الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة ابن خلدون – تيارت
كلية الحقوق والعلوم السياسية
قسم الحقوق

الحماية الجنائية للتوقيع الالكتروني دراسة مقارنة

أطروحة لنيل شهادة دكتوراه طور الثالث

تخصص : التجريم في قانون الأعمال

إعداد الطالبة:

- ترجمان نسيمة

تحت إشراف الأستاذ:

- أ.د: مداح حاج علي

أعضاء اللجنة المناقشة

أعضاء اللجنة	الرتبة	جامعة	الصفة
أ.د. بوشي يوسف	أستاذ التعليم العالي	جامعة ابن خلدون تيارت	رئيسا
أ.د مداح حاج علي	أستاذ التعليم العالي	جامعة ابن خلدون تيارت	مشرفا ومقررا
د. بلاق محمد	أستاذ محاضر "أ"	جامعة ابن خلدون تيارت	عضوا مناقشا
د. قايد ليلى	أستاذ محاضر "أ"	جامعة ابن خلدون تيارت	عضوا مناقشا
د. بوصوار ميسوم	أستاذ محاضر "أ"	جامعة يحي فارس المدية	عضوا مناقشا
د. بن عيسى أحمد	أستاذ محاضر "أ"	جامعة مولاي طاهر سعيدة	عضوا مناقشا

السنة الجامعية: 2021/2020


بسم الله الرحمن الرحيم

شكر وعـــرفان

فبعد شكرنا لله عزوجل خير المتوكل عليه ،لايسعنا في هذا المقام إلا توجيه اسمي عبارات الشكروالتقديروالامتنان إلى الأستاذ الدكتور مداح حاج علي لتفضله بالإشراف على هذه المذكرة ،نسال الله له التوفيق والعطاء وجزاه الله كل خير.

كما أتقدم بالشكروالامتنان للأساتذة الأفاضل رئيس وأعضاء لجنة المناقشة لتفضلهم بقبول مناقشة هذه الرسالة ،داعين لهم بالتوفيق في خدمة العلم وكل من ساهم من قريب أو بعيد في إنجازهذه الرسالة

إهـــــداء

أحمد الله عزوجل أن وفقني لإتمام هذا البحث بغيرمني

ولا قوة ،فلله الحمد والمنة.....

.إلى روح والدي الطاهرة ،تغمده الله برحمته الواسعة وأسكنه فسيح جنانه وجعل قبره روضة من رياض الجنة

.إلى والدتي الكريمة حفظها الله وأطال في عمرها وأرضاها عني في الدنيا والآخرة

إلى رفيق دربي الذي صبرمعي وشجعني وأمدني بروح القوة والتحدي زوجي الفاضل

إلىإخوتي وأخواتي أطال الله بعمرهم وحفظهم

إلى والدي الثاني العزيزوالغالي الذي رافقني طوال مشواري الدراسي أطال الله بعمره وحفظه ورعاه بن عابد عمار

إلى كل أفراد عائلتي

إلى كل أساتذتي طوال مسيرتي الدراسية

إلى كل طالب وباحث كل في مجال تخصصه

إلى كل هؤلاء أهدي هذا العمل المتواضع

قائمة المختصرات

1- باللغة العربية:

ص:	صفحة
ج ر:	الجريدة الرسمية
ق.ع .ج :	قانون العقوبات الجزائري
ق.إ.ج.ج:	قانون الإجراءات الجزائية الجزائري
ق .م.ج:	قانون المدني الجزائري
ق.ع.م :	قانون العقوبات المصري
ق.ع.ف:	قانون العقوبات الفرنسي
ط:	طبعة
ج:	الجزء
د.ت.ن:	دون تاريخ نشر
دج:	دينار جزائري
الو.م.أ:	الولايات المتحدة الأمريكية

2- باللغة الأجنبية:

Art :	Article
N° :	Numéro
P.L :	Public law
Sec :	Section
P :	page
Ed :	édition
Op.cit :	ouvrage précité
Rev :	Revue

مقدمة

مقدمة:

شهد العالم ثورة هائلة في مجال تقنية المعلومات والاتصالات التي أثرت في شتى أوجه الحياة والعلوم والميادين، وعلى كافة القطاعات الاقتصادية، الاجتماعية، السياسية، التعليمية، الأمنية وغيرها من القطاعات المختلفة بما في ذلك قواعد ونظم المعلومات والشبكات.

