد الاختصاص لقانون أي بلد أضرت به الجريمة أو من المتوقع أن تشكل خطورة على مصالحه الحيوية ، ولو كان مكان وقوعها خارج نطاق إقليمها ومن المناسب تبني مبدأ الاختصاص العالمي من أجل تجنب الكثير من المشاكل الناجمة عن تحديد مكان وقوع الجريمة أو ترتب آثارها الضارة [2].

الذي قد لا يكون كذلك متى ما اتخذ صورة الامتناع أو السلوك السلبي ويجد مبرره أيضا في أن الركن المادي للجريمة يقوم على ثلاثة عناصر ، وهي الفعل (النشاط) والنتيجة ، وعلاقة السببية ،

[1] – وهنا يتم تغليب قانون محل تحقق النتيجة إذا كانت الجريمة تامة ، ومن قبيل ذلك جرائم السلوك والنتيجة (الجرائم المادية) ، في حين يفضل مكان النشاط أو السلوك إذا كانت الجريمة قد وقفت عند حد الشروع أو من قبيل جرائم السلوك

[2] – ويقصد بهذا المبدأ أن المحاكم الجنائية تختص بمحاكمة مرتكبي بعض الجرائم الدولية بغض النظر عن مكان وقوع الجريمة وجنسية المتهم. وبالتالي يقوم الاختصاص الجنائي العالمي على منح القضاء الداخلي سلطة محاكمة مجرمين عن أفعال ارتكبوها خارج إقليم الدولة، بغض النظر عن مكان ارتكاب الجريمة أو جنسية المتهم أو الضحية ، فلا تكون الدولة بموجب الاختصاص الجنائي العالمي على علاقة مباشرة بالجريمة من خلال جنسية الجاني أو المجني عليه أومن خلال مكان ارتكاب الجريمة ، كما لاتقوم المتابعة الجنائية على وجود مصلحة خاصة بالدولة ، بل تكون ت المصلحة المشتركة للجماعة الدولية في حماية البشرية من أبشع الجرائم ، هو المحفز على اتخاذ إجراءات المتابعة الجنائية .

يتميز مبدأ الاختصاص الجنائي العالمي بأنه اختصاص أصيل، أي أنه يجد سنده وأصله في التشريع الداخلي للدولة التي ينتمي إليها بوصفه جزءا من النظام القانوني للدولة بعد تبنيها الالتزام الدولي بملاحقة مرتكبي الجرائم الدولية واتخاذ التدابير التشريعية اللازمة ، وكذلك اختصاص تكميلي ، أي أن القضاء الوطني ينعقد اختصاصه طبقا لمبدأ الاختصاص العالمي إذا لم يكن بوسعه ممارسة اختصاصه وفقا لمبدأ الإقليمية أو مبدأ الشخصية أو مبدأ العينية ، وأيضا اختصاص احتياطي ، واختصا ص سابق على اختصاص المحكمة الجنائية الدولية.

الفرع الثاني: موقف القضاء من تنازع الاختصاص الجنائي المعلوماتي

أولا- القضاء الأمريكي والانجليزي :

ي لها في أكثر من مناسبة ، ففي القضاء الأمريكي تشير التطبيقات القضائية إلى أنه يكفي لامتداد ولاية القضاء إلى جريمة وقعت في الخارج أن تكون آثارها قد مست مصالح أمريكية أو الاختصاص الشخصي.

من ذلك ما قضت به المحكمة العليا لولاية نيويورك بصدد جريمة انتهاك قانون المستهلك

مسجلة في الولاية الأولى، وقد أسست المحكمة حكمها على أن قضاء بنسلفانيا ينعقد له الاختصاص الشخصي على اعتبار أن مزود خدمة الإنترنت له مشتركون في الولاية [1].

وثمة قضية مماثلة جرى فيها إعمال المبدأ ذاته (مبدأ النتيجة) ، ألا وهي قضية (مينيسوتا ضد جرانتي جات ريسورت) بشأن بث موقع لألعاب القمار عبر الإنترنت من لاس فيغاس بولاية نيفادا الذي وصل إلى ولاية (مينيسوتا) التي يحظر قانونها مثل هذه الألعاب، وتكرس هذا الاتجاه القضائي فيما انتهت إليه الدائرة الخامسة الاستئنافية في قضية قمار ومراهنات عبر الإنترنت[2].

[1] – إن القانون الأمريكي يتسع نطاق تطبيقه بحيث يمتد إلى الأفعال المرتكبة في الخارج طالما أن آثارها تحققت في الولايات المتحدة الأمريكية. للتفصيل راجع عمر محمد بن يونس، مرجع سابق، ص908.

[2] – وقد اعتبر القضاء المذكور مجرد وضع برمجية فك التشفير(ب ج ب) على الإنترنت بمثابة تصدير لها، وهو ما يخول المحاكم الأمريكية التصدي لها باعتبارها صاحبة الاختصاص، بصرف النظر عن مكان وضع البرمجية. للتفصيل راجع محمد أبو بكر بن يونس، مرجع سابق ، ص910 .

ابهة ، فهو يختص بنظر الدعاوى الناشئة عن إساءة

استخدام الإنترنت

استخدام الحاسوب الصادر سنة 1990، فلكي ينعقد الاختصاص للمحاكم الإنجليزية ، يكفي امتداد آثار الواقعة إلى بريطانيا، ولو كانت هذه الواقعة قد حدثت في الخارج ، وبصرف النظر عن محل إقامة الجاني[1].

ثانيا –القضاء الفرنسي:

أما في فرنسا فتقضي المحاكم الفرنسية باختصاصها ولو حدثت الواقعة في الخارج ، وتطبيق لذلك قضت المحكمة الابتدائية بباريس باختصاص المحاكم الفرنسية ، إذا كان مركز البث موجود خارج الإقليم الفرنسي ، ويقوم الجهاز ببثها ي فرنسا ينعقد الاختصاص للمحاكم الفرنسية غير أنه يلزم توار قاعدة التجريم المزدوج بين القانون الفرنسي وقانون الدولة التي يصدر منها البث[2].

للجرائم التقليدية المعروفة الأمر الذي يجعلها في كثير من الأحيان تستعصي على الخضوع

الصنف من الجرائم المستحدثة تتطلب تجاوز المعايير التي طرحها الفقه للتغلب على مشكلة تنازع الاختصاص [3].

---

[1] – بعبارة أخرى ، يكفي أ

موجود في بريطانيا. راجع محمد بن يونس، مرجع سابق ، ص912 .

[2] – شيماء عبد الغني عطاء الله ، مرجع سابق ، ص371.

[3] – يجب العمل على تبني حلول أكثر مرونة تأخذ في الحسبان النطاق الجغرافي لهذه الجرائم وسهولة ارتكابها وآلية

.

المطلب الثاني: موقف التشريعات من تنازع الاختصاص الجنائي المعلوماتي

كثير من الأحيان لأكثر من قانون ، فإذا وقع السلوك في نطاق بلد معين والآثار الضارة تحققت في نطاق بلد آخر ، فكلاهما واجب التطبيق على الواقعة ، بمعنى تطبيق قانون كل دولة تحقق فيها أحد عناصر الركن المادي .

الأمر الذي يفضي عادة إلى حدوث تنازع في الاختصاص بشأن الجرائم المعلوماتية ، أي أن الفعل يتنازعه قانونان، قانون دولة الإقليم على أساس مبدأ الإقليمية ، وفي الوقت ذاته قد يخضع . ليس هذا فحسب، بل قد ينعقد الاختصاص
[1] ، وللتغلب على هذه

الصعوبات أوجدت التشريعات معايير لتحديد الاختصاص.

الفرع الأول: الاختصاص الجنائي المعلوماتي في التشريع الجزائري

أولا-الاختصاص الجنائي الدولي :

طبقا لمبدأ إقليمية القوانين ينطبق القانون الجزائري على الجرائم التي تقع على إقليم الجزائر بغض النظر عن جنسية مرتكبها أوجنسية المجني عليه [2]، وبالتالي إذا تمت جرائم الانترنت النتيجة بالجزائر.

والعبرة في تحديد دولة القانون المطبق بوقوع الجريمة كاملة أو جزء منها على إقليم الدولة وكذلك

---

[1] -جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص72-73

[2] – نص المشرع الجزائري على هذا المبدأ في لمادة 3 من قانون العقوبات : "يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية الجزائرية طبقا لأحكام قانون الإجراءات الجزائية". يعني تطبيق قانون الدولة على كل الجرائم الواقعة في نطاقه

الحال في الجرائم المستمرة أو التتابعية ، حيث يكفي أن يتحقق جزء من حالة الاستمرار أو فقرة من فقرات التتابع [1].

ووفقا لمبدأ شخصية القوانين يطبق أيضا القانون الجزائري إذا ارتكب جزائري جريمة من جرائم الانترنت أو التجارة الالكترونية، أو كان المجني عليه جزائري الجنسية لحظة وقوع الجريمة .

إلا أن الأخذ بهذا المبدأ قد يصطدم بمجموعة من العقبات، فمن ناحية نجد أن محاكمة المتهم الذي يقيم في دولة أجنبية تحتاج إلى إجراءات طويلة وشاقة وكلفة كما يصطدم بعقبة عدم وجود اتفاقيات لتسليم المجرمين، بالإضافة إلى الإطاحة بمبدأ دستوري وهو عد جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة [2].

وعملا بمبدأ العينية فإن الاختصاص يكون للمحاكم إذا وقعت جريمة من جرائم الانترنت أو التجارة الالكترونية بصفة خاصة تمس مصالح الدولة الأساسية والجوهرية حتى وان وقعت خارج الدولة وبغض النظر عن جنسية مرتكبيها [3].

وأخذ بهذا المبدأ التشريع الجزائري في المادة 588 غير أن المشرع هنا حصر الاختصاص للمحاكم الجزائرية لجرائم ترتكب خارج الإقليم الجزائري وكانت الجريمة جناية أو جنحة ضد سلامة الدولة الجزائرية أو تزييفا أو نقود أو أوراق مصرفية وطنية متداولا وان كان مرتكبها أجنبيا [4].

وعليه إن كيفت الجريمة المعلوماتية بأنها مخلة بأمن الدولة الجزائرية، وفقا لقانون العقوبات الجزائري سواء أكان الإخلال بأمن الدولة سياسيا أو عسكريا أو اقتصاديا، فان الاختصاص هنا

---

[1] – حسين بن سعيد بن سيف الغافري، مرجع سابق، ص544

[2] – جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص60.

[3] – حسين بن سعيد بن سيف الغافري ، مرجع سابق ، ص560.

[4]– تنص المادة 588 على أنه "كل أجنبي ارتكب خارج الإقليم الجزائري بصفة فاعل أصلي أو شريك جناية أو جنحة ضد سلامة الدولة الجزائرية أو تزييفا أو نقود أو أوراق مصرفية وطنية متداولا قانون بالجزائر تجوز متابعته ومحاكمته وفقا لأحكام القانون الجزائري إذا القي القبض عليه في الجزائر أو حصلت الحكومة على تسليمه لها.

يعود للمحاكم الجزائرية. إذ تجوز متابعته ومحاكمته وفقا لأحكام القانون الجزائري إذا القي القبض عليه في الجزائر أو حصلت الحكومة على تسليمه لها [1].

ثانيا –الاختصاص الجنائي الوطني:

يتحدد الاختصاص المحلي للجهات القضائية بمكان وقوع الجريمة ومحل إقامة أحد الأشخاص المشتبه في مساهمتهم في الجريمة أو بالمكان الذي تم في دائرته القبض على هؤلاء الأشخاص، غير أن المشرع الجزائري مدد الاختصاص القضائي لهؤلاء بموجب القانون 14/04 الموافق لـ10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66 /155 الموافق لـ 08 يونيو 1966 والمتضمن قانون الإجراءات الجزائية[2].

1–الاختصاص المحلي للنيابة العامة:

يتحدد الاختصاص المحلي للنيابة العامة وفقا للمادة 37 من قانون الإجراءات الجزائية بمكان وقوع الجريمة ومحل إقامة أحد الأشخاص المشتبه في مساهمتهم في الجريمة أو بالمكان الذي تم في دائرته القبض على هؤلاء الأشخاص[3].

وبالتالي فإن اختصاص وكيل الجمهورية يجب أن لا يتعدى مكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه فيهم أو بمكان القبض على هؤلاء.

لكن لما كانت جرائم الانترنت جريمة قد ترتكب في مكان معين وترتب آثارها في مكان آخر فإن المشرع الجزائري بموجب المادة 37 الفقرة 2 من القانون 14/04 أجاز تمديد الاختصاص

---

[1] – أسند المشرع الجزائري الاختصاص 588 من قانون الإجراءات الجنائية في الجرائم المرتكبة في الخارج ضد أمن الدولة الجزائري ، لكنه اشترط القبض عليه في الجزائر أو حصلت الحكومة الجزائرية على تسليمه لها.

[2] – يلاحظ أن المشرع الجزائري لم يحدد معايير الاختصاص المحلي في الجريمة الالكترونية في القانون 14/04 المعدل والمتمم للأمر رقم 66 /155

[3] – راجع المادة 47 من قانون الإجراءات الجنائية الجزائري

المحلي لوكيل الجمهورية إلي دائرة اختصاص محاكم أخري إلا أنه ترك كيفية تطبيق ذلك عن طريق التنظيم[1].

ويتعين علي ضابط الشرطة القضائية طبقا للمادة 40 مكرر 01 من القانون السابق أن يخبر وكيل الجمهورية لدى المحكمة الكائن بها الجريمة ويبلغونه بأصل ونسختين من إجراءات البحث ويرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدي المجلس القضائي التابعة له المحكمة المختصة [2]، ويطالب النائب العام طبقا للمادة 40 مكرر 2 بالإجراءات فورا إذا أعتبر أن الجريمة تدخل ضمن اختصاص المحكمة المذكورة في المادة 40 مكرر من قانون الإجراءات الجنائية [3].

2- الاختصاص المحلي لقاضي التحقيق:

يقصد بالاختصاص المحلي القاضي التحقيق المجال الذي يباشر فيه قاضي التحقيق عمله في التحقيق ويتحدد الاختصاص المحلي لقاضي التحقيق طبقا للمادة 40 من قانون الإجراءات الجزائية لمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو محل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر.

وبالتالي أجاز المشرع إمكانية تمديد الاختصاص المحلي لقاضي التحقيق في الجرائم المعلوماتية إلى دائرة اختصاص محاكم أخرى لكنه ترك تحديد كيفية تطبيق تلك الإجراءات للتنظيم[4].

3-الاختصاص المحلي لمحاكم الجنح:

---

[1] – وهو المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006، ج ر 63 مؤرخة في 10/08/ 2006 ، والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق .

راجع المادة 37 الفقرة 2 من القانون 14/04المعدل والمتمم للامر 155/66 المتعلق بقانون الإجراءات الجنائية الجزائري

[2] – جباري عبد المجيد ، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة ، دار هومة ، الجزائر 2012 ، ص119.

[3] –راجع المادتين 40 مكرر 1 –40 مكرر 2 من القانون 14/04المعدل والمتمم لقانون الإجراءات الجنائية الجزائري

[4] –إلا أن المشرع ألغى في التعديل الجديد الفقرة 2 و3 من هذه المادة 40 , وأصبحت تنص الفقرة 2 على أنه يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم المعلوماتية .

يتحدد الاختصاص المحلي لمحاكم الجنح طبقا للمادة 329 من قانون الإجراءات الجزائية الجزائري بمكان وقوع الجريمة ، أو بمحل إقامة أحد الأشخاص المتهمين أو شركائهم ، أو بمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى ولو تم القبض لسبب آخر[1].

غير أن المشرع في التعديل الصادر بموجب القانون 14/04 أضاف فقرة رابعة للمادة 329 أجاز فيها في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم [2].

إذن فإن المشرع أجاز بموجب المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006 والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ، في حالة ارتكاب جريمة من جرائم الماسة بأنظمة المعالجة الآلية للمعطيات تمديد اختصاص وكيل الجمهورية واختصاص قاضي التحقيق واختصاص محاكم الجنح [3].

---

[1] – تنص المادة 329 / فقرة 04 من القانون14/04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري يعلى أنه يجوز تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طرق التنظيم في جرائم ... الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ..... '.

[2] – عبد المجيد جباري ، مرجع سابق ، ص119.

[3] – وبالتالي أجاز المشرع الجزائري تمديد الاختصاص الجنائي بموجب المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006، والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ، كالآتي :

– يمتد الاختصاص المحلي لمحكمة سيدي أمحمد ووكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس القضائية للجزائر والشلف والأغواط والبليدة والبويرة وتيزي وزو والجلفة والمدية والمسيلة وبومرداس وتيبازة وعين الدفلى.

– يمتد الاختصاص المحلي لمحكمة قسنطينة ووكيل الجمهورية وقاضي التحقيق بها إلى محاكم لمجالس القضائية لقسنطينة وأم البواقي وباتنة وبجاية وبسكرة وتبسة وجيجل، وسطيف سكيكدة، عنابة، قالمة، برج بوعريريج، الطارف، الوادي، خنشلة، سوق أهراس وميلة .

–يمتد الاختصاص المحلي لمحكمة ورقلة ووكيل الجمهورية وقاضي التحقيق الى محاكم المجالس القضائية ورقلة وأدرار وتامنغست واليليزي وتندوف وغرداية .

–يمتد الاختصاص المحلي لمحكمة وهران ووكيل الجمهورية وقاضي التحقيق إلى محاكم المجالس القضائية لوهران وبشار وتيارت وسعيدة، تسيمسيلت سيدي بلعباس، مستغانم، معسكر البيض، النعامة، عين تيموشنت، غيليزان.

وتجدر الإشارة الى أن المشرع الجزائري مد الاختصاص الجنائية لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق بموجب المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006 والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، لكنه في الحقيقة امتداد داخلي ولبس خارجي ولا يشمل الجرائم الواقعة في الخارج إلا أنه يمكن تطبيق القواعد العامة المنصوص عليها في المواد 582-589 من قانون الإجراءات الجنائية ، بالنسبة للجرائم المرتكبة في الخارج .

الفرع الثاني: الاختصاص الجنائي المعلوماتي في التشريعات المقارنة

في القانون الفرنسي يمتد اختصاص القضاء هناك إلى جرائم الإنترنت التي وقعت في الخارج

عليها الوطني[1].

كما يمنح قانون العقوبات الفلندي الاختصاص للقضاء الوطني في مكان وقوع الجريمة وفي مكان حدوث نتائج الجريمة التي وقعت ، أوفي المكان المقصود حدوثها فيه ي حالة الشروع وفقا للمادة 04 من قانون العقوبات الفلندي[2].

يوسع القانون الأمريكي نطاق تطبيقه بحيث يمتد إلى الأفعال المرتكبة في الخارج طالما أن آثارها تحققت في الولايات المتحدة الأمريكية.

كما تمنح بعض تشريعات الولايات المتحدة الأمريكية كما هو الحال بالنسبة لقانون جرائم الكمبيوتر لولاية أوكلاهوما الاختصاص في الجرائم المعلوماتية إلى محكمة مكان الدخول إلى جهاز الكمبيوتر وكذلك إلى محكمة مكان وجود الكمبيوتر المخترق وفقا للمادة 1957/فقرة 21 [1].

---

[1] – جميل عبد الباقي الصغير ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت ، مرجع سابق ، ص73.

[2] – شيماء عبد الغني عطاء الله ، مرجع سابق ، ص373.وانظر أيضا :

Pascal vergucht.,op ,cit, p336

كما وضع القانون الانجليزي قواعد خاصة للاختصاص في مجال جرائم الكمبيوتر بمقتضى قانون 1990بموجب المادة 5 حتى ولو لم يحدث الفعل المجرم على الإقليم الانجليزي أو تواجد المتهم على هذا الإ ن الانجليزي[2] .

ويسري أيضا القانون الهولندي على تجميع البيانات الذي يقع ي خارج البلاد إذا كان المسؤول عنه يقيم ي البلاد[3].

ونخلص مما سبق إلى أن التشريعات الجنائية لا تواكب حركة الاتصالات و المعلوماتية التي عمت أرجاء العالم لكونها تميل معظمها إلى الطابع الإقليمي [4]، وقد شرعت بعض الدول في عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في الجرائم المعلوماتية ، إلا أن ذلك لم يحقق تقدما في معالجة مشكلات الاختصاص وتبادل الأدلة الجنائية وتسلمين المجرمين ، بل أن الأمر في حاجة إلى قوانين جنائية أكثر مرونة تواكب مرونة التعامل بالحاسوب في مختلف المجالات، أوعلي الأقل وضع تنظيم دولي تتبناه الدول المختلفة في قوانينها لتحديد المحكمة المختصة في جرائم الانترنت [5]

.

---

[1] – راجع المادة 1957/ فقرة21 من قانون جرائم الكمبيوتر الأمريكي.

[2] – شيماء عبد الغني عطاء الله، مرجع سابق، ص279.

[3] – المرجع نفسه ، ص278.

[4] -Johannes f .nijboerm challenges for the law of Evidence Leiden: INRE,P, 1999,p,16.

[5]-Gordon huges,Essqys on computer crime-London : Longman Professional,1995,p,47

المبحث الثاني

سلطة القاضي الجنائي في تقدير الأدلة الرقمية

يشهد العالم ثورة تكنولوجيا المعلومات، قوامها المعلومات والمعرفة التي أصبحت أساسا للتنمية وزيادة الإنتاج وسرعة اتخاذ القرار الصحيح، وهو ما أدى إلى ظهور الحاسوب ذلك الجهاز الذي يتعامل مع المعلومات والمزود بقدرات بارعة ، لكن كما هو شأن كل اكتشاف أو اختراع جديد أدى استخدام الحاسوب ومن بعده الإنترنت إلى مشاكل أخلاقية وقانونية ، حيث برزت أنماط جديدة من الجرائم المعلوماتية.

وتطرح الجريمة المعلوماتية العديد من المشاكل والتحديات الموضوعية والإجرائية، ومن أهمها جمع الأدلة الجنائية واثبات هذه الجرائم ، حيث يحتاج هذا النوع من الجرائم إلى أدلة الكترونية لإثباتها بنظم المعالجة الآلية للمعطيات وأصبح الدليل الرقمي ضرورة لكشف أنماط هذه الجرائم، كما أصبح إنشاء المعامل الجنائية الرقمية مطلبا ملحا لفحص الأدلة الرقمية، وتقييم عملية الإثبات الرقمي وتحليل الجرائم في نطاق نظام الخبرة الأمنية.

وعليه سنبحث هذا المبحث من خلال ماهية الأدلة الرقمية (في المطلب الأول)، وحجية الأدلة الرقمية في(المطلب الثاني).

المطلب الأول: ماهية الأدلة الرقمية

سنبحث ماهية الأدلة الرقمية أو المسماة بالأدلة الالكترونية من خلال مفهوم الأدلة الرقمية (في الفرع الأول) (الفرع الثاني) ;الآتي :

الفرع الأول: مفهوم الأدلة الرقمية

سنعالج هذا الفرع المتعلق بمفهوم الأدلة الرقمية من خلال تعريفها وخصائصها، وأنواعها وأشكالها ، على التفصيل الآتي:

أولا- تعريف الأدلة الالكترونية وخصائصها:

1- تعريف الأدلة الالكترونية:

تعددت التعريفات التي قيلت بشان الدليل الالكتروني أو ما يسمى بالدليل الرقمي وتباينت بين التوسع والتضييق .

ويقصد بالأدلة الرقمية [1]، بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من انجاز مهمة ما[2].

وهناك من يعرفه بأنه الدليل الذي يجد أساسا ففي العالم الافتراضي ويقود إلى الجريمة[3].

هو الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا وهى مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ و تطبيق القانون[4].

كما عرفه البعض على انه معلومات يقبلها العقل والمنطق يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في الحاسوب وملحقاته وشبكات الاتصال ، ويمكن

---

[1] - وترجع تسمية الدليل الرقمي إلى شكل أرقام، و يتم تحويل هذه الأرقام عند عرضها لتكون في شكل صورة أو مستند أو تسجيل.

[2]-christen sagarlataand David j byre, the electronic paper trail: evidentiary, journal of science and technologylqz.22september 1998p.4.

[3] - عمر محمد أبوبكر يونس ، مرجع سابق، ص969.

[4]- خالد ممدوح إبراهيم ، الجرائم المعلوماتية، دار الكر الجامعي ، الإسكندرية 2009، ص 178.

استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل له علاقة بجريمة أو جان أو مجني عليه [1].

يلاحظ على هذا التعريفات أنها تقصر مفهوم الدليل الرقمي على ذلك الذي يتم استخراجه من الحاسب الآلي، ولاشك أن ذلك فيه تضييف لدائرة الأدلة الرقمية، فهي كما يمكن أن تستمد من الحاسب الآلي، فمن الممكن أن يتحصل عليها من آلة رقمية، فالهاتف وآلات التصوير وغيرها من الأجهزة التي تعتمد التقنية الرقمية في تشغيلها يمكن أن تكون مصدراً للدليل الرقمي.

بأنه الدليل المأخوذ من الكمبيوتر ، وهذا يعني أن الدليل الرقمي لا تثبت له هذه الصفة إلا إذا تم أخذه أو استـ ؛ إذا من شأن التسليم بذلك القول إن تلك المجالات المغناطيسية أو الكهربائية قبل فصلها عن مصدرها بواسطة الوسائل الفنية لا تصلح لأن توصف بالدليل الرقمي، أي أن مخرجات الآلة الرقمية لا تكون لها قيمة إثباتيه مادامت في الوسط الافتراضي الذي نشأت فيه أو بواسطته ، وهذا غير دقيق ، وهو ما يجعل التعريفات السابقة تتصف بالقصور لكونها لا تـ [2] .

[1] – محمد الأمين البشري، الأدلة الجنائية الرقمية، المجلة العربية للدراسات الأمنية والتدريب، المجلد17 العدد33 ، ص109.

[2] –عبد الناصر محمد محمود فرغلي وعبيد المسماري ، ورقة بحث مقدمة للمؤتمر العربي لعلوم الأدلة الجنائية والطب الشرعي ، الإثبات الجنائي بالنادلة الرقمية من الناحيتين القانونية والفنية (دراسة تطبيقية مقارنة ، الرياض المنعقد في الفترة 12-2007/11/14، ص13.

وعليه فإنه يمكن تعريف الدليل الرقمي بأنه معلومات مخزنة ففي أجهزة الحاسوب وملحقاتها أو متنقلة عبر شبكات ا لاتصال ، والتي يتم تجميعها وتحليلها باستخدام برامج خاصة لإثبات وقوع الجريمة ونسبتها إلى مرتكبيها [1].

2-خصائص الأدلة الالكترونية :

يتميز الدليل الالكتروني عن الدليل التقليدي بالخصائص والمميزات الآتية :

أ- دليل غير مادي:

ير ملموس ، فهو تلك المجالات المغناطيسية أو الكهربائية، ومن

الدليل، بل أن هذه العملية لا تعدو كونها عمليه نقل لتلك المجالات من طبيعتها الرقمية إلى الهيأة التي يمكن الاستدلال بها[2].

ب- دليل علمي : يعتبر الدليل الرقمي من قبيل الأدلة الفنية أو العلمية يتكون الدليل الالكترونية من بيانات ومعلومات الكترونية غير ملموسة لا تدرك بالحواس العادية بل يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسوب واستخدام نظم برمجية [3].

---

[1]- و كذلك بمكن تعريفه بأنه مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية.

[2] - علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في أطار نظرية الإثبات الجنائي، مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية ونظمته أكاديمية شرطة دبي، في الفترة من 26-28/4/-2003- دبي ص 22.

[3] - ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر ، منشور ضمن أعمال مؤتمر " الأعمال المصرفية والالكترونية " نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي ، في الفترة من 10-12/5/ 2003 ، ص37.

وبالتالي إن فهم مضمون الدليل الرقمي يعتمد على استخدام أجهزة خاصة بتجميع وتحليل محتواه ، و

يعدم قيمته التدليلية في إثبات

الجريمة ونسبها إلى الجاني[1].

إذا كان قد تعرض للعبث والتحريف.

ج- صعوبة التخلص من الدليل الالكتروني:

يتميز الدليل الرقمي بصعوبة محوه ، إذ حتى في حالة محاولة ازالة ذلك الدليل فمن الممكن إعادة إظهاره من خلال ذاكرة الآلة التي تحتوى ذلك الدليل، و كذا يمكن استرداد الملفات الملغاة، وفي المقابل هناك برمجيات يستخدمها الجناة للتخلص من الأدلة الالكترونية [2].

د-الدليل الالكتروني قابل للنسخ :

حيث يمكن استخراج نسخة من الأدلة الجنائية الالكترونية مطابقة للأصل ولها نفس القيمة العلمية ، وهذه الخاصية لاتتوافر في الأدلة التقليدية ، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الضياع والتلف والتغيير[3].

ولقد سمح المشرع الجزائري بالمادة 06 من قانون04/09 نسخ المواد المخزنة في النظام المعلوماتي في دعامة الكترونية ووضعها في أحراز وفقا للقانون.

---

[1] -عمر محمد أبو بكر يونس ، ، مرجع سابق ، ص983.

[2] - لكن محاولة الجاني محو الدليل الرقمي تسجل عليه في ذاكرة الآلة كدليل، وهو ما يمكن من استخدامه كدليل ضده للتفصيل راجع عبد الناصر محمد محمود فرغلي وعبيد المسماري ، مرجع سابق ، ص15 .

[3] - عمر محمد أبوبكر يونس ، مرجع سابق ، ص978.

وقد لاحظ أيضا المشرع البلجيكي ذلك فقام بإضافة المادة 39 من القانون المؤرخ في 28 نوفمبر 2000 التي سمحت بضبط الأدلة الرقمية، مثل نسخ المواد المخزنة في نظم المعالجة الآلية للمعطيات بقصد عرضها على الجهات القضائية [1].

هـ-الدليل الالكتروني متنوع ومتطور:

يشمل الدليل الالكتروني كافة أشكال البيانات الرقمية الممكن تداولها ، كما أنه متطور لتطور البيئة الرقمية ، ويترتب على ذلك صعوبة الوصول إليه ، نتيجة للحماية الفنية لبيانات المواقع ومن جهة أخرى صعوبة ضبط الأدلة الالكترونية ، من خلال استخدام عدة تقنيات كالتشفير [2].

ثانيا-أنواع الأدلة الالكترونية وأشكالها:

سنتناول أنواع الدليل الرقمي، وأشكاله على النحو الآتي:

1 - أنواع الأدلة الالكترونية :

يمكن تقسيم الأدلة الالكترونية، من حيث وجود الدليل وكوسيلة إثبات ، إلى التقسيمات الآتية[3]:

أ- من حيث مصدرها:

لقد حاول فريق من الفقهاء تقسيم الأدلة الالكترونية من حيث مصدرها إلى :الأدلة الالكترونية الخاصة بأجهزة الكمبيوتر وشبكاتها ، الأدلة الالكترونية الخاصة بالانترنت ، الأدلة الالكترونية الخاصة ببرتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات، الأدلة الالكترونية الخاصة بالشبكة العالمية للمعلومات.

ويلاحظ أن هذا التقسيم يتطابق تماما مع التقسيم الفقهي للجريمة المعلوماتية والتي تقسم إلى جرائم الكمبيوتر ، وجرائم الشبكة العالمية ، وجرائم الانترنت ، وجرائم باستخدام الكمبيوتر [1].

---

[1] - خالد ممدوح إبراهيم، مرجع سابق ، ص184.

2-المرجع نفسه ، 185

[3] - ممدوح عبد اللطيف ، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر الانترنت، مرجع سابق ، ص18.

ويلاحظ أيضا على هذه التقسيمات أنها تدور حول موضوع واحد، ألا وهو الدليل الالكتروني الخاص بجهاز الكمبيوتر وشبكاته، فهي ميزت بين شبكات الكمبيوتر والانترنت وبرتوكولات تبادل المعلومات والشبكة العالمية للمعلومات التي هي في الأصل واحد ، فالاختلاف هنا في التسمية لا في المسمى والمعنى [2].

ب- من حيث الإثبات:

قسم الفقه الأدلة الرقمية من حيث الإثبات الى : أدلة رقمية معدة كوسيلة إثبات، وأدلة غير معدة كوسيلة إثبات، على النحو الآتي :

- أدلة رقمية معدة كوسيلة إثبات:

وهذا النوع من الأدلة الرقمية المعدة للإثبات يمكن إجمالها فيما يلي:

-

يساهم الإنسان في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي[3].

-السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الآلة ومن أمثلة ذلك خاص، كإجراء العمليات

الحسابية على تلك البيانات.

- أدلة رقمية غير معدة كوسيلة إثبات:

وهذا النوع من الأدلة الرقمية نشأ دون إرادة الشخص، أي أنها أثر يتركه الجاني دون أن

---

[1] - عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي (دراسة مقارنة بين التشريع الجزائري والقانون المقارن)، دار الجامعة الجديدة ، الإسكندرية ، 2010، ص73.

[2] -خالد ممدوح إبراهيم، مرجع سابق، ص2.

[3] - ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، مرجع سابق ، ص38.

بالآثار المعلوماتية الرقمية[1]، وهى تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافه الاتصالات التي تمت من خلال الآلة أو شبكة الانترنت[2].

غير أن الوسائل

الفنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من نشوئها، فالاتصالات التي تجرى عبر الانترنت والمراسلات الصادر عن الشخص أو التي يتلقاها، كلها يمكن ضبطها بواسطة تقنية خاصة بذلك.

وتبدو أهمية التمييز بين هذين النوعين، فيما يلي:

–

دليلاً على الوقائع التي يتضمنها، في حين يكون الحصول علي النوع الثاني من الأدلة بإتباع تقنية خاصة لا تخلو من صعوبة وتعقيد.

– أن النوع الثاني

.

–

لاحقاً وهو ما يقلل من إمكانية فقدانه، و

عرض للفقدان لأسباب منها فصل التيار الكهربائي عن الجهاز مثلاً .

---

[1] – المرجع نفسه ، ص39.

[2] –حيث يتم الاعتماد في ضبط هذا النوع من الأدلة على ما يعرف ببروتوكول IP مستخدم الشبكة تحدي الجهاز الذي يستعمله من خلال بيانات الجهاز عند مزود الخدمة ، راجع في ذلك عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية ففي جرائم الكمبيوتر والانترنت، مرجع سابق ، ص63–64.

2 -أشكال الدليل الرقمي:

يتخذ الدليل الرقمي ثلاثة أشكال رئيسة: هي الصور الرقمية، والتسجيلات والنصوص المكتوبة [1]

أ -الصور الرقمية:

وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفى العادة تقدم الصورة إما في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية ، والواقع أن الصورة الرقمية تمثل تكنولوجيا بديلة للصورة الفوتوغرافية التقليدية وهي [2].

ب -التسجيلات الصوتية:

وهى التسجيلات التي يتم ضبط وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات الصوتية على الانترنت ،والهاتف وغيرها من التسجيلات الصوتية .

ج - النصوص المكتوبة:

وتشمل النصوص المكتوبة بواسطة الحاسوب الآلي، ومنها الرسائل عبر البريد الالكتروني، ولقد قبل القضاء الأمريكي بسجلات الحاسوب المكتوبة كدليل الكتروني ويسميها سجلات الحاسوب المخزنة (computer stored records) وهي التي تشير إلى الوثائق التي تحتوي عل كتابات(writings)[3].

---

[1] _ إن الأدلة الإلكترونية ، إما أن تكون مخرجات ورقية يتم إنتاجها عن طريق الطابعات ، أو الراسم ، أو مخرجات غير ورقية ، كالأشرطة والأقراص الممغنطة وأسطوانات الفيديو وغيرها من الأشكال الإلكترونية غير التقليدية، أو تتمثل في عرض مخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به ، أو الإنترنت بواسطة الشاشات أو وحدة العرض.

[2] - ممدوح عبد المطلب، أدلة الصور الرقمية في الجرائم عبر الكمبيوتر، مركز شرطة دبي، 2005، ص109-110.

[3] - عائشة بن قارة مصطفى، مرجع سابق، ص74-75.

الفرع الثاني : شروط قبول الأدلة الإلكترونية

إذا كانت الأدلة المحصلة من الوسائل الإلكترونية قد توجس منها كل من القضاء والفقه خيفة من عدم تعبيرها عن الحقيقة نظرا لما يمكن أن تخضع له طرق الحصول عليها من التعرض للتزييف والتحريف والأخطاء المتعددة، فإنه لذلك تطلب الأمر توافر شروط تضفي عليها المصداقية ، ومجموعة إجراءات لجمع هذه الأدلة ، على النحو الآتي :

أولا- شروط قبول الأدلة الإلكترونية في الإثبات الجنائي :

لقبول هذه الأدلة الالكترونية كأساس تبنى عليه الحقيقة كأدلة إثبات في المواد الجنائية[1]، فيلزم أن تتوافر فيها الشروط الآتية:

1- وجوب أن تكون هذه الأدلة يقينية :

الحكم بالإدانة ، ذلك أنه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين، ويمكن التوصل إلى ذلك من خلال ما يعرض على القاضي من الأدلة الإلكترونية، والمصغرات الفيلمية، وغيرها من الأشكال الإلكترونية.

وهكذا يستطيع القاضي من خلال ما يعرض عليه من مخرجات إلكترونية، أن يحدد قوتها الاستدلالية، أي قيمة ما يتمتع به الدليل الالكتروني من قوة استدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص أو كذبه[2].

ويشترط قانون البوليس والإثبات في بريطانيا لسنة 1984 ، حتى تتحقق يقينية الأدلة الإلكترونية أن تكون البيانات دقيقة وناتجة عن الحاسوب بصورة سليمة.

---

[1]- -Rodrigues(A),le droit portugais, la preuve en procédure pénal comparé comparée, association internationale de droit pénal R,I,D,p.1992,p206ets.

[2]-Ali Ahmed rached : « De l'intime conviction du juge vers une théorie scientifique de la preuve en matière criminelle, éd. Pedone, Paris 1942, p. 3.

أما في كندا فإن الرأي السائد في الفقه هو اعتبار مخرجات الحاسوب من أفضل الأدلة ، لذا فإنها تحقق اليقين المنشود في الأحكام الجنائية[1].

وتنص القواعد الفيدرالية الأمريكية على أن الشرط الأساسي للتوثيق أو التحقق من صحة أو صدق الدليل كشرط مسبق لقبوله هو أن يفي بأمارة أو بينة كافية تدعم الوصول إلى الأمور التي تتصل بالموضوع بما يؤيد الادعاءات[2].

ويقرر الفقه الياباني قبول الأدلة المستخرجة من الحاسوب التي تم تحويلها إلى الصورة المرئية سواء كانت هي الأ ه الاستثناءات المنصوص عليها في المادة 323 من قانون الإجراءات الجنائية الياباني ، ففي هذه الحالة يتحقق اليقين الذي يبنى عليه الحكم الجنائي، كما يمكن أن يتحقق اليقين لهذه المخرجات من خلال التقارير الخبراء.

وفي تشيلي ينص القانون الخاص بالحاسوب على قبول السجلات الممغنطة للحاسوب وكذلك النسخ الناتجة عنها، ومعنى ذلك أن هذه السجلات وصورها تحقق اليقين المنشود لإصدار الأحكام الجنائية، في هذا المجال (المادة 221 من قانون أصول المحاكمات الجزائية التشيلي)[3].