فإلى وقت قريب كانت المعاملات اليومية للأشخاص تتميز بالوضوح والدقة والتحديد في مضمونها ومحتواها إلى جانب توفر قدر من الأمان والثقة اتجاهها، ويعود السبب في ذلك إلى الطريقة التي كانت يتم بها تحرير تلك المعاملات، حيث تكتب في محررات ورقية يمكن الرجوع إليها كلما تطلبت الحاجة، وبالتالي لم يكن من اليسير إنكارها أو تغيير محتواها، ولم يكن الأمر يقتصر على توثيق تلك المحررات، وإنما يتم تذييلها بتوقيع أصحاب الشأن (الأطراف المتعاملة) عليها بما يفيد الإقرار بصحة مضمونها ومحتواها وصدورها ممن وقعها، أما في الوقت الراهن وبظهور التطورات التكنولوجية التي تمثلت في ظهور شبكة المعلومات (الانترنت) جعلت العالم يتحول إلى قرية صغيرة، وقلصت المسافات الجغرافية بين الأفراد.

فمنذ ظهور هذه الآلية الذكية والناس في كافة دول العالم تتطلع إليها وتقدم على استخدامها كنافدة يطل منها مستخدميها على العالم كله ويتعرفون من خلالها على ما يجري حولهم من أحداث، ويمارسون نشاطاتهم وتصرفاتهم دون ترحال، إذ بواسطتها تم كسر حواجز المكان والزمان، فهي تصل الأشخاص ببعضهم البعض في ثوان معدودة بل في أجزاء من الثانية في بعض الأحيان.

فقد واكب شيوع استخدام تكنولوجيا التقنيات الحديثة في إبرام التصرفات القانونية عدة تغييرات في كثير من المفاهيم القانونية كمفهوم الكتابة والتوقيع والمحرر، فبينما كانت هذه التصرفات تنشأ بواسطة الكتابة التقليدية (الخطية) وتوقع بواسطة أحد أشكال التوقيع التقليدي على وسيط مادي محسوس (ورقي)،أصبحت الآن تنشأ بواسطة تقنيات حديثة تتألف من كتابة إلكترونية وتوقع إلكترونيا على وسيط غير مادي وغير محسوس عن طريق إدخال المعلومات بطريقة رقمية وتخزينها لبيانات إلكترونية في جهاز الحاسب الآلي نفسه،أو على أقراص (cd)أو أقراص مدمجة بذاكرة (CD ROMS) وعملية التخزين قد تكون بصورة دائمة أو لفترة ومنه يمكن لأصحاب الشأن الرجوع إلى ما تم كتابته وقراءته بشكل واضح.

كما وأصبح التعاقد بين الأطراف من مختلف أنحاء العالم ممكنا وذلك دون التقاء أطرافه عبر فضاء افتراضي لا مادي، حيث يتواصل البائع مع المشتري عبر هذه الشبكة فيتم تبادل المعلومات والبيانات الخاصة بالعقد بينهما بدءا بتكوينه إلى غاية تنفيذه في إطار ما يسمى بالتجارة الالكترونية التي أصبحت

من التطورات الجديدة في مجال الأعمال إذ تستخدم تطبيقات التكنولوجيا الحديثة للمعلومات والاتصالات بين الشركات والمؤسسات وعملائها وكذا الشركات والهيئات العامة للدولة وذلك بهدف رع القدرة على انجاز الأعمال التجارية والحكومية، ولكي يمكن إبرام تلك المعاملات التجارية وأن تكون لها الحجية القانونية وأن تستوفي كافة عناصر بقائها واستمرارها ولكي يمكن ضمان حقوق المؤسسات والأفراد والهيئات المتعاملة بها لا بدى من وجود آلية تثبت الحقوق والالتزامات ، وأن تتلاءم مع الشكل الالكتروني لهذه المعاملات، إذا وجب استخدام المحررات والتوقيعات في الشكل الالكتروني.