---

[1]–هلالي عبد الله أحمد، "حجية المخرجات الكمبيوترية في المواد الجنائية"، دراسة مقارنة، دار النهضة العربية،1997 ص95.

[2] _

أفضل الأدلة المتاحة لإثبات هذه البيانات وبالتالي يتحقق مبدأ اليقين لهذه الأدلة . راجع علي حسن الطوالبة، مرجع سابق ، ص191 .

[3] – سعيد عبد اللطيف حسن، "إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت"، الجرائم الواقعة في مجال تكنولوجيا المعلومات، دار النهضة العربية، القاهرة، ط1، 1999، ص15.

واعتبر المشرع الأردني نظام المعالجة الإلكترونية
المحقق ضبط الدليل الإلكتروني من خلال المادة 21 من قانون المعاملات الإلكترونية رقم (85) لسنة 2001 ، الذي يعطي إمكانية إثبات الحق
تفتيش نظم الحاسوب والإنترنت[1].

وبالتالي تخضع الأدلة الإلكترونية بمختل أنواعها لتقدير القاضي الجنائي ويجب أن يستنتج منها الحقيقة بما يتفق مع اليقين ويبتعد عن الشك والاحتمال [2].

2 – وجوب مناقشة الأدلة الإلكترونية تطبيقا لمبدأ شفوية المرافعة:

ويعني مبدأ وجوب مناقشة الدليل الجنائي بصفة عامة أن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى، وهذا يعني أن الأدلة المتحصلة من جرائم الحاسوب والإنترنت سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسوب ، أم كانت بيانات مدرجة في حاملات البيانات ، أم اتخذت

الأخذ بها كأدلة إثبات أمام المحكمة[3].

وعليه فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات يجب أن يعرض في الجلسة ليس من خلال ملف الدعوى في التحقيق الابتدائي لكن بصفة مباشرة أمام القاضي ،

---

[1] – علي حسن الطوالبة، مرجع سابق ، ص192

[2] – والقاضي يمكنه أن يصل إلى يقينية الأدلة الالكترونية المتقدم ذكرها عن طريق المعرفة الحسية التي تدركها الحواس من خلال معاينته لهذه المخرجات وفحصها، وعن طريق المعرفة العقلية عن طريق ما يقوم به من استقراء واستنتاج ليصل إلى الحقيقة التي يهدف إليها ويجب أن يصدر حكمه استنادا إليه . للتفصيل راجع هلالي عبد الله أحمد، "حجية المخرجات الكمبيوترية في المواد الجنائية"، مرجع سابق، ص96. وانظر أيضا

Gorphe François : « Les décisions de justice », étude psychologique et judiciaire, Paris, : Sirey, Presses universitaires de France, 1952, p. 123.

[3] – علي حسن الطوالبة، مرجع سابق ، ص193– وانظر هلالي عبد اللاه أحمد، "حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص102.

وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحاسبات الحواسيب[1]، وقد حرصت بعض التشريعات الإجرائية ، كالتشريع الفرنسي الذي نص على هذا الشرط في المادة2/427 [2].

ومن القواعد العامة المستقرة في القانون الجنائي عدم قبول البينة السماعية أمام المحاكم الجنائية، إلا في حالات استثنائية حصرها القانون بشروط مشددة، ويرجع عدم قبول البينة السماعية إلى استحالة استجواب ومناقشة الشاهد الأصلي بواسطة المحكمة والدفاع ولاستثناءات البينة السماعية علاقة بمناقشة حجية الأدلة الجنائية الإلكترونية ، وعلى سبيل المثال لقد تضمنت القواعد الفيدرالية

المحفوظة في أي شكل ، وكذلك الوقائع والأحداث والآراء ونتائج التحاليل المنقولة بواسطة

لكونها بيانات أكثر دقة ومحفوظة بأسلوب علمي يختلف عن غيرها من الأدلة السماعية ، والأدلة الجنائية الإلكترونية من هذا القبيل لكونها معدة بعمليات حسابية دقيقة[3].

ويترتب على مناقشة أدلة الحاسوب والإنترنت النتائج عدم جواز أن يقضي القاضي في الجرائم معلوماته الشخصية، و ضرورة التأهيل التقني والفني للقضاة لمواكبة المناقشة العلمية لأدلة الحاسوب والإنترنت بشكل يتماشى مع التقارير المؤتمرات الخاصة بجرائم الحاسوب[4].

---

[1] – علوماتية الذين يكون قد سبق أن سمعت أقوالهم في التحقيق الابتدائي ، فإنه يجب أن يعيدوا أقوالهم مرة أخرى من جديد أمام المحكمة، كذلك فإن خبراء الأنظمة المعلوماتية على اختلاف تخصصاتهم، ينبغي أن يمثلوا أمام المحاكم لمناقشتهم، أو مناقشة تقاريرهم التي خلصوا إليها .

[2]– هلالي عبد اللاه أحمد، "حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص104–105.

[3] – محمد الأمين البشري، الأدلة الجنائية الرقمية، مرجع سابق ، ص128–129.

[4] – هلالي عبد اللاه أحمد، "حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص 110وما بعدها.

3 – مشروعية الأدلة الالكترونية :

إن أهم هدف للدستور هو صيانة كرامة الإنسان وحماية حقوقه لذلك تتضمن الدساتير الحديثة وهذه

النصوص الواردة في الدستور تفرض على المشرع عند وضع قواعد الإجراءات الجنائية الالتزام بها وعدم الخروج عنها ، وكذلك فإن إجراءات الحصول على الأدلة الجنائية يجب أن تكون ضمن العام [1].

تم الحصول عليه عن طريق مخالفة القانون ، و

هو الدليل الوحيد فلا يصح الاستناد عليه في إدانة المتهم ، فإذ ما شاب التفتيش الواقع على نظم الحاسوب عيب فإنه يبطله ، والتفتيش الذي يقوم به المحقق بغير الشروط التي نص عليها القانون [2].

وفي إطار مشروعية الأدلة الإلكترونية ، نجد أن القانون الفرنسي رغم أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة ، إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية ، أم في جرائم الحاسوب والإنترنت[3].

ويشير رأي فقهي فرنسي إلى أن القضاء قد قبل استخدام الوسائل العلمية الحديثة في البحث والتنقيب عن الجرائم تحت تحفظ أن يتم الحصول على الأدلة الجنائية ، ومن بينها الأدلة المتحصلة من الحاسوب والإنترنت ، بطريقة شرعية ونزيهة ، وكذلك في سويسرا وبلجيكا[4].

---

[1] – ويعتبر البطلان من النظام العام ، ويجوز لكل ذي مصلحة التمسك به كما أن للمحكمة أن تقضي به من تلقاء نفسها راجع علي محمد طوالبة ، مرجع سابق ، ص184-185.

[2] – هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص119.

[3] - Chevallier Jean Yves : «Rapport de Synthèse pour les pays d'Europe Continentale, la preuve en procédure en pénale comparé», Association internationale de droit pénal, R.I.D.P, 1992, p..51

[4] – هلالي عبد اللاه أحمد، "حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص121.

ولقد تضمن قانون الشرطة والإثبات الجنائي الإنكليزي لعام 1984 ، بموجب المادة 69 شروط قبول مخرجات الحاسوب أمام القضاء ، وهي كالآتي[1]:

- يجب ألا يوجد أساس معقول للاعتقاد أن البيان الخاطئ أو غير دقيق ، بسبب الاستعمال الخاطئ ، أي الاستعمال غير الملائم للظروف أو للغرض.

- يجب أن تكون جميع المكونات المادية للحاسوب كانت تعمل بدقة و متوافق .

أما بالنسبة للتشريع الجزائري فتضمن بعض الضمانات التي يجب الالتزام بها أثناء البحث عن الدليل الرقمي في الجرائم المعلوماتية بشكل يضمن حقوق المتهم وحرياته، وبالتالي الحفاظ على مشروعية الدليل المستمد في هذه الجرائم.

إذ استلزمت المادة 45 من قانون الإجراءات الجنائية الجزائري ، على ضرورة أن تتم عمليات التفتيش بحضور صاحب المسكن [2]، غير أنه يجب عند تفتيش أماكن يشغلها ملزم قانونا بكتمان السر المهني أن تتخذ مقدما جميع التدابير اللازمة لضمان احترام ذلك السر، وكذا جرد الأشياء المستندات المحجوزة.

لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات باستثناء الأحكام المتعلقة بالحفاظ على السر المهني و كذا جرد الأشياء و حجز المستندات المذكورة أعلاه .

كما استوجبت المادة 47 من قانون الإجراءات الجنائية بأنه لا يجوز البدء في تفتيش المساكن و معاينتها قبل الساعة الخامسة (5) صباحا، و لا بعد الساعة الثامنة (8) مساء غلا إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل أو في الأحول الاستثنائية المقررة قانونا.

---

[1] – علي محمد طوالبة ، مرجع سابق ، ص190.

[2] – تنص للمادة 45 من قانون الإجراءات الجنائية ، على أنه إذا تعذر حضور صاحب المسكن وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له. و إذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته.

لكن عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبييض الأموال و الإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش و المعاينة و الحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل و ذلك بناء على إذن مسبق من وكيل الجمهورية المختص [1].

4- وجوب خضوعها لتقدير المحكمة.

لقد تضمن قانون الشرطة والإثبات الجنائي الإنكليزي لعام 1984 توجيهات في كيفية تقدير قيمة البيان المستخرج عن طريق الحاسوب طبقا للمادة 11، حيث أوصت بمراعاة كل الظروف 69، وبوجه خاص
مراعاة المعلومات المعاصرة، أي ما إذا كانت المعلومات المتعلقة بأمر قد تم تزويد الحاسوب بها في وقت معاصر لهذا الأمر أم لا ، وكذلك مسألة ما إذا كان أي شخص من المتصلين على أي نحو بإخراج البيانات من الحاسوب لديه دافع لإخفاء الوقائع [2].

أما في هولندا استبعد التشريع الهولندي الأدلة غير القانونية ، فإذا كانت بيانات الحاسوب المسجلة في ملفات الشرطة غير قانونية ، فذلك يؤدي إلى نتيجة مؤداها ضرورة محو هذه البيانات

---

[1] -عندما يتعلق الأمر بالجرائم المذكورة في الفقرة الثالثة أعلاه، يمكن قاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا و في أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك.

[2] – ولقد قضت محكمة الاستئناف في إنكلترا بذلك ، حيث بينت في حكمها كيفية التعامل مع الأدلة المستخرجة من الحاسوب ، ويتلخص الحكم بما يلي: (أنه يبدو لهذه المحكمة – أنه من الخاطئ رفض أو إنكار أية مزايا أو صلاحيات

التسجيل ، حيث يمكن التثبت من ذلك وكذلك يمكن التعرف بوضوح على الأصوات المسجلة والمستخلص الدليل وثيق الصلة بالموضوع ، للتفصيل راجع علي محمد طوالبة ، مرجع سابق ، ص189.

وعدم إمكانية استخدامها كدليل جنائي بسبب مبدأ استبعاد الأدلة غير القانونية[1]، أما في اليابان فقد أصدرت محكمة مقاطعة (KOFV) حكما أقرت فيه مشروعية التصنت للبحث عن الدليل، حيث أن .[2]

ومن أمثلة الطرق غير المشروعة التي يمكن أن تستخدم في الحصول على الأدلة الناتجة عن الجرائم المعلوماتية ، الإكراه المادي والمعنوي في مواجهة المتهم المعلوماتي من أجل فك شفرة نظام من النظم المعلوماتية أو الوصول إلى دائرة حل التشفير أو الوصول إلى ملفات البيانات المخزنة ، واستخدام التدليس أو الغش أو الخداع في الحصول على الأدلة الإلكترونية [3].

ولقد صادقت لجنة الوزراء التابعة للمجلس الأوروبي في 1981/1/2 على اتفاقية خاصة بحماية البيانات ذات الطبيعة الشخصية، ونصت على ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ودقيقة، ومستمدة بطرق مشروعة،
في غير الأغراض المخصصة لها ، وحق الشخص المعني في التعرف والإطلاع على البيانات المسجلة المتعلقة به وتصحيحها وتعديلها ومناقضتها ومحوها إذا كانت باطلة[4].

---

[1] –أسامة عبد الله قايد ، مرجع ، ص93.

[2] – لكن الفقه الياباني يستبعد الأدلة الجنائية غير المشروعة ، سواء كانت تقليدية أم أدلة حاسوب أو . راجع هلالي عبد اللاه أحمد، "حجية المخرجات الكمبيوترية في المواد الجنائية، مرجع سابق، ص37

[3] – وكذلك التحريض على ارتكاب الجريمة المعلوماتية من قبل أعضاء الضابطة العدلية ، كالتحريض على الغش أو . راجع جميل عبد الباقي ، أدلة
الإثبات الجنائي والتكنولوجيا الحديثة ، مرجع سابق ، ص111.

[4] –حسن طوالبة ، مرجع سابق ، ص189.

ثانيا_ إجراءات جمع الأدلة الكترونية:

نظمت التشريعات كيفية استنباط الدليل عن طريق إجراءات تتبع وصولا الى هذه الغاية ، وأهم هذه الإجراءات المعاينة والتفتيش والضبط و وندب الخبراء.

لكن نظرا لعجز وسائل التحري والتحقيق الكلاسيكية عن مواجهة الجرائم الحديثة وخاصة جرائم الانترنت استحدثت التشريعات المقارنة وسائل تحري وتحقيق حديثة من أهمها إجراء واعتراض المراسلات والاتصالات، والتسرب والمراقبة الالكترونية

وكذلك تبنى المشرع الجزائري التسرب، واعتراض المراسلات وتسجيل الأصوات والتقاط الصور بموجب القانون 22/06 المؤرخ في 22 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجنائية الجزائري ، وكذا المراقبة الالكترونية في قانون 09-04 المتعلق بالوقاية من جرائم الاتصال والمعلومات ومكافحتها على التفصيل الآتي :

1-اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

استحدث المشرع الجزائري هذه الإجراءات في قانون الإجراءات الجزائية بموجب التعديل 22/06 المؤرخ في 20 ديسمبر 2006 في الفصل الرابع من المادة 65 مكرر5 إلى 65 مكرر10 من قانون الإجراءات الجنائية الجزائري [1].

أ-شروط اعتراض المراسلات:

لم يعرف المشرع الجزائري اعتراض المراسلات والتقاط الصور وتسجيل الأصوات في المواد المادة 65 مكرر5 إلى 65 مكرر10 من قانون الإجراءات الجنائية [1] .

1- قانون 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر 66- 155المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجنائية، ج.ر. عدد صادرة في 2006 .

يستوجب قانون الإجراءات الجزائية شروط تتمثل في الإذن القضائي ، ومحضر العمليات والقيام بها بواسطة ضابط الشرطة القضائية المأذون له أو المناب ، كالآتي :

-الإذن المكتوب:

وفقا للمادة 65 مكرر5 من ق .ا.ج ، يأذن بهذه الإجراءات وكيل الجمهورية عندما تقتضي ذلك ضرورات البحث و التحري ، وفي حالة فتح تحقيق قضائي
إذن من قاضي التحقيق وتحت مراقبته المباشرة [2] .

ويشترط فيه بموجب المادتين 65 مكرر5، 7 الإذن بهذه الإجراءات عند توافر السبب ، وهو أن تقتضي ذلك ضرورات البحث والتحقيق [3] ، وكذلك الإذن بإجراءات الاعتراض في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو جرائم الصرف أو جرائم الفساد [4] .

كذلك يشترط في الإذن أن يتضمن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن السكنية المقصودة أو غيرها، والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها وأن يكون مكتوبا تحت طائلة البطلان لأن الأصل في العمل الإجرائي الكتابة ، وأيضا أن يسلم لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية [5].

---

[1]-عرف القانون الأمريكي في المادة 04 اعتراض الاتصالات بأنه اكتساب سماعي أو غيره لمحتوى أية اتصالات سلكية .

[2]– انظر عبد الله هلالي, تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ص138.

[3]- راجع المادة 65 مكرر 5 من قانون الإجراءات الجنائية

[4]- راجع المادة 65 مكرر 5 من قانون الإجراءات الجنائية

[5] - يشترط أيضا وفقا للقواعد العامة أن يكون مصدره مختصا نوعيا ومكانيا أصلا بالبحث أو التحقيق في الجريمة التي صدر الإذن بشأنها، ووفقا للقواعد العامة يتحدد الاختصاص النوعي بحسب نوعية الجريمة أما الاختصاص المكاني بمحل

- **محضر العمليات :**

استوجب المشرع الجزائري في المادة 65 مكرر9على ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص ، أن يحرر محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري، ويذكر بالمحضر أيضا بتاريخ وساعة بداية هذه العمليات والانتهاء منها [1].

كما أوجب عليه في المادة 65 مكرر 10وصف أو نسخ المراسلات والصور أو المحادثات المسجلة والمفيدة في إظهار الحقيقة كمرفقات تودع بالملف، وتنسخ وتترجم المكالمات التي تتم باللغة الأجنبية عند الاقتضاء بمساعدة مترجم يسخر لهذا الغرض.

- **صفة القائم بالعمليات :**

وفقا للمواد 65 مكرر8 ،9، 10 من قانون الإجراءات الجنائية [2]، يقوم بعمليات الاعتراض والالتقاط والتسجيل ضابط الشرطة القضائية المأذون له أو المناب ، ويجوز لوكيل الجمهورية أو ضابط الشرطة القضائية المناب أن يسخر كل عون مؤهل لدى مصلحة أو وحدة عمومية أو

الواقعة، أو ضبط المتهم، أو محل إقامته [5]. راجع عبدا لله أوهابية , شرح قانون الإجراءات الجزئية الجزائري (التحري والتحقيق) ، دار هومة ، الجزائر, 2004، ص. 213.

[1]– طبقا للمادة 214 ق. إ.ج .لايكون لهذه المحاضر قوة في الإثبات إلا إذا كانت صحيحة في الشكل, والأدلة الواردة بها طبقا للمادة 215 مجرد استدلالات ملم ينص القانون على خلاف ذلك .

[2] –راجع المواد 65 مكرر 8.9.10 من قانون الإجراءات الجنائية .

خاصة مكلفة بالمواصلات السلكية أو اللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65 مكرر 5 [1].

ب- سلطات الضبطية القضائية والرقابة على عملها :

رأينا أن المشرع الجزائري أجاز لوكيل الجمهورية أو قاضي التحقيق أن يأذن بهذا الإجراء لضابط الشرطة القضائية وتحت رقابته ، عندما تقتضي ضرورات التحري والتحقيق في إحدى الجرائم المذكورة في المادة65 مكرر 5 لاسيما الجرائم المعلوماتية ، على التفصيل الآتي :

-صلاحيات واسعة للضبطية القضائية :

في إطار مكافحة الجرائم المعلوماتية منح المشرع الجزائري في المواد 65 8 ،9 ،10 مكرر من قانون العقوبات [2]، ضابط الشرطة القضائية المأذون له أو المناب ، القيام بعمليات الاعتراض والالتقاط والتسجيل ، وفي سبيل القيام بهذه العمليات منحه سلطات واسعة من النواحي آلاتية :

-سمح المشرع لضابط الشرطة القضائية بوضع الترتيبات التقنية دون موافقة المعنيين ، من اجل التقاط و تثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية [3] .