ونظرا لأهمية هذه العناصر في إبرام التصرفات التي يتم عن طريق الوسائط الحديثة خاصة تلك التي تتم عن طريق شبكة الانترنت وتشجيعا للتجارة الالكترونية فقد تظافرت الجهود على الصعيد الدولي والإقليمي والوطني لإصدار تشريعات وأحكام قانونية تقر وتعترف بحجية هذه الأشكال المبتكرة ومن أهم التشريعات التي صدرت في هذا الشأن: القوانين النموذجية كقانون أونسترال النموذجي للتوقيع الالكتروني، التوجيه الأوروبي بشأن التوقيعات الالكترونية وكذا أبرمت المعاهدات كمعاهدة بودابست وغيرها، وأصدرت القوانين الداخلية في معظم دول العالم.

فالجزائر وكغيرها من دول العالم سعت هي الأخرى إلى الاستفادة من تكنولوجيات الإعلام والاتصال والعمل على الانتشار الواسع لاستعمال الحاسوب وشبكة الانترنت في شتى المجالات، وهو ما يترجم اتجاه الجزائر نحو توفير متطلبات الحكومة الإلكترونية و التجارة الإلكترونية رغم مايفرضه ذلك من تحديات كبيرة لتأمين هذا الفضاء من مختلف أشكال الاعتداءات الإلكترونية ،فقد اصدر المشرع الجزائري قانون رقم 04/15 المؤرخ في 2015/02/01[1] المحدد القواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين الذي حاول من خلاله وضع البنية القانونية لتوقيع الإلكتروني و كذلك بث الثقة فيه عن طريق وضع نظم المصادقة عليه من أجل التأكد من صحته مع فرض الجزاءات والمسؤوليات في حالة عدم مراعاتها.

فإذا كانت الثورة المعلوماتية التي جاء بها الحاسب الآلي إيجابيات وقدرتها على تغيير أوجه الحياة إلى الأحسن و الأفضل إلا أنها تحمل في طياتها أيضا جوانب مظلمة أفرزتها الاستعمالات غير المشروعة لنظم الحاسب الآلي مرورا بالمحررات الالكترونية وسيئاته،وفي مجال التوقيع الإلكتروني و نظرا لتوغله في

[1]- القانون: رقم 15-04 المؤرخ في 2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج ر، رقم 06 المؤرخة في: 2015/02/10.

معاملات البشر و الهيئات الحكومية و الخاصة، وترتيب الثقة في المعاملات بين الناس على مدى أحكام منظومته القانونية و الفنية و بما أن معاملات الإلكترونية و بالخصوص التجارة الإلكترونية تتم في بيئة افتراضية مملوءة بالمخاطر المتعلقة بانتحال هوية أطراف التصرف الإلكتروني،واختراق بياناتهم المتداولة و إنكار عملية الشراء و البيع و التبادل أو دفع قيمة مستحقات مختلف السلع و الخدمات عبر الانترنت ، بعدما كان الاعتداء على الأموال يتم بواسطة السرقة التقليدية أو النصب ،أصبحت هذه الأموال يعتدي عليها عن طريق اختراق شبكات معلوماتية دون الحاجة إلى المساس بأي وثائق أو محررات ورقية،بإضافة إلى قرصنة المواقع الإلكترونية و أنظمة المعالجة الآلية للمعطيات و قواعد البيانات سواء المتعلقة بالأفراد أو المؤسسات الدولية وكذا عمليات الاحتيال و الإطلاع على المعلومات السرية و الاستفادة منها و العبث بها عن طريق حذفها أو تعديلها أو تعطيل الوصول إليها.

لذا كان لزاما على جل التشريعات سواء العربية منها أو الغربية وضع ترسانة قانونية لحماية المصالح المهمة بمنظومة التوقيع الإلكتروني ، من خلال تجريم الأفعال الماسة به و فرض جزاءات على مرتكبي هذه الاعتداءات خاصة و أن الجناة في هذه الجرائم يتسمون بخبرة التي تمكنهم من تطويع تقنية الحاسب الآلي الذي أضاف الكثير لقدرات الإنسان بمنحه إمكانية الاحتفاظ بكم هائل من المعلومات إلى جانب معالجتها بسرعة فائقة للقيام بأعمال إجرامية لم تكن معروفة من قبل ، فلجريمة اليوم ليست كجريمة الأمس،فلمجرم بات يعمل قبل إقدامه على نشاطه الإجرامي بالتفكير في أسلوب لايترك أثار مادية تدل عليه.

لهذا كان من الضروري مواكبة هذا التطور و إدخال وسائل حديثة في عملية اكتشاف هذه الجرائم،لذا حاولت أجهزة البحث و التحقيق الاستعانة بالوسائل الحديثة في إثبات الجريمة لعلها تفك الخيوط المتشابكة للواقعة الإجرامية التي من الصعب الكشف عن مرتكبيها ، فيما إذا اعتمدنا فقط على الوسائل التقليدية التي هي عادة أقل فعالية مقارنة بوسائل ارتكاب الجرائم ،هذا من جهة، و من جهة أخرى فإن النيابة و القضاء أيضا يجدون أنفسهم يتعاملون مع نوعية جديدة من الأدلة في مجال الإثبات الجنائي ومن ثم تتولد العديد من المشكلات الإجرائية المتعلقة بكيفية تقديم الدليل الإلكتروني ومصداقيته و حجيته التي تستلزم وضع آليات قانونية و فنية لتعامل معها و استخلاص النتائج الذي توصل إلى الجناة في هذه الجرائم ، غير أنالأمر لا يتوقف عند هذا الحد فمن الضروري تتبع الدعوى الجنائية وصولا إلى إنزال العقاب وهو مايستلزم تحديد القانون الواجب التطبيق على تلك الجرائم.

كما وتبدو المشكلات الإجرائية في مجال جرائم التوقيع الإلكتروني لتعلقها في كثير من الأحيان ببيانات معالجة إلكترونيا وكيانات منطقية غير مادية مخزنة في شبكات إلكترونية موجودة في الخارج تثير مسألة الدخول إليها أو محاولة جمعها أو تحويلها إلى الدولة التي يجرى فيها التحقيق مشكلات تتعلق بسيادة الدولة او الدول الأخرى التي يوجد لديها هذه البيانات وفي هذه الحالة يحتاج الأمر إلى تعاون دولي في مجال البحث و التفتيش و التحقيق وجمع الأدلة و تسليم المجرمين بل و تنفيذ الأحكام الأجنبية الصادرة في هذا المجال .

كما و يعتبر تحديد القضاء المختص للنظر في جرائم الاعتداء على التوقيع الإلكتروني من أهم الصعوبات الحديثة التي أسفر عنها التعامل التقني للحاسب الإلكتروني عن بعد ، ويرجع السبب في ذلك إلى أن تعقد شبكة الانترنت وتنوع طرق استخدامها لايسمح بتحديد مكان ارتكاب الجريمة الذي يمر عبر عدة دول بنفس الوقت ،مما يؤدي إلى صعوبة تحديد المحكمة الجنائية المختصة بنظر ففعل الاعتداء ومن جهة أخرى تعد جرائم التوقيع الإلكتروني من الجرائم العالمية العابرة للحدود تتميز بخاصية عدم الاعتراف بالحدود الجغرافية كما أنها تتحرك في فضاء شبكي يصعب معه ملاحقة المجرمين مما يفرض حتمية تعاون دولي حقيقي وفعال على جميع الأصعدة سواء على مستوى التجريم أو العقاب أو على مستوى الإجراءات ناهيك عن تطوير آليات الملاحقة القضائية الوطنية و الدولية من خلال إحداث مؤسسات متخصصة مثل الانتربول و المحكمة الجنائية الدولية المتخصصة، و تطبيق القواعد الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية ووضع ترتيبات ضمن التشريعات و القوانين الوطنية لتحقيق أقصى حد ممكن من التعاون مع الدول الأخرى لغرض تسهيل التحقيق أو الإجراءات المتعلقة بجرائم التوقيع الإلكتروني.