---

[1]- وتجدر الإشارة إلى انه يترتب على تخلف احد شروط عمليات الاعتراض والالتقاط والتسجيل بطلان الإجراء وعدم الاعتماد بما قد يتمخض عنه من دليل جنائي . راجع سليمان عبدا المنعم ،أصول الإجراءات الجنائية (دراسة مقارنة) منشورات الحلبي الحقوقية ,لبنان ، 2003 ص876

[2]- راجع المواد 65 8 ،9 ،10 مكرر من قانون العقوبات

[3] - وبالتالي سمح المشرع الجزائري بتسجيل الأصوات في أماكن عمومية أو خاصة، بينما قصر التقاط الصور في الأماكن الخاصة. على خلاف المشرع الفرنسي الذي أورد استثناءات في المواد 706 من قانون الإجراءات الجنائية بحيث لايمكن الدخول بأي شكل من الأشكال إلى :

-الاماكن التي تحتوي عل مؤسسات إعلامية

-الأماكن ذات الطابع المهني للأطباء والموثقين والمحضرين

- سيارات النواب والمحامين

– يجوز لضابط الشرطة القضائية باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية أو اللاسلكية ، وبالتالي سمح له المشرع بتلقى أي مراسلة مهما كان نوعها مكتوبة أو مسموعة ، وبغض النظر عن وسيلة ارسالها وتلقيها عن طريق وسائل الاتصال السلكية أو اللاسلكية [1].

– يسمح الإذن المسلم لضابط الشرطة القضائية بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون [2]، وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن. وبالتالي هذه العمليات تجرى دون علم أو موافقة أصحاب الاماكن ، وفي أي وقت .

–يسلم الإذن لضابط الشرطة القضائية لمدة أقصاها أربعة (4)أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ، وبا
التحقيق ، فكلما اقتضى الأمر تجديدها تستمر تلك العمليات .

–يجوز ضابط الشرطة القضائية المناب أن يسخر كل عون مؤهل لدى مصلحة أو وحدة عمومية أو خاصة مكلفة بالمواصلات السلكية أو اللاسلكية للتكفل بالجوانب التقنية لتلك العمليات.

وعلى الرغم من هذه السلطات الكبيرة لضابط الشرطة القضائية المأذون له أو المناب في سبيل إنجاح عمليات الاعتراض والتقاط والتسجيل كأساليب لمكافحة الجريمة المعلوماتية ، غير أن هذه

---

[1] – عبد المجيد جباري ، دراسات قانونية في المادة الجزائية ، دار هومة ، الجزائر 2012 ، ص.62.

[2] – تنص المادة 3/47 من قانون الإجراءات الجنائية ، عندما يتعلق الأمر بالجرائم المعلوماتية فانه يجوز إجراء التفتيش والمعينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص
ويمكن قاضي التحقيق أيضا ف ي مرحلة التحقيق الابتدائي ، عندما يتعلق الأمر بالجرائم المذكورة في الفقرة الثالثة أعلاه، أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا و في أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك

العمليات يراعى فيها عدم المساس بالسر المهني المنصوص عليه في المادة 45 من قانون الإجراءات الجنائية .

-الرقابة القضائية على عمل الضبطية القضائية:

نظرا للصلاحيات الواسعة في عمليات الاعتراض والالتقاط والتسجيل، أخضع القانون عمل الضبطية القضائية للرقابة القضائية، حفاظا على حقوق وحريات الأفراد ومبدأ المشروعية وبناءا على المادة 65 مكرر4،5 من ق .ا.ج ، تنفذ العمليات المأذون بها تحت المراقبة المباشرة لوكيل الجمهورية المختص ، أو تحت الرقابة المباشرة للقاضي التحقيق في حالة فتح تحقيق ابتدائي .

ويراقب القضاء العمليات المأذون بها رقابة المشروعية، أي مراقبة مدى مطابقة عمليات الاعتراض والالتقاط والتسجيل للقانون، كوجوب حصول ضابط الشرطة القضائية على إذن، وعدم تجاوزه مدة الإذن وعدم المساس بالسر المهني, وغيرها من الجوانب الهامة

كما يراقب القضاء تلك العمليات رقابة موضوعية، من خلال تقدير مدى قيمة وكفاية أدلة الإثبات الموجودة في محاضر الضبطية القضائية [1].

2- التسرب :

سمح المشرع الجزائري أيضا بإجراء التسرب في الجريمة المعلوماتية في المواد 65 مكرر11-65 مكرر18 من قانون الإجراءات الجنائية ، كما نص عليه في **المادة 56** من **القانون رقم 01/06** المتعلق بالوقاية من الفساد ومكافحته.

---

[1] – وبالتالي يقتصر دور القضاء على الجوانب القانونية والموضوعية، بينما تعود الرقابة التقنية لضباط الشرطة القضائية أو الأعوان المسخرين لهذا الغرض، باعتبارهم أكثر معرفة و دراية بتقنيات التحري والتحقيق .

أ-مفهوم التسرب وشروطه :

-مفهوم التسرب :

عرف المشرع الجزائري التسرب في المادة 65 مكرر 12 بأنه قيام ضابط أو عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك معهم أو كخاف [1].

يمارس ضابط أو عون شرطة قضائية عملية التسرب نصت تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية ، في صورة فاعل أو شريك لهم [2]، أو كخاف بإيهام مرتكبي الجرائم السالفة الذكر بأنه واحد منهم وذلك من خلال إخفائه للأشياء التي تتم عملية اختلاسها أو تبديدها أو .

-شروط التسرب :

يستوجب قانون الإجراءات الجزائية في التسرب : الإذن المكتوب ، وتقرير عملية التسرب الجهة القائمة بالتسرب ، على النحو الآتي:

***الإذن المكتوب :**

يشترط المشرع الجزائري في المادة 65 مكرر11 أن يصدر الإذن بإجراء التسرب من طرف وكيل الجمهورية، أو قاضي التحقيق وتحت مراقبته المباشرة، بعدإخطار وكيل الجمهورية [3] .

كما يشترط القانون بالمواد 65 مكرر 15 من ق .إ.ج في الإذن : أن يكون مكتوبا تحت طائلة البطلان ، ذلك أن الأصل في العمل الإجرائي الكتابة ، كذلك يجب أن يكون الإذن مسببا

---

[1]- راجع المادة 65 مكرر 12 من قانون رقم 06-22المؤرخ في 20 ديسمبر 2006المعدل والمتمم للأمر 66-155المتعلق بقانون الإجراءات الجنائية ، ج. ر عدد84 صادرة في 24 ديسمبر2006.

[2]- راجع تعريف الشريك والفاعل المواد 41 و 42 من قانون العقوبات الجزائري.

[3]- راجع المادة 65 مكرر11 من قانون الإجراءات الجنائية الجزائري.

إذ يعتبر التسبيب أساس العمل القضائي، ومن ثم كان لزاما إظهار الأدلة القانونية والموضوعية بعد تقدير جميع العناصر المعروضة عليه من طرف ضابط الشرطة القضائية ، كذا يستلزم المشرع أن يسلم لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري، أو التحقيق ضمن نفس الشروط الشكلية والزمنية [1] .

***تقرير عملية التسرب :**

استوجب المشرع الجزائري في المادة 65 مكرر13 ، على ضابط الشرطة القضائية المكلف بتنسيق العملية أن يحرر تقريرا [2]، يتضمن كل العناصر الضرورية لمعاينة الجرائم غير تلك التي تعرض للخطر أمن الضابط أو العون المتسرب، والأشخاص المسخرين طبقا للمادة 65 مكرر14 من قانون الإجراءات الجنائية الجزائري [3] .

*** الجهة المختصة بالقيام بعملية التسرب :**

وفقا للمادة 65 مكرر 12 يقوم بعملية التسرب ضابط الشرطة القضائية أو عون الشرطة القضائية تحت مسؤولية الضابط المكلف بتنسيق العملية، كما يقوم بها الأشخاص المسخرين لهذا الغرض من قبل ضابط الشرطة القضائية المكلف بتنسيق العملية المادة 65 مكرر 14 .

---

[1] –طبقا للمادة 65 مكرر 15 من قانون الإجراءات الجنائية الجزائري يجوز أيضا للقاضي الذي رخص بإجراء التسرب أن يأمر بوقفه قبل انقضاء المدة المحددة ، ويجب أيضا أن تذكر في الإذن الجريمة ، وهوية ضابط الشرطة القضائية كما يجب أن تودع الرخصة في ملف الإجراءات .

[2] –ولا يكون لهذه المحاضر قوة في الإثبات إلا إذا كانت صحيحة في الشكل طبقا للمادة214 ، ولا تعتبر المحاضر والتقارير المثبة للجنايات أو الجنح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك وفقا للمادة 215، على خلاف الأدلة الواردة بالمحاضر المنصوص عليها بالمادة 216 من قانون الإجراءات الجنائية فلها حجيتها مالم يدحضها دليل عكسي بالكتابة أو شهادة الشهود . راجع مروك نصر الدين ، المرجع السابق، ص 877.

[3] – راجع المادة 65 مكرر14 ، والمادة 65 مكرر14 من قانون الإجراءات الجنائية .

ب-سلطات المتسرب وحمايتة القانونية :

في إطار تدعيم دور الضبطية القضائية في مكافحة الجرائم المعلوماتية، منح المشرع الجزائري سلطات لضباط أو أعوان الشرطة القضائية المكلفين بالتسرب تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية ، كما ووفر لهم حماية قانونية ، على التفصيل الآتي :

- سلطات المتسرب:

قرر قانون الإجراءات الجزائية لضابط أو عون الشرطة القضائية تحت مسؤولية الضابط المكلف بالتسرب ، سلطات خلال عملية التسرب ، وبعد وقفها أو انقضائها ، كالآتي :

*** سلطات المتسرب خلال سريان عملية التسرب :**

قررت المادة 65 مكرر 12 لضابط أو عون الشرطة القضائية المتسرب السلطات الآتية:

ـ استعمال هوية مستعارة وعدم إظهار هويته الحقيقية بقصد حمايته، بحيث عاقب المشرع الجزائري في المادة 65 مكرر 16 من قانون الإجراءات الجنائية كل من يكشف هويته المتسرب بالحبس من سنتين إلى خمسة سنوات وبغرامة مالية من 000 50 إلى000 200 دج كل من يكشف هوية المتسرب دون وقوع ضرر له ، كما عاقبت بالحبس من 05 سنوات إلى 10 سنوات وغرامة من 200.000 دج إلى 500.000 دج ، على الكشف على هوية المتسرب المفضي إلى أعمال عنف في حق المتسرب أو ذويه وهم زوجة أو أبناء أصوله المباشرين [1].

ـ اقتناء أو حيازة أو نقل أو تسليم أو إعطاء أموال أو منتجات أو معلومات متحصل عليها من ارتكاب الجرائم أو المستعملة في ارتكابه وفقا للمادة 65 مكرر 14.

---

[1]- طبقا للمادة 65 مكرر16 من قانون الإجراءات الجنائية ، ويعاقب المشرع أيضا يعاقب من 10 سنوات إلى 20 سنة والغرامة من 500.000 دج إلى 1.000.000 دج على الكشف المفضي إلى وفاة المتسرب أو أحد ذويه المذكورين سابقا دون الإخلال عند الاقتضاء بتطبيق أحكام الفصل الأول المتعلقة بالجنايات والجنح ضد الأفراد .

_ استعمال أو وضع تحت تصرف مرتكبي الجرائم وسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال وفقا للمادة 65 مكرر 14 ، وذلك بهدف إبعاد الشكوك حول المتسربين وتسهيل عملهم في كسب ثقة المجرمين [1].

*** سلطات المتسرب بعد وقف أو انقضاء مدة التسرب**

طبقا للمادة 65 مكرر 17 إذا تقرر وقف عملية التسرب أو انقضاء المدة المحددة في رخصة التسرب ولم تمدد، يمكن للمتسرب مواصلة النشاطات المذكورة في المادة 65 مكررا 14 للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا على ألا تتجاوز ذلك مدة 4 أشهر، ويخبر القاضي المصدر لرخصة التسرب في أقرب الآجال 4 أشهر دون أن يتمكن من توقيف نشاطه في ظروف يمكن للقاضي أن يرخص بتمديدها 4 أشهر على الأكثر [2] .

-الحماية القانونية للمتسرب:

وفر المشرع الجزائري حماية قانونية في المادتين 65 مكرر14، و 65 مكرر16، تتمثل في انعدام مسؤوليته الجنائية ، ومعاقبة كل من يكشف عن هوية المتسرب ، كالآتي :

---

[1]- وبالتالي الحصول على كافة المعلومات المتعلقة بهذه الشبكة الإجرامية من حيث عدد عناصرها وهويتهم وطرق اتصالاتهم وأماكن التقائهم والوسائل المستعملة في ذلك والحيل التي يستخدمونها إلى غير ذلك من المعلومات

[2]_ وبالتالي أجاز المشرع الجزائري للمتسرب مواصلة نشاطاته المذكورة في المادة 65 مكرر 17 ، بشرط ألا يتجاوز نشاطه مدة 4 أشهر القاضي المصدر للرخصة المنصوص عليها في المادة 65 مكرر 11، كما يمكن للقاضي تمديدها 4 أ شهر أخرى .

*** انعدام المسؤولية الجزائية للمتسرب:**

تنص المادة 65 مكرر14 من قانون الإجراءات الجزائية [1]، على أنه يمكن ضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرب والأشخاص الذين يسخرونهم لهذا الغرض دون أن يكونوا مسؤولين جزائيا ، القيام اقتناء أو حيازة أو نقل أو تسليم، أو إعطاء أموال أو منتوجات أو معلومات متحصل عليها من ارتكاب الجرائم أو المستعملة في ارتكابها ، أو استعمال أو وضع تحت تصرف مرتكبي الجرائم وسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال [2].

*** العقاب على الكشف على هوية المتسرب :**

نظرا للمخاطر الحقيقية التي يكون القائم بالتسرب عرضة لها في حياته ، وعلى أفراد عائلته عاقب المشرع بموجب المادة 65 مكرر16 بعقوبات في حق كل من يكشف عن هوية المتسرب أو يتسبب ذلك الكشف عن الاعتداء عليه أو على أهله أو يقضي إلى وفاته ، على النحو التالي :

-يعاقب على الكشف على هوية المتسرب دون وقوع ضرر له ، بالحبس من سنتين إلى خمسة سنوات وغرامة مالية من 00 50 إلى000 200 دج .

-أما الكشف على هوية المتسرب المفضي إلى أعمال عنف في حق المتسرب أو ذويه وهم زوجة أو أبناء أصوله المباشرين ، يعاقب عليه بالحبس من 05 سنوات إلى 10 سنوات وغرامة من200.000 إلى 500.000 دج .

---

[1] - راجع المادة 65 مكرر14 من قانون الإجراءات الجنائية الجزائري .

[2] - وبالتالي يمكن للقائمين بعملية التسرب القيام بالأفعال الواردة في 65 مكرر14 ، أثناء أداء مهامهم دون أن يكونوا مسؤولين جزائيا أي أنهم محميين قانونا بحكم الإذن الذي يرخص لهم بذلك بشرط احترام الإجراءات الشكلية والموضوعية المنظمة له.

- إلى وفاة المتسرب أو أحد ذويه المذكورين سابقا ، تكون العقوبة من 10 سنوات إلى 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.

3- المراقبة الالكترونية:

ينص المشرع الجزائري على المراقبة الالكترونية في المادة 04 من قانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أ-حالات المراقبة الالكترونية : لم يعرف المشرع الجزائري المراقبة الالكترونية في قانون 09-04 بل عدد حالاتها وذكر شروطها، بل عرفها في المادة 65 مكرر5 من قانون الإجراءات الجنائية على أنها وضع ترتيبات تقنية دون موافقة المعنيين من أجل بث وتسجيل الكلام المتفوه به [1].

وفقا للمادة 04 يمكن القيام بعمليات المراقبة في حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، أو في حالة توفير معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني ، أو لمقتضيات التحريات والتحقيقات القضائية ، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية ، أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة [2].

---

[1] – راجع المادة 65 مكرر 5 من قانون 22/06 المؤرخ في 2006 المعدل والمتمم للأمر 155/66 المؤرخ في 1966 المتضمن قانون الإجراءات الجنائية .

[2] – ويلاحظ أن المشرع الجزائري سمح بعمليات المراقبة الالكترونية كأسلوب وقائي قبل وقوع الاعتداء في جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة ، والاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني نظرا لخطورة هذه الجرائم بينما يتم اللجوء إلى المراقبة الالكترونية لضرورة التحريات والتحقيقات عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة .

ب-شـروط المراقبة الالكتــرونية

تتمثل شروط المراقبة الالكترونية وفقا للمادة 04 من قانون رقم 09-04: في الإذن المكتوب إذ لايجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه الاباذن مكتوب من السلطة القضائية المختصة . عندما يتعلق الأمر بالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها [1].

ويمنح الإذن المذكور من طرف النائب العام لدى مجلس قضاء الجزائر لمدة ستة (6) أشهر قابلة للتجديد على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها . ويشترط المشرع أن تكون الترتيبات التقنية المستعملة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بحياة الخاصة للغير.

المطلب الثاني: حجية الأدلة الالكترونية في الإثبات الجنائي

تتنوع نظم الأدلة الجنائية في الإثبات الجنائي، بين التي تأخذ بنظام الأدلة القانونية في الإثبات، وأخرى تعتنق نظام الإثبات الحر القائم على حرية القاضي الجنائي في الاقتناع، وتلك التي تجمع بين النظامين بما يسمى بالنظام المختلط [2].

---

[1] – ينص المشرع الجزائري على الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته في المادتين 13 و14 من قانون 09-04 ، وترك المشرع تحديد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم.

[2] – ووجه الفرق بين نظام الأدلة القانونية و نظام الأدلة الإقناعية، أن القاضي في النظام الأول يتقيد القاضي في الإثبات الجنائي بأدلة يحددها له المشرع مقدما ويقدر له قيمتها في الإثبات، فيتقيد القاضي بأن يستمد اقتناعه من هذه الأدلة دون غيرها، أما في نظام الأدلة الإقناعية فإن القاضي لا يقيده المشرع بأدلة إثبات لسلطته التقديرية في تقديراي دليل يمكن أن يتولد منه اقتناعه .

وعلى الرغم من سيادة نظام الأدلة الإقناعية في الإثبات لإثبات الجنائي في جل التشريعات المقارنة، إلا أن البعض منها قد يطبق في إثبات بعض الجرائم نظام الأدلة القانونية ، وذلك عندما ينص المشرع على تقييد سلطة القاضي في الإثبات بأدلة معين ومثال ذلك إعطاء حجية للمحاضر المحررة في بعض المخالفات بالنسبة لما ورد فيها وقائع إلى أن يثبت العكس ، وتقييد سلطة القاضي في إثبات بعض الجرائم بأدلة معينة[1]، وهذه الحجية وتلك القيود التي ترد على حرية القاضي في الاقتناع ليس المقصود منها افتراض ارتكاب المتهم للوقائع التي تنص على إعطائها الحجية ولكنها تعفي القاضي من إعادة التحقيق فيها، ويظل القاضي يملك سلطة تقدير هذه الأدلة ليستمد منها اقتناعه، ويظل المتهم معتصما بمبدأ افتراض براءته إلى أن يثبت عكس ذلك بالأدلة الكافية والمنطقية. بالنظر إلى الطبيعة الخاصة التي تتميز بها الأدلة الإلكترونية وما قد يصاحب الحصول عليها من خطوات معقدة، فإن قبولها في الإثبات قد يثير العديد من المشكلات، كالتلاعب فيها وتغيير الحقيقة التي يجب أن تعبر عنها.

يختلف موقف القوانين من حجية الأدلة الرقمية بحسب طبيعة نظام الإثبات السائد ، وعليه فإننا سوف نتطرق إلى موقف التشريعات اللاتينية (الفرع الأول) ثم موقف التشريعات الانجلوساكسونية وذات الصيغة المختلطة (الفرع الثاني) .

الفرع الأول: موقف التشريعات اللاتينية

أولا- حرية القاضي الجنائي بالاقتناع بالأدلة الالكترونية:

لم تفرد القوانين اللاتينية مثل القانون الفرنسي والقوانين الأخرى التي تأثرت به كالقانون كالجزائري والمصري ، نصوصا خاصة بمدى حجية الأدلة الالكترونية بل تترك حرية الإثبات لأطراف الخصومة في أن يقدموا ماهومناسب لاقتناع القاضي، حيث يلتمس القاضي تكوين اقتناعه من أي دليل يطرح أمامه، ويقوم بتقدير قيمته الإقناعية حسب ضميره.

[1] - راجع المادة 341 من قانون العقوبات الجزائري

وبالنظر إلى القوانين اللاتينية حيث يسود مبدأ حرية الإثبات والاقتناع، فإن سلطة القاضي الجنائي في قبول الأدلة الرقمية لا تثير صعوبات سواء بالنسبة لمدى حرية قبول الأدلة الرقمية لإثبات الجرائم الالكترونية ، أم مدى حرية القاضي في تقدير الأدلة الالكترونية[1].

وبالتالي يجوز للقاضي الجنائي الاستناد إلى الدليل الالكتروني لإثبات الجريمة في سائر الجرائم والجرائم الالكترونية على وجه الخصوص، باعتبارها أدلة إثبات في المواد الجنائية [2]. ففي فرنسا مثلا نجد أن مشكلة قبول الدليل الرقمي أمام القضاء الجنائي لا تطرح إشكالا في نظر الفقهاء، فالمبدأ هو حرية الأدلة وحرية القاضي في تقدير هذه الأدلة، اخذ بها المشرع وقبلها القضاء بناء على مجموعة شروط أهمها، أن يتم الحصول عليها بطريقة شرعية ونزيهة وأن يتم مناقشتها حضوريا الأطراف[3].

ولقد أثيرت في فرنسا مشكلة الإثبات لمحاضر المخالفات التي تتم عن طريق جهاز السينموتر، وانتهى القضاء هناك إلى عدم اعتبار هذه المحاضر
ذهب كل من الفقه والقضاء، إلى أن أي محضر لا تكون له قوة إثباتيه إلا إذا أثبت فيه محرره وقائع تدخل في اختصاصه، وأن يكون قد شاهدها أو سمعها أو تحقق منها بنفسه،[4].

---

[1] – هشام محمد فريد ، الجوانب الإجرائية للجريمة المعلوماتية مرجع السابق ، ص150. أنظر أيضا مروك نصر الدين ، محاضرات في الإثبات الجنائي ، الجزء الثاني (أدلة الإثبات الجنائي)، الكتاب الأول (الاعتراف والمحررات) ، الطبعة الرابعة ، دار هومة ، الجزائر ، 2010 .

[2] – إلا أن الاقتناع يجب أن يكون منطقيا وليس مبنيا على محض التصورات الشخصية للقاضي، فهذا المبدأ لا يعني التحكم القضائي، بل إن القاضي ملزم بأن يتحرى المنطق الدقيق في تفكيره الذي قاده إلى اقتناعه، فإذا كان تقديره للأدلة لا يخضع لرقابة محكمة النقض، إذ ليس لها أن تراقبه في تقديره إلا أن لها أن تراقب صحة الأسباب التي بنى عليها اقتناعه.

[3] – جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجيا الحديثة ، مرجع السابق ، ص34. مروك نصر الدين مرجع سابق ، ص468.

[4] – ومحكمة المقض الفرنسية أن أشرطة التسجيل الممغنطة التي يمكن أن تكون لها قيمة دلائل في الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي .كذلك قضت هشام فريد رستم ، مرجع السابق ، ص155.

إلا أن الاتجاه الحديث في فرنسا لم يعد يقف عند المفهوم المحدود للمستندات ، بل تطور بحيث أصبح يقبل الأدلة الإلكترونية كدليل إثبات ، إذ اعترف الفقه والقضاء الجنائيين في فرنسا الأدلة الالكترونية كالأشرطة المغنطيسية والأوراق المغنطيسية وغيرها من الأشكال الالكترونية الأخرى بأن لها قيمة دلائل الإثبات وبالتالي تصلح كأدلة إثبات أمام القضاء[1].

وفي البرازيل يسود النظام الإجرائي مبدأ حرية القاضي الجنائي في الاقتناع وعليه يتركز تنظيمه للإثبات الجنائي، لا يتقيد القاضي في حكمه بأنواع معينة من الأدلة، ويكون له، من حيث المبدأ قبول أي دليل يمكن أن يتولد معه اقتناعه، وهو ما يسمح بالقول، كقاعدة أولية بأن المتحصل عليها عن طريق آلة [2].

وقد اتجه أيضا الاتحاد الأوربي منذ منتصف الثمانينات إلى توجيه مشرعي دول أوربا لإقرار حجية الوثائق الالكترونية ، والاهم من ذلك التوجيه بعدم اشتراط أن تبرز من قبل منظميها والاستعاضة بشهادات خطية صادرة عن جهات مالكة النظم أو جهات وسيطة لظهور مشكلات

عمليات المعالجة وفي إطار تقنيات البرمجة القائمة على الذكاء الصناعي[3].

أما في مصر والجزائر فقد خلا قانون الإجراءات الجنائية من التعرض لحجية الأدلة الالكترونية ، ورغم ذلك فانه يمكن الاستناد إليها في إثبات الجريمة الالكترونية أو نفيها، لان المشرع المصري والجزائري أخذا بمبدأ الإثبات الحر[4].

---

[1] – هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص43.

[2] – هشام فريد رستم ،الجوانب الإجرائية للجريمة المعلوماتية مرجع سابق ، ص159.

[3] –عبد الفتاح حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت ، مرجع سابق ، ص164.

[4] –عبد الباسط خلاف ، مرجع سابق ، ص450-451

وتخضع هذه التشريعات اللاتينية الأدلة الإلكترونية للسلطة التقديرية للقاضي الجنائي، فإن استراح إليها ضميره ووجدها كافية ومنطقية فيمكنه أن يستمد اقتناعه ويعول عليها في الحكم الذي ينتهي إليه، إذ لايكفي الحصول على الدليل الرقمي وتقديمه للقضاء كدليل للإدانة[1].

ثانيا – تأثير الطبيعة العلمية للأدلة الالكترونية على اقتناع القاضي :

إن سلطة القاضي الجنائي في تقدير الدليل لا يمكن أن نتوسع في شأنها فالقاضي بثقافته القانونية

يتمتع من حيث قوته التدليلية بقيمة إثباتيه قد تصل إلى حد اليقين ، فهذا هو شأن الأدلة العلمية عموماً تقوم على أسس علمية دقيقة ولا حرية للقاضي الجنائي في مناقشة الحقائق العلمية الثابتة ، ولكن تقديره يكون للظروف والملابسات التي أحاطت به [2].

نظرا للطبيعة الفنية الخاصة للدليل الرقمي التي تمك

الحقيقة د

الخطأ في إجراءات الحصول على دليل صادق في الإخبار عن الحقيقة تبدو عالية في مثل هذا النوع من الأدلة ، ولذلك تثور فكرة الشك في مصداقيتها كأدلة للإثبات الجنائي، فتلك مسألة فنية لا يمكن للقا ، فبحث

مصداقية هذا الدليل هي من صميم فن الخبير لا القاضي.

---

[1] – إن سلطة القاضي الجنائي في تقدير الدليل تكون للظروف والملابسات التي أحاطت به ، ولا حرية للقاضي الجنائي في مناقشة الحقائق العلمية الثابتة ، لان الأدلة العلمية وخاصة الأدلة الالكترونية قائمة على أسس علمية دقيقة.

[2] – بحيث يكون في مقدور القاضي أن يطرح هذا الدليل ، وذلك عندما يجده لايتسق منطقيا مع ظروف الواقعة وملابساتها إذ ليس بمجرد توار الدليل العلمي يحكم القاضي مباشرة بالبراءة أو الإدانة. راجع عائشة بن قارة مصطفى، مرجع سابق ، 239 وما بعدها, وانظر أيضا :

Alan gahtan,Electronic evidence, Thomas Canada limitedm1999m p37

وعليه يقدر الخبير الأدلة الالكترونية من ناحية خضوعها للعبث [1]، ويمكن التأكد من سلامة الدليل الرقمي من العبث من خلال علم الحاسوب ، حيث يلعب ع
المعلومات الفنية التي تساهم في فهم مضمون وهيأة الدليل الرقمي، وهذه العلوم يستعان بها في كشف مدى التلاعب بمضمونه .

وتبدو فكرة التحليل التناظري الرقمي أيضا من الوسائل المهمة للكشف عن مصداقية الدليل الرقمي، ومن خلالها تتم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن خلال ذلك يتم التأكد من مدى حصول عبث في النسخة المستخرجة [2].

في الحصول على الدليل الرقمي نادرة للغاية، إلا أنها تظل ممكنة، ويرجع الخطأ إلى عدة أسباب ، أهمها الخطأ في استخدام الأداة المناسبة في الحصول على الدليل الرقمي، ويرجع ذلك للخلل في الشفرة المستخدمة أو بسبب استخدام مواصفات خاطئة ، أو الخطأ في استخلاص الدليل، ويرجع ذلك إلى اتخاذ قرارات لاستخدام الأداة تقل نسبة صوابها عن 100%
وسائل اختزال البيانات .

ونظرا لأن الإجراءات الفنية للحصول على الدليل الرقمي، يمكن أن يعتريها خطأ قد يشكك في سلامة نتائجها ، فإنه يمكن اعتماد باختبارات داوبورت [1]، كوسيلة للتأكد من سلامة الإجراءات

---

[1] –

ويسر، بحيث يظهر وكأنه نسخة أصلية تعبر عن الحقيقة.

[2] – كما يمكن التأكد من ذلك خلال استخدام الخوارزميات ، حتى في حالة عدم الحصول على النسخة الأصلية للدليل الرقمي أو في حالة أن العبث قد وقع على النسخة الأصلية ، هناك أيضا نوع من الأدلة الرقمية يسمى بالدليل المحايد، يساهم في التأكد من مدى سلامة الدليل الرقمي. راجع ممدوح عبد الحميد عبد المطلب، زبيده محمد قاسم، عبد الله عبد العزيز، مرجع سابق ، ص247.

المتبعة في الحصول على الدليل الرقمي من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات وللتأكد من سلامة هذه الإجراءات من الناحية الفنية[2].

وعليه فإذا توافرت في الدليل الرقمي شروط المذكورة سلامته من العبث والخطأ ، فإنه قد يبدو من غير المقبول أن يعيد القاضي تقييم هذا الدليل وطرحه من جديد على بساط البحث ، فالدليل لذا

هناك ما يرقى لمستوى التشكيك في الدليل ، وهو ما لا يستطيع القاضي الجزم به متى توافرت في هذا الدليل شروط السلامة ، بحيث يقتصر دور القاضي على بحث صلة الدليل بالجريمة ، أي

مصداقيته[3].

يمكن القول بأن التطور العلمي قد يؤثر بلا شك على نظام الاقتناع القضائي فقد يعلى هذا التطور من تقارير الخبراء، بالنظر إلى كثرة المسائل الفنية البحتة التي سوف تفرزها تطبيقات ثورة الاتصالات عن بعد، فهذا التطور قد يزيد من دور الخبرة في المسائل الجنائية،بالنظر إلى أن الكثير من الجرائم التي ترتكب كنتيجة لهذه الثورة ستقع على مسائل إلكترونية ذات طبيعة فنية

---

[1] – ترجع أصول هذا الاختبار (اختبارات داو برت) للحكم الذي أصدرته المحكمة العليا الأمريكية في قضية داوبورت ضد مريل دو للصناعات الدوائية 1993 ، راجع ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت ، دار الكتب القانونية ، مصر ، 2006، ص130–131.

[2] – يتم إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج المبتغاة، وذلك بإتباع اختبارين:

– اختبار السلبيات الزائفة : ومفاد هذا الاختبار أن تخضع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الرقمي، وأنه لا يتم إغفال بيانات مهمة عنه.

– اختبار الايجابيات الزائفة :

من التأكد من أن هذه الأداة لا تعرض بيانات إضافية جديدة.

[3] – نصت قوانين بعض الدول التي تعتنق نظام الأدلة القانونية على الحجية القاطعة للأدلة الرقمية ، راجع هلالي عبد الإله أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص 95.

معقدة، أو قد تستخدم هذه الوسائل في ارتكابها، وبالنظر إلى تطور مجالات الخبرة فإنه سوف تتسع مجالات اللجوء إليها[1].

الفرع الثاني : موقف التشريعات الانجلوساكسونية والتشريعات المختلطة

أولا _ موقف التشريعات الانجلوساكسونية :

يسود القوانين الانجلوساكسونية نظام الإثبات القانوني أو المقيد، حيث يحدد المشرع أدلة الإثبات ويقدر قيمتها الإقناعية، ومؤدى ذلك أن تقيد القاضي في حكمه بالإدانة أو البراءة بأنواع معينة من الأدلة، أو بعدد منها طبقا لما يسمى التشريع المطبق، دون أن يأبه في ذلك بمدى اقتناع القاضي بصحة ثبوت الواقعة أو عدم ثبوتها، إذ يقوم اقتناع المشرع بصحة الإسناد أو عدم صحته مقام اقتناع القاضي، وهكذا فإن اليقين القانوني يقوم أساسا على افتراض صحة الدليل بصرف النظر عن حقيقة الواقع أو ظروف الدعاوى [2].

ويثير قبول الأدلة المتحصلة من الوسائل الإلكترونية مشكلات عديدة في ظل القواعد الأنجلوأمريكية للإثبات الجنائي، والتي تعتنق كمبدأ أساسي الإثبات بالشهادة التي تتعلق بالواقعة محل ولذلك فإن قبول الأدلة الإلكترونية والتي هي عبارة عن إشارات الكترونية ونبضات ممغنطة يمثل مشكلة أمام القضاء في هذا النظام، إذ لا يمكن للمحلفين أو القاضي من مناظرة الأدلة المتولدة منها ووضع أيديهم عليها، وهذا يجعلها بمثابة أدلة ثانوية وليست أصلية[3].

---

[1] – جميل عبد الباقي الصغير، أدلة الإثبات والتكنولوجيا والأدلة الحديثة ، مرجع سابق، ص22.

[2] – و يتميز نظام الإثبات القانوني بأن المشرع هو الذي يقوم بالدور الإيجابي في عملية الإثبات في الدعوى، فهو الذي ينظم قبول الأدلة أو بإضفاء حجية دامغة على بعض الأدلة وأخرى نسبية على البعض الآخر، أما دور القاضي فهو آلي لا يتعدى مراعاة توافر الأدلة وشروطها[2]. راجع هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية مرجع سابق ، ص50.

[3] – هشام محمد فريد ، الجوانب الإجرائية للجريمة المعلوماتية مرجع سابق ، ص172.

وبالرجوع لقانون الإثبات الجنائي الانجليزي لسنة 1965، نجده تضمن تنظيما محددا لمسألة قبول مخرجات الحاسب كأدلة إثبات في المواد الجنائية، إلا أنه اعتبر أن المستند الناتج عن الحاسب لا يقبل كدليل إذا لم يستكمل باختبارات الثقة المنصوص عليها في القسم 69 [1].

كما صدر في إنجلترا قانون للإثبات الجنائي في سنة 1984 وعمل به بدءا من عام 1986 حيث نصت المادة 68 منه على أنه يقبل الإثبات بالمحررات الالكترونية إذا توافرت الشروط[2]:

– أن يكون المحرر عبارة عن سجل أو جزء من سجل يعده الشخص بموجب واجب يقع على عاتقه ليثبت فيه معلومات مقدمه إليه من شخص آخر يمكن قبول افتراض توافر علمه الشخصي بالأمور المتعلقة بها المعلومات.

–ألا يكون الشخص التي تستقي منه المعلومات متاح وجوده أو ممكنا تعيينه أو تتبعه أو يكون غير متوقع منه تذكر الأمور المتعلقة بالمعلومات.

ولقد نصت المادة 69 من ذات هذا القانون على أن الناتج من الوسائل الإلكترونية لا يقبل كدليل إذا تبين وجود سبب معقول يدعو إلى الاعتقاد بأن هذا الناتج غير دقيق أو أن بياناته غير ويجب كذلك أن يكون الحاسب الناتج منه المخرج الإلكتروني يعمل بكفاءة وبصورة سليمة[3].

ويلاحظ أن هذه التحفظات الأخيرة لا تطبق إلا إذا كانت مطبوعات الحاسب دليلا حقيقيا أو أصليا وليس مجرد نقل عن الغير.

وفي الولايات المتحدة الأمريكية فقد صدرت قوانين في بعض الولايات لتنظيم الإثبات الجنائي فقد صدر في ولاية كاليفورنيا في عام 1983 تشريعا للإثبات وقد نص هذا التشريع على أن النسخ

---

[1] – ويمكن تلخيص هذه الاختبارات في ضرورة عدم وجود سبب معقول للاعتقاد بأن المستخرج الحاسوبي غير دقيق أو أن بياناته غير سليمة، كما يجب أن يكون الحاسب الناتج منه هذا المستخرج يعمل بكفاءة وبصورة سليمة.

[2]– هشام محمد فريد ، الجوانب الإجرائية للجريمة المعلوماتية ، مرجع سابق ، ص174–176.

[3] علي محمود علي حمودة، مرجع سابق ، ص 23

المستخرجة من الحاسب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه البيانات، بل أنه في ولاية "أيوا" صدر قانون للحاسب الآلي في سنة 1984 نص على قبولها كأدلة اثبات [1].

وهوما سار عليه القضاء الأمريكي في أحكامه المختلفة، من أن الأدلة الالكترونية يجب أن تكون مقبولة كأدلة إثبات، طالما كان الحاسب المتولد عنه يؤدي وظائفه بصورة سليمة، وكان القائم عليه تتوافر فيه الطمأنينة والثقة[2].

ثانيا- موقف التشريعات ذات الطبيعة المختلطة :

كما قبلت القوانين ذات الطبيعة المختلطة الأدلة الالكترونية كأدلة إثبات، إذ نجد قانون الإجراءات الجنائية الشيلي قد سعى إلى توسيع طرق الإثبات بنصه في المادة 113 على أن الأفلام السينمائية والحاكي (الفونوغراف) والنظم الأخرى الخاصة بإنتاج الصور والصوت، والاختزال، وبصفة عامة أي وسائل أخرى قد تكون ملائمة، ووثيقة الصلة، وتفضي إلى استخلاص المصداقية، يمكن أن تكون مقبولة كدليل الإثبات، لصعوبة إثبات الجرائم المعلوماتية ، ومراعاة منه للتطورات العلمية الحديثة، وذلك بغرض إدخال وسائل إثبات حديثة وثيقة الصلة وملائمة كي تستمد منها المحكمة اقتناعها[3].

وعلى ضوء ذلك يرى رجال الفقه الشيلي أن الدليل الناتج عن الحاسوب يمكن أن يكون مقبولا في المحكمة كدليل كتابي أو مستندي مثله مثل النظم الحديثة الأخرى لجمع وتسجيل المعلومات، ذلك أن التقدم التقني قد تجاوز المفهوم التقليدي للمستند ، وأصبح يسمح بالحصول على وسائل

---

[1] – كما حسم القانون الأمريكي الفيدرالي حجية الدليل الالكتروني من خلال تعديل المادة 1/101 قانون الإثبات الفدرالي ، التي أصبحت تشمل المواد المكتوبة والمسجلة والالكترونية[1]. راجع عائشة بن قارة مصطفى، المرجع السابق، ص 206. أسامة المناعسة، مرجع سابق ، ص287 .