فالتوقيع الالكتروني له أهمية كبيرة في كافة المعاملات القانونية سواء أكانت مدنية أو تجارية فقد كانت البدايات الأولى لظهورها بمناسبة عمليات الدفع الالكتروني لدى البنوك والمصارف، ولا يزال هذا المجال تطبيقا خصبا لاستخدام التوقيع الالكتروني لاسيما مع توسع أعمال الصرافة والبنوك الالكترونية.

كما أن لهذا الموضوع قدرا من التداخل بينه وبين التجار الالكترونية فإذا كان قوام هذه التجارة هي تبادل السلع والخدمات، فإن هذا التبادل لا يعدد أن يكون في حقيقة الأمر عقدا يستجمع كافة شروطه القانونية من إيجاب وقبول ويقترن بتوقيع ينسب إلى صاحبه ويرتب أثاره القانونية.

ومن ثم فإن الاعتداء على التوقيع الالكتروني من شأنه المساس بالثقة والأمان في المعاملات التي تكون التجارة الالكترونية محلا لها.

كما ويعتبر موضوع الحماية الجنائية لتوقيع الالكتروني بالغ الأهمية سواء من الناحية النظرية كونه يعالج جرائم الاعتداء على التوقيع الالكتروني من حيث القواعد العامة أو في النصوص الخاصة.

من خلال بيان السلوكات والأفعال الجنائية التي ترتكب ضد الآخرين بواسطة الحاسب الالكتروني ومن خلال شبكة الانترنت لوضع ضوابط قانونية وقضائية لتعامل معها وردع مرتكبيها.

وتبدو أهمية البحث في أنه يدم أسلوبا عمليا وقانونيا يبين كيفية إثبات جرائم التوقيع الالكتروني التي تتم عبر أجهزة الكمبيوتر.

تتضح الأهمية العملية لدراسة من خلال التأكيد على ضرورة اكتساب رجل الضبط القضائي لمهارات فنية وتقنية مختلفة مع ضرورة الاستعانة بخبراء استشاريين في مجال جرائم التوقيع الالكتروني، حيث أنه لابد من توافر الخبرة والمهارات التقنية لكشف الأدلة الناتجة عن هذه الجرائم وأيضا إلى لفت انتباه المعنيين والمسؤولين عن الأجهزة والتنظيمات والمؤسسات العلمية للمساهمة في مكافحتها والحد منها والتحذير من مخاطرها.

ومن الناحية التطبيقية تبدوا أهمية هذه الدراسة في إيضاح قصور قانون العقوبات والإجراءات الجنائية الحالي في مواجهة الجرائم المتعلقة بتوقيع الالكتروني ولذلك لابد من البحث عن وسائل تكميلية لجزاءات الجنائية لتحقيق الحماية التقنية والحماية القانونية عن طريق القضاء.

كانت أسباب اختياري لهذا الموضوع في ضوء بعدين موضوعي و ذاتي ،الأسباب الذاتية ترجع إلى الشعور بأهمية و ضرورة البحث في هذا الموضوع و الطموح العلمي الذي يدفع باتجاه تقصي الجديد في ميدان القانون الجنائي للأعمال ،و الرغبة في المساهمة ولو بشكل محدود في إثراء النقاش القانوني في مثل هذه المواضيع.

أما الأسباب الموضوعية فتمحورت جول الحداثة القانونية و التشريعية للحماية الجنائية للتوقيع الإلكتروني ،مما يدفع نحو البحث في مدى انسجام النصوص القانونية لهذه المنظومة مع المستجدات الراهنة في مجال المعاملات ا إلكترونية خاصة في ضل أهمية التوقيع ا إلكتروني و أهمية المصادقة على هذا التوقيع بما يضفي عليه حجية في الإثبات فضلا عن وسائل الحماية الجنائية المعتمدة من قبل المشرع لمواجهة جرائم التوقيع الإلكتروني.