[2] – هلالي عبد اللاه أحمد، "حجية المخرجات الكمبيوترية في المواد الجنائية"، مرجع سابق، ص49 وما بعدها.

[3] –هشام فريد رستم ، الجوانب الإجرائية للجريمة المعلوماتية مرجع سابق ، ص164-165.

أخرى من التسجيلات ، طالما أن هذه الوسائل العلمية من قبيل المستندات فإنها تدخل في مفهوم المادة 187 التي تنص على المستندات العامة والخاصة بوصفها وسيلة لإثبات[1].

وفي اليابان حصر المشرع الياباني طرق الإثبات في أربعة طرق إثبات مقبولة وهي أقوال المتهم ، وأقوال الشهود ، والقرائن ، والخبرة ، أما بالنسبة للأدلة الالكترونية فيقرر الفقه الياباني أنها لايمكن أن تستخدم كأدلة إثبات في المحكمة لكونها غير مرئية ، لذا يكون من الضروري تحويلها إلى شكل مرئي كي تستخدم كوسيلة أثبات ، سواء كانت أصلية أم نسخة من هذا الأصل[2].

وتجدر الإشارة إلى أن الأنظمة القانونية المختلفة قد قبلت الأدلة المتحصلة من الوسائل الإلكترونية كأدلة إثبا الانجلوساكسوني قد أورد الكثير من الشروط لقبولها كأدلة إثبات نظرا لطبيعة هذا النظام والذي يعتمد في الأصل على النظام الاتهامي القائم على مبدأ التواجهية .

[1] – علي حسن محمد طوالبة، مرجع سابق ، ص198. راجع كامل عفيفي عفيفي ، مرجع سابق ، ص374.

[2] – هشام فريد رستم ، الجوانب الإجرائية للجريمة المعلوماتية مرجع سابق ، ص159. هلالي عبد اللاه أحمد، "حجية المخرجات الكمبيوترية في المواد الجنائية"، مرجع سابق، ص62.

خـاتمــة

خـاتمـة

إن الأهمية المتزايدة للتجارة الالكترونية، أصبحت تقتضي ضرورة التدخل القانوني لتوفير الحماية اللازمة لهذه التجارة الالكترونية من جرائم الاعتداء عليها ، وبناءا على ذلك اهتمت التشريعات وخاصة المقارنة بتوفير حماية جنائية للتجارة الالكترونية سواء في نصوص عامة أم خاصة.

وعليه جاءت دراستنا للحماية الجنائية للتجارة الالكترونية من خلال بابين تناولنا في الباب الأول الحماية الجنائية الموضوعية للتجارة الالكترونية في النصوص العامة المتعلقة بجرائم الأموال وجريمة التزوير ، ومن خلال النصوص الخاصة بالمواقع والبيانات الشخصية ووسائل التجارة الالكترونية ، أما الباب الثاني بحثنا فيه الحماية الجنائية الإجرائية للتجارة الالكترونية قبل مرحلة المحاكمة في مرحلتي البحث والتحقيق الابتدائي ، وفي مرحلة المحاكمة من خلال تحديد المحكمة الجنائية المختصة وسلطة المحكمة الجنائية في قبول وتقدير الأدلة الالكترونية .

وتوصلنا من خلال تلك الدراسة إلى أن أحكام القضاء في العديد من لدول على اعتبار المعلومات مالا في مفهوم جرائم الأموال ، وبالتالي تطبق عليه نصوص جرائم الأموال ، إلا أنها توفر حماية كافية للمعلومات من جريمة الإتلاف ، بخلاف بقية نصوص جرائم الأموال الأخرى والتي توفر حماية نسبية وغير كافية للمعلومات ، مما حدا بالبعض إلى الدعوة إلى ضرورة تدخل تشريعي لحسم هذا الخلاف أو بسط حماية جزائية مباشرة بواسطة نصوص خاصة ، وهو ما تحقق بالنسبة لجريمة الإتلاف المعلوماتي التي نصت عليها العديد من التشريعات في نصوص خاصة كالتشريع الفرنسي والانجليزي والجزائري والتونسي وغيرها من التشريعات .

ويمكن أيضا تطبيق نصوص جرائم التزوير على المحررات التجارية الالكترونية ، انطلاقا من عمومية هذه النصوص ، وكون الهدف من تجريم التزوير حماية الثقة العامة في المحررات بغض النظر عن طبيعتها ، وقد حسمت بعض التشريعات هذا الخلاف ، كالتشريع الفرنسي والتشريع

الانجليزي والتي وسعت من مفهوم المحرر محل جريمة التزوير ليشمل كافة المحررات المادية وغير المادية .

جاء التشريع الفرنسي بحماية جنائية لمواقع التجارة الالكترونية كنظام معلوماتي ، وكانت تلك الحماية متوازنة من خلال توسيع نطاقها ، وتقرير عقوبات مناسبة وردعية ، لكنها دون أن تكون مشمولة بحماية فنية ، كما وفر التشريع الأمريكي حماية جنائية لها باعتبارها نظم في جرائم الكمبيوتر ، لكنه اهتم بالتفاصيل أكثر لأنه يهنك بالأمن القومي والجانب الاقتصادي ، ولم يجرم مجرد الدخول ، بل تطلب أن يتعلق الأمر بمعلومات متعلقة بمصالح الدولة العليا، كما وفرت بعض التشريعات العربية كالتشريع الجزائري والتونسي حماية للمواقع في إطار جرائم الاعتداء عل أنظمة المعطيات أسوة بالتشريع الفرنسي ، و شملت تلك الحماية عدة جرائم لكنها تضمنت عقوبات غير ردعية .

وفرت بعض التشريعات المقارنة حماية جنائية للبيانات الشخصية ، كالتشريع الفرنسي الذي حماها جنائيا في نصوص خاصة في إطار قانون العقوبات ، من خلال تجريم عدة جرائم سلبية وايجابية ، وقرر لها عقوبات مناسبة وردعية وخاصة الغرامة التي وصلت الى 300 ألف أورو كما عاقب عليها ولو بالإهمال ، وكذلك جاء التشريع الجزائري بحماية جنائية خاصة للبيانات الشخصية في أطار قانون العقوبات ، لكنها متواضعة وغير كافية لأنها اقتصرت على جرائم قلة ورغم ذلك عاقبت على الشروع وجعلت صفح الضحية جائز أمام المتابعة ، وعلى خلاف ذلك جاء التشريع التونسي بحماية جنائية أفضل بكونها واسعة النطاق ، وكانت الغرامات كبيرة وصلة الى 100الف دينار في جريمة الإفشاء ، لكمه يلاحظ أنه عاقب بالغرامات ، واقتصر العقاب على مزودي الخدمات أو أحد أعوانه دون غيرهم .

نظمت بعض التشريعات الأوربية بعض القواعد الخاصة بالمسؤولية الجنائية بوسطاء الانترنت تتمشى مع القواعد العامة كاحترامها لقرينة البراءة من خلال تكليف النيابة العامة بإثبات أدلة الإدانة ، واحترام مبدأ شخصية العقوبة ، كما خصت بعض التشريعات العربية كالتشريع الجزائري

في إطار قانون 09-04 ، والتشريع التونسي في إطار قانون المبادلات والتجارة الالكترونية لسنة 2001، وتعد تلك الجهود خطوة جريئة ، لكنها تظل غير كافية من ناحية أنها ضيقت في مطاق المسؤولية الجنائية وقصرتها على جرائم قليلة ، وتفتقر الى عقوبات مناسبة خاصة في جريمة الإفشاء ، إذ أحالتنا في عقوبتها الى القواعد العامة رغم خطورة هذه الجرائم .

لم يخص التشريع الفرنسي والجزائري التوقيع الالكتروني بحماية جنائية خاصة ، بل يمكن حمايته في إطار القواعد العامة لقانون العقوبات من خلال جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات ، وجريمة التزوير ، وكذلك الحال بالنسبة للتشريع الفيدرالي الامريكي من خلال جرائم الكمبيوتر، إلا أن تلك الحماية قاصرة كما أسلفنا على مصالح الدولة العليا أو إحدى المؤسسات الاقتصادية .

على خلاف تلك التشريعات خصت بعض التشريعات العربية التوقيع الالكتروني بحماية جنائية كالتشريع التونسي الذي جاء بحماية شملت العديد من الجرائم سواء في إطار النصوص العامة أم في النصوص الخاصة ، وجاء بعقوبات مناسبة ، كما خصه التشريع المصري بحماية جنائية في إطار قانون رقم 15-2004 المتعلق بالتوقيع الالكتروني في المادتين 21، 23، وشملت تلك الحماية العديد من الجرائم ، لكن المشرع لم يجرم الشروع وبالتالي لاعقاب على الشروع فيها، ، ولم يميز بين تعطيل التوقيع الالكتروني الذي يترتب عليه توقيف مصلحة خاصة،أو توقيع مصلحة عامة ، كما لم بجرم صنع أو حيازة برامج معدة لاعتداء عل التوقيع الالكتروني ، وبالتالي لم يكرس الحماية الوقائية .

حاول الفقه والقضاء توفير حماية جنائية لبطاقات الوفاء والائتمان ، لكن في الحقيقة أن النصوص القائمة وان كانت توفر حماية قدرا من الحماية الجناية لبطاقة الوفاء من الاستخدام غير المشروع لبطاقة الوفاء من قبل حاملها ، إلا أنها توفر حماية غير كافية من بعض الجرائم المحدودة فقط ، كحالة امتناع حامل البطاقة عن رد البطاقة الملغاة الذي جريمة خيانة الأمانة وأيضا في حالة تواطؤ حاملها مع التاجر فإنهما يساءلان جزائيا بجريمة النصب .

أما بالنسبة للاستخدام غير المشروع لبطاقة الوفاء والائتمان من قبل الغير ، فالنصوص القائمة توفر حماية جنائية كافية نوعا ما من العديد من الجرائم ، إذ يشكل الاستخدام غير المشروع لبطاقة وفاء مسروقة أو مفقودة من قبل الغير جريمة النصب، على اعتبار أن المتهم انتحل اسما كاذبا و هو اسم الحامل الشرعي للبطاقة ، كما قد يحدث أن يكون هناك تعدد مادي مع الارتباط بين جريمة النصب و جريمة أخرى كالسرقة أو التزوير، أو إخفاء أشياء مسروقة، ففي هذه الحالة تطبق عقوبة الجريمة ذات الوصف الأشد ،كما يمكن تطبيق أحكام التزوير على بطاقة الوفاء سواء جريمة التزوير أو استعمال محرر مزور لكون نصوص جريمة التزوير جاءت عامة هذا من جهة، ومن جهة أخرى عدم إمكانية القراءة البصرية للمحررات لا ينفي عنها صفة المحرر.

على الرغم من هذه الحماية الجنائية التي توفرها النصوص القائمة من خلال جريمة السرقة والنصب والتزوير واستعمال محرر مزور ، إلا إن الأمر بحاجة إلى تدخل تشريعي لتجريم بعض الصور كتجاوز الحامل لرصيده ، أو تقليد البطاقة الصور ، وذلك بتعديل النصوص القائمة كما هو الحال في التشريع الكندي الصادر عام 1985، والتشريع الأسترالي لعام 1983، أو بإصدار نصوص خاصة، كما هو الحال بالنسبة للمشرع الفرنسي الذي استحدث قانون أمن الشيكات، وبطاقات الوفاء رقم 1382/91 الصادر في عام 1991، وبالتالي الحماية الجنائية العامة لبطاقة الوفاء من خلال جرائم الأموال والتزوير بحاجة إلى حماية جنائية خاصة إضافية ومكملة.

وعليه فان أغلب التشريعات العربية باستثناء البعض كالتشريع الجزائري والتونسي والمصري والامارتي ، لم تعدل نصوصها الجنائية ولم تستحدث نصوصا خاصة بتجريم الاعتداء على المستندات الالكترونية بصفة عامة كالمواقع الالكترونية والتوقيع الالكتروني وبطاقات الائتمان بصفة خاصة على الرغم من أهميتها العملية ، بخلاف التشريعات المقارنة كالقانون الفرنسي الذي عدل نص التجريم الخاص بجريمة التزوير التقليدية على نحو شمل نطاقها معه المستند الإلكتروني واستحدث تشريع لحماية بطاقة الائتمان، وكذلك الحال بالنسبة للتشريع الألماني الذي أضاف إلى باب التزوير نصوصا خاصة بتزوير المستند الإلكتروني.

بالإضافة الى الإشكاليات القانونية الموضوعية التي أثارتها جرائم التجارة الالكترونية أثارت أيضا بعض الإشكاليات الإجرائية ، إذ إن التحقيق والبحث في جرائم الإنترنت لاسيما جرائم التجارة الالكترونية وملاحقة مرتكبيها يتم بصعوبة وتعقيد بالغين، مما أدى إلى ظهور تحدي كبير لأجهزة الضبط القضائي سواء على المستوى الدولي أو المستوى الوطني نتج عنه بعض الصعوبات التي تعيق عمل هذه الأجهزة.

لذلك أنشأت بعض التشريعات الأجنبية كفرنسا وانجلترا ، و.م.أ ، ضبطية قضائية متخصصة في مكافحة الجرائم المعلوماتية ، كما أنشا المجتمع الدول الانتربول كجهاز دولي متخصص بالضبط القضائي في جرائم الإنترنت والذي ساهم في الكشف عن كثير من القضايا الدولية وضبط مرتكبيها وبالإضافة إلى ذلك فأن الدول الأوربية أنشأت منظمات ومكاتب متخصصة بجرائم الإنترنت وموجدة في الدول الأوربية الاوربول تعمل على مراقبة المشتبه بهم عبر الحدود وملاحقة المجرمين.

كذلك أنشأت بعض التشريعات العربية كمصر والإمارات ضبطية قضائية متخصصة في مكافحة الجرائم المعلوماتية ، وكذلك الحال في التشريع الجزائري من خلال استحداث مركز لمكافحة جرائم الانترنت على مستوى الدرك الوطني ، والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بموجب قانون رقم 09-04 المتعلق بالوقاية من جرائم الاتصال والمعلومات ومكافحتها ، والتي لها دور كبير في مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية ، وأيضا وتبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم .

يتمثل الاختصاص الأصيل للضبطية القضائية في البحث والتحري ، إلا أن هنالك من الظروف ما يستدعي التدخل المباشر والسريع بإجراء من إجراءات
والمحافظة على أدلة الجريمة، لذا يجوز لأعضاء الضبط القضائي في الجرائم المعلوماتية لاسيما

التجارة الالكترونية سلطة اتخاذ بعض إجراءات التحقيق الابتدائي كالتفتيش والضبط والمعاينة منزله ، وذلك في حالة التلبس وكذلك في حالة صدور أمر إليه من قاضي التحقيق أو المحقق.

على الرغم من إنشاء بعض التشريعات لضبطية قضائية متخصصة في مكافحة الجرائم المعلوماتية ، إلا أن إجراءات التحري والتحقيق لاسيما التفتيش والضبط والمعاينة تتم في كثير من الدول وخاصة العربية في إطار النصوص الإجرائية التقليدية ، وهذا لا يتلاءم في الحقيقة مع طبيعة وخصوصية الجرائم المعلوماتية لاسيما جرائم التجارة الالكترونية ، باستثناء بعض التشريعات كالتشريع الفرنسي والانجليزي والبلجيكي مثلا ، والتي حسمت قابلية نظم الحاسوب والانترنت للتفتيش والضبط والمعاينة ، بل أكثر من ذلك سمحت بلجيكا بامتداد التفتيش خارج إقليم الدولة ، وكذا التشريع الجزائري الذي سمح بالتفتيش والمعاينة والضبط في المادتين 45، و47 من قانون الإجراءات الجنائية في أي وقت ، ودون حضور صاحب المسكن المشتبه فيه أو المتهم خروجا على القواعد العامة ، كما سمح بالتفتيش والضبط في قانون 09-04 .

استحدثت التشريع الجزائري أيضا وسائل تحري وتحقيق حديثة لمكافحة الجرائم المعلوماتية كإجراء اعتراض المراسلات والاتصالات، والتسرب في إطار قانون الإجراءات الجنائية ، والمراقبة الالكترونية في قانون 09-04 المتعلق بالوقاية من جرائم الاتصال والمعلومات ومكافحتها .

إذ منح لضابط الشرطة القضائية في إطار عملية اعتراض المراسلات صلاحيات واسعة كوضع الترتيبات التقنية دون موافقة المعنيين ، في أماكن خاصة أو عمومية ، وفي أي وقت ، وبغير علم أو رضا أصحابها، ويسلم الإذن لمدة أقصاها أربعة (4)أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق .

وفي المقابل أخضع المشرع الجزائري عمل الضبطية القضائية للرقابة القضائية، حفاظا على حقوق وحريات الأفراد ومبدأ المشروعية، وتنفذ العمليات المأذون بها تحت المراقبة المباشرة لوكيل الجمهورية المختص، أو تحت الرقابة المباشرة للقاضي التحقيق في حالة فتح تحقيق ابتدائي.

ويراقب القضاء العمليات المأذون بها رقابة المشروعية، أي مراقبة مدى مطابقة عمليات الاعتراض والالتقاط والتسجيل للقانون، كما يراقب القضاء تلك العمليات رقابة موضوعية، من خلال تقدير مدى قيمة وكفاية أدلة الإثبات الموجودة في محاضر الضبطية القضائية .

في إطار تدعيم دور الضبطية القضائية في مكافحة الجرائم المعلوماتية، منح المشرع الجزائري أيضا سلطات لضباط أو أعوان الشرطة القضائية المكلفين بالتسرب تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية ، سواء خلال سريان عملية التسرب ، أو بعد وقف أو انقضاء مدة التسرب، بحيث يمكن للمتسرب مواصلة نشاطاته للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا ، كما ووفر المشرع الجزائري حماية قانونية للمتسرب ، تتمثل في انعدام مسؤوليته الجنائية ، ومعاقبة كل من يكشف عن هوية المتسرب .

بالإضافة الى ذلك تبنى المشرع الجزائري المراقبة الالكترونية في المادة 04 من قانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ذلك في بعض الجرائم الخطيرة ، كحالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، أو في حالة توفير معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني أو لمقتضيات التحريات والتحقيقات القضائية ، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية ، أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة .

إن تنامي جرائم التجارة الالكترونية ، وتخطي آثارها حدود الدول ، أفرز جملة من التحديات القانونية على الصعيد الإجرائي ، من أبرزها مشكلة تنازع الاختصاص بصدد هذه الجرائم باعتبار أن آثارها تتجاوز حدود الدول ،

إذ حسنت بعض التشريعات مسألة الاختصاص الجنائي في الجرائم المعلوماتية، كالتشريعات الأجنبية لفرنسا وانجلترا ، و.م.أ، والتي جعلت الاختصاص لمحاكمها الوطنية حتى ولو وقعت

الجريمة المعلوماتية في الخارج طالما تحققت آثارها في الداخل ، وكذلك مد التشريع الجزائري الاختصاص في هذه الجرائم ،لكنه امتداد داخلي وليس خارجي ، لا يمتد الى الجرائم الواقعة في الخارج ، رغم ذلك فبمكن تطبيق القواعد العمة الواردة في المواد 582-589 من قانون الإجراءات الجنائية الجزائري .

رغم ذلك فان الحلول الوطنية غير كافية لكونها تميل معظمها إلى الطابع الإقليمي ، بل يحتاج الأمر إلى تعاون وتنسيق بين الدول لتجاوز هذه العقبات الإجرائية فلا يجوز امتداد الإجراءات الجنائية

الموجودة في وسط افتراضي خارج حدود الدولة تطبيقاً لاتفاقات الإنابة القضائية، أو وفقا لنظام تبادل المساعدات ، وبالتالي لامناص من التعاون الدولي في هذا المجال بمقتضى اتفاقية ثنائية أو متعددة الأطراف، أو على الأقل الحصول على إذن الدولة التي تلك الإجراءات في مجالها الإقليمي.

كما اتجهت بعض الدول الى تطبيق مبدأ الاختصاص الجنائي العالمي لحل مشكل الاختصاص الجنائي في الجرائم المعلوماتية العابرة للحدود ، لكن هذا المبدأ تعترضه ي قانونية كرفض تسليم المجرمين ، والحصانة القضائية ، وتقادم العقوبة ، وصعوبات عملية سياسية ومالية إذ كثير ما يحول الجانب السياسي والمالي دون محاكمة الأشخاص المشتبه فيهم أو المتهمين .

وتكتنف أيضا هذه الجرائم أيضل صعوبات تتعلق بإثبات هذه الجرائم وقبول الدليل بشأنها لكن رغم ذلك الأنظمة

الانجلوساكسوني قد أورد الكثير من الشروط لقبولها كأدلة إثبات نظرا لطبيعة هذا النظام والذي يعتمد في الأصل على النظام الاتهامي .

على الرغم من القيمة العلمية القاطعة للدليل الالكتروني ، لكن يبقى يخضع لسلطة القاضي الجنائي التقديرية، لأن يقتصر دور القاضي على بحث صلة الدليل بالجريمة أي أن الشك في الدليل الرقمي لا يتعلق بمضمونه كدليل ، عنه.

يمكن القول بأن التطور العلمي قد يؤثر بلا شك على نظام الاقتناع القضائي، فقد يعلى هذا التطور من تقارير الخبراء ، بالنظر إلى كثرة المسائل الفنية البحتة التي سوف تفرزها تطبيقات ثورة الاتصالات عن بعد، فهذا التطور قد يزيد من دور الخبرة في المسائل الجنائية.

وبناءا على هذه النتائج اقترح اعتبار المال المعلوماتي المعنوي كالبرامج والمعلومات على قدم المساواة في الحماية الجنائية مع الأموال المنصوص عنها في قوانين العقوبات التقليدية.

وضرورة توسيع في مفهوم المحرر محل جريمة التزوير في التشريع الجزائري كما فعلت بعض التشريعات الأجنبية كالتشريع الفرنسي.

إعادة النظر في حماية المواقع والحماية الجنائية للبيانات الشخصية في التشريع الجزائري ، بتوسيع نطاقها من حيث الجرائم ، وتقري عقوبات مناسبة وردعية .

وتقرير حماية جنائية خاصة لبطاقات الدفع والسحب في التشريع الجزائري ، أ, تعديل النصوص القائمة لتشمل جميع صور الاعتداء على هذه البطاقات .

كذا إعادة النظر في قواعد المسؤولية الجنائية لوسطاء الانترنت في التشريع الجزائري ، من خلال توسيع نطاقها ، وتقرير عقوبات مناسبة .

ضرورة إصدار قانون خاص بالتوقيعات الإلكترونية يتم من خلاله بيان بشكل مفصل شروط صحة التوقيع الإلكتروني، تحديد أنواعه و بيان حجية كل نوع تحديد الشروط الدنيا على الأقل في المنظومة المستعملة في إنشاء التواقيع الإلكترونية وكيفية استخدامها والأجهزة المستخدمة في ذلك بتنظيم مسألة التشفير. وبيان جرائم الاعتداء على التوقيع الالكتروني .

و ي المجال المعلوماتي توكل لها مهمة منح التوقيعات الإلكترونية والتزويد بخدمات التصديق وتنظيم كيفية قبول شهادات تصديق هيئات أجنبية معتمدة لدى دولها لتنشيط التجارة و المبادلات.

يتعين على المشرع الجزائري تحيين جملة من القوانين لاسيما القانون الجنائي، أو اعتماد قانون بشأن التجارة الإلكترونية لمسايرة التطور الحاصل خاصة مع فتح السوق الوطنية على الاستثمار الأجنبي.

وضرورة تعاون الدول فيما بينها من اجل إصلاح تشريعاتها الجنائية ووضع قوانين لمكافحة ومتابعة مرتكبي هذه الجرائم ، وضرورة إنشاء لجان متخصصة في مكافحة جرائم الإنترنت في الدول العربية، ذلك لمواجهة حداثة هذه الجريمة من حيث أساليبها وأدواتها المستعملة في تنفيذها لكون جرائم التجارة الالكترونية جرائم عابرة للحدود.

و اعد الإجرائية الحالية بما يتمشى مع طبيعة الجرائم المعلوماتية عبر الوطنية ، أواستحداث قواعد مناسبة في مجال الإجراءات الجنائية بشان التحقيق في هذه الجرائم بشكل يضمن تحقيق التوازن بين متطلبات تحقيق العدالة والحفاظ على خصوصية الحياة الخاصة للأفراد .

و حث الدول العربية على إبرام اتفاقية فيما بينها على غرار على غرار اتفاقية مكافحة الإرهاب وعلى غرارالاتفاقية الأوروبية بغية تعزيز التعاون القضائي والشرطي بجميع صوره لمواجهة التحديات الإجرائية الناجمة عن جرائم التجارة الالكترونية العابرة للحدود ، والاهتمام بالتأهيل المناسب لكوادر الأجهزة القضائية بما يجعلها قادرة على التعامل مع جرائم التجارة الالكترونية بكفاءة.

كما يلزم تدخل المشرع لتحديد معايير الاختصاص في الجريمة المعلوماتية بشكل عام وجرائم التجارة الالكترونية بشكل خاص ، وعدم تركها لاجتهاد الفقه والقضاء، بحيث يكون من الملائم أن

ينعقد الاختصاص لقانون أي بلد أضرت به الجريمة أو من المتوقع أن تشكل خطورة على مصالحه الحيوية ، ولو كان مكان وقوعها خارج نطاق إقليمها ، فمن المناسب تبني مبدأ الاختصاص العالمي أو الشامل ، من أجل تجنب الكثير من المشاكل الناجمة عن تنازع الاختصاص.

و ضرورة النص صراحة في التشريع الجزائري على الأدلة الرقمية كأدلة إثبات في المجال الجنائي والاعتراف لها بحجية قاطعة باعتبارها استثناء على سلطة القاضي الجنائي في تقدير الدليل ، مع إمكانية النص على وسائل التأكد من سلام
الدليل ، وعقد اتفاقيات دولية للاستفادة من نظام الإنابة القضائية وتبادل المعلومات لتفادي مشكلة البحث عنا الدليل الرقمي خارج الحدود.

وأخيرا التوسع في عقد الاتفاقيات الدولية للاستفادة من نظام الإنابة القضائية وتبادل المعلومات في المجال المعلوماتي لتفادي مشكلة البحث عن الدليل الرقمي خارج حدود الدولة .

تم بحمد الله وعونه

قائمة المـراجـع

قائمة المراجـع

أولا – المراجع باللغة العربية :

أ– الكتب العامة :

1–أحمد عبد الخالق، التجارة الالكترونية و العولمة ، منشورات المنظمة العربية للتنمية الإدارية مصر ، 2006 .

2–أحمد أبو الروس قانون جرائم التزييف والتزوير والرشوة واختلاس المال العام من الوجهة القانونية والفنية، المكتب الجامعي الحديث 1998.

3–أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري الجزء الثاني ، ديوان المطبوعات الجامعية ، الجزائر ، 1999 .

4–أحمد فتحي سرور ، الوسيط في قانون الإجراءات الجنائية ، الطبعة السابعة ، دار النهضة العربية ، القاهرة مصر 1993.

5– أحمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية، دار هومة للطباعة والنشر والتوزيع، الجزائر، دون طبعة، 2005.

6– أحسن بوسقيعة، المنازعات الجمركية ، دار الحكمة للنشر والتوزيع ،الجزائر، 1998.

7– أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص ، الجزء الأول ، ط7، دار هومة الجزائر، 2014.

8–إسحاق إبراهيم منصور، المبادئ الأساسية ي قانون الإجراءات الجزائية الجزائري ، ديوان المطبوعات الجامعية ، الجزائر ، 1995.

9- أكرم عبد الوهاب، التجارة الالكترونية، مكتبة ابن سينا ، القاهرة ، 2004 .

10-انتصار نوري ، دراسة في علم الإجرام والعقاب، دار المطبوعات الجامعية، الإسكندرية 1980.

11-حسنين المحمدي بوادي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر الجامعي الإسكندرية، 2004.

12-حسن صادق المرصفاوي ، قانون العقوبات ، دار المعارف ، 1962.

13-حسنين المحمدي بوادي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر الجامعي، الإسكندرية، 2004، ص.164

14- رمسيس بهنام ، النظرية العامة للقانون الجنائي ، الطبعة الثانية ، الإسكندرية منشأة المعارف ، الإسكندرية ،1968.

15- سليمان مرقص، المدخل للعلوم القانونية، الطبعة الأولى، (د- ت).

16- سعد أحمد محمود سلامة، التبليغ عن الجرائم، دراسة مقارنة، رسالة دكتوراه، أكاديمية الشرطة، القاهرة، 2003.

17-عبد القادر القهوجي، و فتوح عبد الله الشاذلي شرح قانون العقوبات، (القسم الخاص) دار المطبوعات الجامعية،الإسكندرية ، 2003 .

18- عبد المنعم فرج الصدة ، أصول القانون، دار النهضة العربية ،القاهرة ، 1975.

19- عبد المجيد جباري، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة دار هومة ، الجزائر 2012.

20- عبدا لله أوهابية ، شرح قانون الإجراءات الجزئية الجزائري(التحري والتحقيق) دار هومة الجزائر, 2004 .

21-عبد الرحمن خلفي، محاضرات في قانون الإجراءات الجزائية، دار الهدى، عين مليلة، الجزائر،(د- ت).

22-عبد الواحد محمد الفار، الجرائم الدولية وسلطة العقاب عليها، دار النهضة العربية، القاهرة، 1996.

23-عمر خوري ، شرح قانون الإجراءات الجزائية الجزائري , دار هومة , الجزائر ,2007 .

24- علاء الدين شحاتة، التعاون الدولي في مجال مكافحة الجريمة، القاهرة، 2000.

25- محمد عوض، الجرائم المضرة بالمصلحة العامة، دار المطبوعات الجامعية، الإسكندرية، 1985.

26- محمد زكي أبو عامر قانون العقوبات (القسم الخاص)، دار الجامعة الجديدة، الإسكندرية ، 2005.

27- محمد زكي أبو عامر ، الإجراءات الجنائية ، الطبعة السادسة ، دار الجامعة الجديدة ، الإسكندرية مصر ، 20005.

28- محمد فتحي عيد، الإنترنت ودوره في انتشار المخدرات، أكاديمية ناصيف العربية للعلوم الأمنية، الرياض ، 2003.

29- محمود مصطفى، شرح قانون العقوبات، القسم الخاص، مطبعة جامعة القاهرة مصر، 1984.

30- محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، الطبعة الثانية ، دار النهضة العربية، القاهرة ، 1994.

31- نبيل إبراهيم سعد، الإثبات في المواد المدنية و التجارية في ضوء الفقه و القضاء، منشأة المعارف، الإسكندرية، 2000.

32-نجاة أحمد إبراهيم ، المسؤولية الدواية عن انتهاكات قواعد القانون الدولي الإنساني منشأة المعارف ، الإسكندرية ، 2009 .

33- نصر الدين مروك ، محاضرات في الإثبات الجنائي ، الجزء الثاني (أدلة الإثبات الجنائي)، الكتاب الأول (الاعتراف والمحررات) ، الطبعة الرابعة ، دار هومة ، الجزائر ، 2010 .

34-هدى قشقوش ، شرح قانون العقوبات ، القسم الخاص ، دار النهضة العربية القاهرة ، 20007.

ب- الكتب المتخصصة:

1- أحمد حسام طه تمام، الجرائم الناشئة عند استخدام الحاسب الآلي (ودراسة مقارنة)، دار النهضة العربية، القاهرة مصر 2000.

2-أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومة للطباعة والنشر الجزائر 2006.

3-أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات دار النهضة العربية القاهرة مصر 1998.

4-أسامة محمد المناعسة، جلال محمد الزعبي و فاضل الهواوشة ، جرائم الحاسب الآلي والانترنت دراسة مقارنة ، الأردن : دار وائل للنشر ، الطبعة الأولى 2001.

5-إبراهيم الدسوقي،الجوانب القانونية للتعاملات الإلكترونية ، مجلس النشر العلمي ، جامعة الكويت 2003 .

6-الياس ناصيف ، العقود الدولية ، العقد الالكتروني في القانون المقارن ،ط1 ، منشورات الحلبي الحقوقية ، بيروت ،2009.

7- إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الحديثة للنشر، الإسكندرية، 2008.

8-جميل عبد الباقي الصغير، الحماية الجنائية و التقنية لبطاقات الائتمان الممغنطة، دار النهضة العربية للنشر، القاهرة، مصر، 2003.

9-جميل عبد الباقي، القانون الجنائي و التكنولوجيا الحديثة، الطبعة الأولى ، دار النهضة العربية، القاهرة مصر ، 1996.

10-جميل عبد الباقي الصغير، القانون الجنائي والانترنت ، دار النهضة العربية القاهرة، 2002.

11-جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002.

12-جميل عبد الباقي الصغير، الجوانب الإجرائية لجرائم الانترنت ، دار الفكر العربي ، القاهرة ، 20001.

13-جهاد رضا الحباشنة، الحماية الجزائية لبطاقة الوفاء، دار الثقافة، عمان الأردن، 2008.

14- خالد ممدوح إبراهيم ، الجرائم المعلوماتية، دار الكر الجامعي ، الإسكندرية مصر ، 2009 .

15- سامح محمد عبد الحكيم، الحماية الجنائية لبطاقات الائتمان، درا النهضة العربية، القاهرة مصر ، 2003.

16-سعيد عبد اللطيف حسن، "إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت"، الجرائم الواقعة في مجال تكنولوجيا المعلومات، الطبعة الأولى ، دار النهضة العربية، القاهرة مصر 1999.

17-شيماء عبد الغني محمد عطاء الله، الحماية الجنائية للمعاملات الالكترونية، دار الجامعة الجديدة، الإسكندرية مصر ، 2007.

18- عبد الحميد ثروت ، التوقيع الإلكتروني، دار الإسكندرية مصر ، 2007.

19-عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية مصر ، 2006.

20-عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الأنترنت، دار الفكر الجامعي، الإسكندرية مصر ، 2006،

21-عبد الفتاح بيومي حجازي، المبادئ الاجراءات الجنائية في جرائم الكومبيوتر والإنترنت، دار الكتب القانونية، القاهرة مصر ، 2007.

22-عبد الفتاح بيومي حجازي، التجارة الالكترونية العربية، الكتاب الأول شرح قانون المبادلات والتجارة الالكترونية التونسي، دار الفكر الجامعي، 2003.

23- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية الكتاب الثاني الحماية الجزائية لنظام التجارة الالكترونية، دار الفكر الجامعي الإسكندرية مصر ، 2002 .

24- عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت ، دار الكتب القانونية ، مصر المحلة الكبرى ، 2004.

25- علي كحلون، الجوانب القانونية لقنوات الاتصال الحديثة و التجارة الالكترونية، دار إسهامات ، تونس2002.

26-عمر سالم، الحماية الجنائية لبطاقة الوفاء، الطبعة الأولى ، دار النهضة العربية ، القاهرة مصر ، 1995.

27- عماد علي الخليل، الحماية الجزائية لبطاقة الوفاء (دراسة تحليلية مقارنة)، دار وائل للنشر عمان، الأردن، 2000.

28-عايد رجا الخلايلة ، المسؤولية التقصيرية الالكترونية ،المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب والانترنت، دار الثقافة للنشر والتوزيع ، عمان الأردن، 2009.

29- عامر محمود الكسواني ،التجارة عبر الحاسوب ، دار الثقافة للنشر والتوزيع ، عمان الأردن ، 2008 .

30-عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي (دراسة مقارنة بين التشريع الجزائري والقانون المقارن)، دار الجامعة الجديدة ، الإسكندرية ، 2010.

31- عبد الباسط خلاف ،الحماية الجنائية لوسائل الاتصال الحديثة (الحاسب الالكتروني الكمبيوتر ، الانترنت)،دار النهضة العربية ، القاهرة ، 2004.

32-علي حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت (دراسة مقارنة) عالم الكتب الحديث ،الأردن ، 2004 .

33-علي العريان ، الجرائم المعلوماتية ، الإسكندرية : دار الجامعة الجديدة للنشر الإسكندرية ، 2004.

34- عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي ، دار الجامعية للطباعة والنشر ، الإسكندرية ، 1999.

35-عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي ، الطبعة الأولى دار النهضة العربية ، القاهرة ، 2001.

36- عبد الله هلالي ، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، دار النهضة العربية،1997.

37- عبد الله هلالي ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة ، دار النهضة العربية ، القاهرة مصر ، 2006.

38-عبد الله هلالي ، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية ، دار النهضة العربية القاهرة مصر ، 2003.

39- عفيفي كامل عفيفي ، جرائم الكمبيوتر ، منشورات الحلبي الحقوقية ، بيروت لبنان ، 2000.

40- عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية(دراسة مقارنة) دار النهضة العربية ،القاهرة، 2001.

42- فهد بن سيف بن راشد الحوسني ، جرائم التجارة الالكترونية ووسائل مواجهتها ،دراسة مقارنة السحاب للنشر والتوزيع ، عمان الأردن، 2010.

43- كوثر مازوني ، الشبكة الرقمية وعلاقتها بالملكية الفكرية ، دار الجامعة الجديدة ، الإسكندرية مصر ، 2008 .

44- لورنس محمد عبيدات ، إثبات المحرر الالكتروني ، دار الثقافة للنشر والتوزيع ' عمان الأردن، 2005 .

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

46- مصطفى محمد موسى، دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، مصر 2005.

47- محمد الأمين البشري، التحقيق في الجرائم المستحثة ، جامعة نايف للعلوم الأمنية ، الرياض 2004.

48-ممدوح عبد المطلب، أدلة الصور الرقمية في الجرائم عبر الكمبيوتر، مركز شرطة دبي، 2005.

49- ممدوح محمد على مبروك ، مدي حجية التوقيع الإلكتروني في الإثبات ، دار النهضة العربية ، القاهرة 2005 .

50- محمد عبد الله أبو بكر سلامة، جرائم الكومبيوتر والانترنت (موسوعة جرائم المعلوماتية)، دار المعارف، بالإسكندرية مصر، 2006.

51-محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت ، دار النهضة العربية ، القاهرة ،2005.

52- محمد عبيد الكعبي ، الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية القاهرة مصر 2010.

53- محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، دار الفكر الجامعي الإسكندرية مصر ، 2003.

54- محمد أمين الرومي ، جرائم الكمبيوتر والانترنت ، الدار الجامعية للطباعة والنشر، الإسكندرية مصر 2004.

55- محمد أمين الشوابكة ، جرائم الحاسب والانترنت ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع ،عمان الأردن ، 2004.

56- محمد حسين منصور المسؤولية الالكترونية ، دار الجامعة الجديدة ، الإسكندرية 2003 .

57- محمد خليفة الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية 2007.

58- محمد شتا ، فكرة الحماية الجنائية لبرامج الحاسوب ، دار الجامعة الجديدة للنشر ،الإسكندرية مصر ، 2001.

59- محمد مرهج الهيتي محمد حماد ، التكنولوجيا الحديثة والقانون الجنائي الأردن ، دار الثقافة للنشر والتوزيع ، الطبعة الأولى عام 2004.

60-نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، 2005.

61-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، دار الفكر الجامعي، الإسكندرية ، 2007.