تهدف هذه الدراسة إلى محاولة الوصول إلىإستراتيجية متكاملة على المستوى التشريعي والتقني والأمني لمكافحة جرائم التوقيع الالكتروني فمن ناحية تعمل على إيجادإستراتيجية مكملة للقوانين الجنائية الموضوعية والإجرائية لمواجهة هذه الجرائم. وكذا تحديث الآليات التقليدية التي لا تكفي على المستوى الجنائي الإجرائي الدولي وحتى تتواكب مع التطور التقني في شبكات الاتصال وتحديد وسائل التحقيق، إضافة إلى تفعيل التعاون الدولي مجال مكافحة جرائم التوقيع الالكتروني.

لقد كان لهذا الموضوع دراسات سابقة تمثلت في دراسات عربية و أخرى وطنية تمثلت فيما يلي ،الدراسات الوطنية في :الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة لصالح شنين وهو بحث مقدم للحصول على شهادة الدكتورة في القانون الخاص بكلية الحقوق و العلوم السياسية جامعة أبو بكر بلقايد تلمسان 2012-2013 بإضافة إلى دراسة أخرى تمثلت في الحماية الجنائية للتوقيع و التصديق الإلكترونيين في التشريع الجزائري لعزيزة لرقط ،وهي ورقة بحثية منشورة على شكل مقال في مجلة الاجتهاد لدراسات القانونية و الاقتصادية بالمركز الجامعي لتمنراست عدد 11 جانفي 2017،أما الدراسات العربية فتمثلت في القواعد الخاصة بالتوقيع الإلكتروني لعيسى الربضي وهي رسالة مقدمة لنيل شهادة الدكتورة في الحقوق بجامعة عين شمس القاهرة ،مصر 2011 ،إضافة إلى الحماية الجنائية للتوقيع الالكتروني 'لأيمن رمضان أحمد وهي رسالة مقدمة لنيل شهادة الدكتورة في الحقوق بجامعة عين شمس القاهرة ،مصر سنة 2010. ومايميز دراستي عن كل الدراسات السابقة اولا انها دراسة مقارنة تمحورت حول بيان نوع الحماية المقررة لمنظومة التوقيع الالكتروني في جل التشريعات سواء العربية او الغربية و كذا بيان موقف التشريع الجزائري اتجاه جرائم التوقيع الالكتروني من تجريم و عقاب و كذا بيان خصوصية اجراءات البحث و التحري وصولا الى انزال العقاب على الجاني

نظرا لأهمية التوقيع الإلكتروني في المعاملات المدنية عموما و التجارية خصوصا و بالأخص فيما يتعلق بموضوع الحماية الجنائية التي أولاها المشرع لهذا الإجراء القانوني وعن هذه المشكلة يمكن أن نتساءل كالآتي :

ما مدى فعالية الحماية التي أقرها كل من التشريع الجزائري و التشريع المقارن للتوقيع الالكتروني؟

كما وأن البحث في موضوع الحماية الجنائية للتوقيع الالكتروني قد واجهته صعوبات كثيرة فمن ناحية فإن تناول المشرع الجزائري للحماية الجنائية لتوقيع الالكتروني يتسم بالحداثة، وهو ما يرتبط بندرة المراجع المتخصصة في هذا الموضوع، ومن ناحية أخرى فإن بحث الحماية الجنائية للتوقيع

الالكتروني يستلزم الوقوف على الطبيعة التقنية للتوقيع الالكتروني وآلية استخدامه، وهو ما يتسم بالدقة ويستلزم قدرا من التخصص.