62-نعيم مغبغب، مخاطر المعلوماتية والانترنت، المخاطر على الحياة الخاصة وحمايتها، دراسة مقارنة، بدون ناشر، 1998.

63-نهلا عبد القدر مومني ، الجرائم المعلوماتية ، دار الثقافة ، عمان،2008 .

64- هشام محمد فريد ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة مصر 1992.

65-هشام محمد فريد ، الجوانب الإجرائية للجرائم المعلوماتية ، دراسة مقارنة ، مكتبة الآلات الحديثة ،أسيوط ، 1992.

66- هدى قشقوش ، الحماية الجنائية للتجارة الالكترونية عبر الانترنت(دراسة مقارنة) ، دار النهضة العربية ،القاهرة ، 2000.

67-هدى حامد قشقوش جرائم الحاسب الالكتروني في التشريع المقارن ، دار النهضة العربية القاهرة، 1999.

68- وليد الزبيري ، التجارة الالكترونية عبر الانترنت ، دار المناهج ، عمان الأردن ،2004.

ج- الرسائل الجامعية:

1- آمين أعزان ، الحماية الجنائية للتجارة الالكترونية (دراسة مقارنة)، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق كلية الحقوق جامعة عين شمس ، 2009.

2-أيمن رضا محمد أحمد، التوقع الإلكتروني، رسالة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق بجامعة عين شمس، 2010.

4- حسن بن سعيد بين سيف الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت (دراسة مقارنة) ، رسالة مقدمة لنيل درجة الدكتوراه ، جامعة عين شمس كلية الحقوق ، 2007.

3- عمر أبوبكربن يونس ، الجرائم الناشئة عن استخدام الانترنت ، رسالة دكتوراه، جامعة عين شمس ، 2004.

4-أيمن عبد الحفيظ عبد الحميد، إستراتيجية مكافحة جرائم الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه، أكاديمية الشرطة، بدون سنة طبع، ص 455.

5- نافذ ياسين محمد المدهون، النظام القانوني لحماية التجارة الالكترونية، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق ، جامعة عين شمس ، 2007.

6-محمد عبيد الكعبي ، الحماية الجنائية للتجارة الالكترونية ، رسالة دكتوراه في الحقوق جامعة القاهرة ، 2009.

7- مجراب الدوادي ، أساليب البحث والتحري الخاصة على ضوء قانون 22/06 المتضمن قانون الإجراءات الجزائية، مذكرة ماجستير، كلية الحقوق بن عكنون، الجزائر، 2011/2010، ص.134.

د- المقالات العلمية والبحوث:

1-أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني (دراسة مقارنة) المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر:اكادمية شرطة دبي مركز البحوث والدراسات رقم العدد : 1 ، من26 إلى 28 نيسان 2003 ، بدبي الإمارات العربية المتحدة.

2-الهاشمي الكسراوي،" الجريمة المعلوماتية"، مجلة القضاء والتشريع ، جويلية 2006.

3- سليمان أبو بكر ، أنواع جرائم الحاسب الآلي وكيفية ضبطها ، مجلة الشرطة ، العدد 56 ، 03 أوت 2000 م .

4-حسام كامل الاهواني ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الآلي ، مجلة العلوم القانونية ، عين شمس ، العدد 1، 2 ، 1990.

5- زهير اسكندر،"التشريع التونسي والتكنولوجيات الجديدة للمعلومات"، مجلة القضاء والتشريع ، ديسمبر 2005.

6-علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في أطار نظرية الإثبات الجنائي، مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية ، في الفترة من 26-2003/4/28 دبي.

7- محمد أبو العلا عقيدة ، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية ،المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر:اكادمية شرطة دبي ، مركز البحوث والدراسات بتاريخ 200326 نيسان دبي الإمارات العربية المتحدة.

8- يونس عرب، جرائم الكومبيوتر والإنترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002، أبو ظبي.

9-عبد الناصر محمد محمود فرغلي وعبيد المسماري ن ورقة بحث مقدمة للمؤتمر العربي لعلوم الأدلة الجنائية والطب الشرعي ، الإثبات الجنائي بالنادلة الرقمية من الناحيتين القانونية والفنية (دراسة تطبيقية مقارنة ، الرياض، المنعقد في الفترة 12-2007/11/14.

10-عماد بوخريص وحسنى غديره ، جرائم الإعلامية ، ملتقى جهري بمحكمة الاستئناف بسوسة 2 جوان 2001.

11- محمد الأمين البشري، الأدلة الجنائية الرقمية، المجلة العربية للدراسات الأمنية والتدريب، المجلد17 العدد33.

12- ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، أنموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر ، منشور ضمن أعمال مؤتمر " الأعمال المصرفية والالكترونية " نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي ، في الفترة من 10-12/5/ 2003 .

13- محمد أمين البشرى ، التحقيق في جرائم الحاسب الآلي: دراسة مقدمة إلى المؤتمر الذي عقدته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في موضوع "القانون والكمبيوتر

والإنترنت"، العين في الفترة من 1-3 مايو سنة محمد أبو العلا عقيدة ، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية ،المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر :اكادمية شرطة دبي ، مركز البحوث والدراسات بتاريخ 200326 نيسان دبي – الإمارات العربية المتحدة.

14- يونس عرب، جرائم الكومبيوتر والإنترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي أبوظبي الامارات 2002.

15- محمد رايس ، الحماية الجنائية للسند الالكتروني ، مجلة الدراسات القانونية العدد الأول 2006-2007.

16- محمد رايس ، حجية الإثبات بالتوقيع الالكتروني طبقا لقواعد القانون المدني الجديد محاضرات ألقيت على طلبة ماجستير –مسؤولية مهنية- كلية الحقوق جامعة تلمسان ، 2009.

17- عمر الفاروق الحسيني ، تأملات في بعض صور الحماية القانونية لنظم الحاسب الآلي بحث مقدم لمؤتمر الحاسب الالكتروني ، القاهرة ، ماي 1991.

هـ- النصوص القانونيـة :

1-النصوص القانونية الوطنية :

-النصوص التشريعية :

1- القانون رقم 14/04 الموافق لـ 10نوفمبر 2004 م المعدل والمتمم للأمر رقم 66 /155 الموافق 8يونيو سنة 1966م المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية للجمهورية الجزائرية العدد 71 الموافق لـ 10 نوفمبر 2004 .

2- القانون رقم 15/04 الموافق لـ 10نوفمبر 2004 ، المعدل والمتمم للأمر رقم 66 /156 الموافق لـ8يونيو سنة 1966م المتضمن قانون العقوبات ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 71، الموافق لـ 10 نوفمبر 2004

3- القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 155/66 الموافق ل 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 84 صادرة في 24 ديسمبر 20006.

4-القانون رقم 22/06المؤرخ في 20 ديسمبر2006 ، المعدل والمتمم للأمر رقم 66 /156 الموافق لـ8يونيو سنة 1966م المتضمن قانون العقوبات. ج .ر . عدد 84 صادرة في 24 ديسمبر 2006.

- القانون رقم القانون رقم23/06المؤرخ في 20 ديسمبر2006 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات ج ر عدد 84 صادرة في 23 ديسمبر 2006.

5- القانون رقم 04/09 المؤرخ في 5 أوت 2009 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ، ج.ر.عدد 47 الصادرة في 16 أوت لسنة 2009.

5- الأمر رقم 66 /155 الموافق لـ 8يونيو سنة 1966، المتضمن قانون الإجراءات الجزائية الجزائري ، ج.ر صادرة في 1966.

6- الأمر رقم 66 /156 الموافق لـ 8يونيو سنة ،المتضمن قانون العقوبات الجزائري، ج.ر صادرة في 1966 .

النصوص التنظيمية :

7-المرسوم التنفيذي 2000-307 المؤرخ في 14 أكتوبر سنة 2000، يعدل المرسوم التنفيذي 98-257 المؤرخ في 25 أوت 1998 الذي يضبط شروط وكيفيان إقامة خدمات الانترنت، الجريدة الرسمية عدد 60 لسنة

8-المرسوم التنفيذي 98-257 المؤرخ في 25 أوت 1998، الذي يضبط شروط وكيفيات إقامة خدمات الانترنت، واستغلالها، والمعدل بموجب المرسوم التنفيذي 2000-307 المؤرخ في 14 أكتوبر سنة 2000.

- المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006 ، والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق،ج ر 63 مؤرخة في 10/08/ 2006.

ب- النصوص القانونية الأجنبية :

1- القانون رقم 95 لسنة 1996 المعدل لقانون رقم 58 لسنة 1937 المتضمن قانون العقوبات المصري .

2-قانون 15رقم لسنة 2004 ناعة تكنولوجيا المعلومات بجمهورية مصر العربية .

3-القانون ا عدد 89 لسنة 1999 المؤرخ في 2 أوت 1999المتعلق بجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و المعدل لقانون العقوبات التونسي .

4-القانون عدد83 لسنة 2000 المؤرخ في 9 أوت 2000 المتعلق بالمبادلات والتجارة. الالكترونية التونسي .

5-القانون عدد 63 لسنة 2004 المؤرخ في 27 جويلية 2004 المتعلق بحماية المعطيات الشخصية المعدل لقانون العقوبات التونسي .

6-القانون الأردني رقم 85 لسنة 2001 الخاص بالتعاملات الالكترونية.

7-القانون البحريني الصادر بتاريخ 14 سبتمبر 2002 المتضمن الجارة الالكترونية. 8- قانون رقم 2 لسنة 2002 المتضمن قانون التجارة الإلكترونية لإمارة دبي .

9 - القانون الفرنسي رقم 17 – 78 الصادر في 06 جانفي 1978 المتعلق المعلوماتية والحريات

10-القانون الفرنسي رقم 1382/91 الصادر في 30 ديسمبر 1991 ، والخاص بنشاط و رقابة مؤسسات الائتمان.

11-القانون الفرنسي رقم 719 /2000 الصادر بتاريخ 01أوت المتعلق بتعديل أحكام القانون المتعلق بحرية الاتصالات رقم 1067 /86 الصادر بتاريخ 30 أيلول 1986.

12- القانون الصادر في سنة 1994 المتضمن قانون العقوبات الفرنسي الجديد .

13-القانون الألماني الصادر 10أوت 1997، المتضمن الأعمال التقنية الوسيطة في مجال الانترنت.

- القانون الانجليزي الصادر في سنة 1999 المتضمن إساءة استخدام الحاسوب .

15-القانون الأمريكي الصادر سنة 1984 المعدل في سنة 1996 ،المتعلق بجرائم الحاسوب .

16–التوجيه الأُوروبي بالإجماع في 8 حزيران 2000م التوجيه رقم 2000/31، والمتضمن الأوجه القانونية لخدمات شركات المعلومات.

17 – تقرير قسم التقارير والدراسات بمجلس الدولة في شأن الانترنت والخطوط الرقمية والذي وافقت عليه الجمعية العمومية للمجلس في 02 جويلية 1998.

ثانيا : المراجع باللغة الأجنبية :

1_ باللغة الفرنسية:

A -OUVRAGES :

-GENERAUX

1- ALAIN HOLLANDE –(X), pratique du droit d'informatique ,4eme édition Delmas, paris 1998.

2-ATIAS (Christian) .La protection Penale de la vie privee.

XII emees Journees de I'Association française de droit pénal en hommage au doyen Fernard BOULAN (Aix-en-Provence, 17-19 mars 1994), Presses universitaires d'Aix-marseille, 1994, p. 87-103.

3-Ali Ahmed rached : « De l'intime conviction du juge vers une théorie scientifique de la preuve en matière criminelle, éd. Pedone, Paris 1942.
4-AVAN (D) , Guide juridique de l'informatique, Paris, Bordas, 1999.

5- BERTRAND (A) , Le droit d'auteur et les droit voisins, DALLOZ DELTA 1999.

6-BECOURT (Daniel. La personne face aux medias, Gayette du palais, no.254, 6 sept. 1994.

7-Chevallier Jean Yves : «Rapport de Synthèse pour les pays d'Europe Continentale, la preuve en procédure en pénale comparé», Association internationale de droit pénal, R.I.D.P, 1992.

8-Chamoux (F), « la loi sur la fraude informatique de nouvelle**s** incriminations », JC P édition Générale, Doctrine, 1988, n 3321.

9-Cass.crim. 5 janv.1994, p.1994, JC éd. Entreprise, I, 359.ob. vivant et les tanc.

10-CHAMOUX (F), la loi sur la fraude informatique de nouvelles incriminations, JCP, éd. .Doctrine

11-Cabrillac (M) et Mouly (Ch) , Droit pénal de de la banaue et du crédit, Masson, paris, 1982 ..-Gassin ®. la protection pénale d'une nouvelle universalité de fait en droit français : le système de traitement automatisé des données, Dalloz 1989, 4ème cahier, .

12-cyrilrojinsky.commerce électronique et responsabilité des acteurs de l'internet Europe www.droit-technologie.or

13 - DAVIO (E) , internet face au droit ,cohiers du C.R.I.D 12 é d . story – scientica, 1997, P. 80- Encyclopédie juridique, DALLOZ ,2émé ,édition , 1976.

14- Encyclopédie juridique , DALLOZ ,2émé ,édition , 1976.

15- E.Carprishi, le juge et la preuve électronique.

16- FOEX (Raymound A.)La loi federale sur la protection de la vie privee du 23 mars 1979 revue penale suisse, no. 1, 1982.

17-Gassin ®. la protection pénale d'une nouvelle universalité de fait en droit français : le système de traitement automatisé des données, Dalloz 1989, 4ème cahier.

18-Gorphe François : « Les décisions de justice », étude psychologique et judiciaire, Paris, Sirey, Presses universitaires de France, 1952.

19- Laure Rassat (M) , Droit Pénal spécial, Dalloz , paris.

20- Rose (Ph), la crinimelité informatique, é 2eme edition DAHLAB 1988.

21-De Lassalle (G), "Microsoft se plain du pritage de ses logiciel, 03/05/2001 .WWW.AFRIK.COM

22 - Larguier (J) ,Droit pénal spécial , Dalloz , 2eme édition , paris 1998.

23- LECLERCQ (Jean).Preuve et signature electroniques de la loi du 13 mars 2000 au decret du 30 mars 2001.

24- MARCO (Estelle De).Le Droit Penal Applicable sur Internet, Memoire de D.E.A. Informatique et Droit Sous La direction de Monisieur le 11professeur Michel Vivant, Universite de Montpellier 1 Institut de Recherches et d'Etudes pour le Traitement de l'Information juridique, 1998 www.juriscom.net/universite/memoire6/penal/html.

25-Michel VIVANT et autres, Droit de l'informatique et des resèques,1833.

26- PIETTE-COUDOL (Thierry) / BERTRAND (Andre). Internet et la loi, Dalloz, 1997

27- TI MUNICH, 28 mai 1998, Aff. "Compuserve" in P. Coëtlogon, cite par P. KOCH, "Le régime de responsabilité des fournisseurs d´accès et d´hébergement sur internet en droit Allemand", Légipresse, décembre, 1999, chronique

B- articles :

1-Deveze *(J),* « *Atteinte au système automatisé des données* », jurisclasseur pénal 1997 PE3/294

2- Didier(J), « Les Truquages et usages Frauduleux des cartes magnétiques »JCP. Ed.G,I, 1986, n 3229.

3-kaspersen (H.W.K) : Computer crimes and others crimes aganiste information technology in the Netherlands. Rev. int. dr.pen. 1993

4- Luc GRYNBAUM, "LCEN. Une immunité relative des prestataires de services Internet", Communication- Commerce électronique, Études, Septembre 2004, nº 28.

5- Meunier (C.): La loi du 28 Nov. 2000 relative a la criminalité informatique. Rev. Dr. Pen. Crime. 2002.

6- Motherncblager (M.), Rapp. Prec. Rev. int. dr. pen.1993

7-Rodrigues(A),le droit portugais, la preuve en procédure pénal comparé comparée, association internationale de droit penalR,I,D,.1992.

8-Podovo(Y.) : unapercu de la lutte contre la cybercriminalité en France. R.S.C. 2002,. Spec.

9- PELLETIER (Herve) .Atteinte a la vie privee, Art. 226-1 a 226-3, JurisClasseur Penal, 1994.

2- باللغة الانجليزية :

1-ABA Section Creates First Digital Signature Guidelines– To Aid In Security of The Internet, 1996.

2-christen sagarlataand David j. byre, the electronic paper trail: evidentiary, journal of science and technology lqz. 22september 1998.

3- Draft of a Law on the Framework Conditions for Electronic– Signatures and to Amend Other Regulations. (In the Version decided by the Cabinet on 16 August 2000).

4- Electronic– Patient Management, About TERP 2003: www.medrecinst.com/index.about.shtml.

5-Electronic Records and Signatures in Healthcare and the– Interplay of E-Sign, HIPAA and UETA, 2001.

Www.diffuse.org/commerce.

6-Gordon huges, Essqys on computer crime-London : Longman professional,1995.

7- GIBBS (Jffrey N.) And MAZAN (kate– Duffy), Electronic signatures: Understanding FDA's Electronic Records and Signatures Regulation, Medical Device & Diagnostic Industry Magazine, may 1999.

Www.devicelink.com/mddi/archive/99/05/009.

8- Guide the Electronic Commerce Regulation, 2002

www.diffuse.org/commerce.

9-Johannes f .nijboerm challenges for the law of Evidence Leiden: INRE,P, 1999..

10-PASKIN (Xan) / SCHALDACH-PAVIA (Jeannie, Computer crimes, American Criminal Law Review, 1996, Vol. 33.

11-Report to the Governor and Legislature on New York States Electronic Signatures and Records Act

12-Report to the Governor and Legislature on New York State's Electronic Signatures and Records Act.

13-Gordon huges, Essqys on computer crime-London :

Longman professional,1995.

الفـهـرس

الفهـرس

الباب الثاني

مدى كفاية الحماية الجنائية الإجرائية للتجارة الالكترونية

الملخص :

لقد نتج عن طهور تكنولوجيا المعلومات ما يسمى بالتجارة الالكترونية سواء على مستوى الأفراد أو الشركات أو الدول، وأصبحت التجارة الالكترونية تحتل أهمية كبيرة لمزاياها العديدة والمتنوعة، أهمها سهولة انجاز العمليات التجارية و تنوع و توسع نطاق الأسواق.

وترتب عن الأهمية المتزايدة للتجارة الالكترونية عدة مشاكل قانونية أخطرها الجريمة المعلوماتية على نحو يهدد التنمية الاقتصادية، مما أدى إلى ضرورة توفير حماية جنائية للتجارة الالكترونية.

وعليه اتجهت العديد من الدول و منها الجزائر إلى توفير حماية جنائية موضوعية و إجرائية للتجارة الالكترونية سواء في إطار نصوص عامة أم في نصوص خاصة بالتجارة الالكترونية.

Résumé :

Le progrès de la technologie informatique à fait apparition ce qu'en appelle le commerce électronique sur au niveau des individus ou des sociétés ou des Etats, cette dernière est devenue très important car il à plusieurs avantages telque, l a facilité de réalisation des opérations commerciales et l'Elargissement des marchés.

L'importance du commerce électronique à engendré beaucoup de problème juridiques ainsi que le crime électronique qui menace le développement économique.

Il est nécessaire d'introduire une protection pénal ce, ci. A partir de là les Etats a pris la procédure de protégé pénalement ce domaine objectivement et procédurement ainsi dans les textes générales ou spéciales, l'Algérie.

ABSTARCT :

After the apparisation of preformation technology causes the electronique commerce (trade) different levels : individu or societes or states (country) become importance for their a vantages : facilities easy un the realisation commercial operations and widen of markets.

It's importance baby many problems juridique, which menace the development economique such as : the electronic crimes.

It's necessary to protect this commerce by penal law (penal act). Starte such as Algeria takes procedure to protect this domain by genel or special texts.