وبناءا على ذلك جاءت دراستي المقارنة لموضوع الحماية الجنائية للتوقيع الإلكتروني على المنهج التحليلي،من خلال دراسة وشرح الجوانب الموضوعية والإجرائية لتوقيع الإلكتروني في بعض التشريعات العربية كالتشريع الجزائري،والمصري،التونسي،وفي أبرز التشريعات الأجنبية كالتشريع الفرنسي،والتشريع الإنجليزي،والأمريكي.

كما اعتمدت على المنهج المقارن من خلال مقارنة الحماية الجنائية للتوقيع الإلكتروني في بعض القوانين العربية والأجنبية وبيان معالجتها للمشكلة من خلال القوانين التقليدية والإلكترونية، ومدى اعتراف القضاء بذلك في الإثبات من جهة ومقارنة التشريعات الحديثة لتوقيع الإلكتروني من خلال القوانين الدولية وعربية والغير عربية .

وبناءا على ما أسلفنا ولكي نتمكن من تغطية عناصر الموضوع ووفقا لما بيناه من تساؤلارتأينا تقسيم هده الدراسة إلى:

تناولت في الباب الأول القواعد الموضوعية للحماية الجنائية للتوقيع الإلكتروني وقسمت هذا الباب إلى فصلين تناولت في الفصل الأول،الأحكام الوقائية للحماية الوقائية لتوقيع الإلكتروني بينما تطرقت في الفصل الثاني إلى،الجرائم الماسة بمنظومة التوقيع الالكتروني، أما الباب الثاني فخصصته للحماية الإجرائية لتوقيع الإلكتروني وقسمته إلى فصلين،حيث تناولت في الفصل الأول إجراءات الإثبات الجنائي في جرائم التوقيع الإلكتروني أماالفصل الثاني التعاون الدولي لمواجهة جرائم الاعتداء على التوقيع الإلكتروني، وخاتمة كانت لأهم النتائج والتوصيات المتوصل إليه.

الباب الأول

الأحكام الموضوعية للحماية الجنائية للتوقيع الالكتروني

لقد ترتب على التطور الكبير في استخدام الحاسبات الآلية في كافة جوانب الحياة ظهور طرق ووسائل حديثةفي المعاملات لا تتلاءم مع الإثبات باستخدام التوقيع بمفهومه التقليدي وخاصة مع انتشار نظم المعالجة الالكترونية للمعلومات لذا فقد لزم اللجوء لاستخدام التوقيع والمحررات الالكترونية في المعاملات وقد ظهر التوقيع الالكتروني في البداية في عمليات الدفع الالكتروني في البنوك وهو ما يعرف ببطاقات الائتمان الممغنطة.

وفد حظي التوقيع الالكتروني بأهمية كبيرة في المعاملات القانونية وصار الاعتماد عليه في عقود التجارة الالكترونية لذا فقد تعاظم دوره في إثبات المعاملات التجارية[1].

ونظرا لأهمية الدور الذي يقوم به التوقيع الالكتروني فقد تزايد معدل جرائم الاعتداء عليه، وأصبح من الضروري استخدام تقنيات حديثة في عمليات التحقيق والتحري والكشف عن أدلة الجريمة خصوصا وأنها تستهدف محلا ذا طبيعة مغايرة لمحل الجريمة التقليدية هذا ما يستوجب تدخل المشرع الجزائي لتوفير الحماية لهذه الأنماط الخطيرة من الجرائم.

وتقتضي دراسة الحماية الجنائية للتوقيع الالكتروني، بحث في التدابير التقنية اللازمة لتوفير حماية وقائية من مخاطر الاعتداء عليه.

وكنتيجة لذلك أقرت بعض التشريعات والاتفاقات الدولية بعض الإجراءات الوقائية لتجنب وقوع الاعتداء على التوقيع الالكتروني، والحد من الأضرار الناتجة عن ذلك، فضلا عن النصوص العقابية واجبة التطبيق على من يثبت ارتكابه تلك الجرائم.[2]

غير أن البحث في موضوع الحماية الوقائية للتوقيع الالكتروني، تقتضي بالضرورة الوقوف على مدلول الحماية التقنية من ماهية التوقيع الالكتروني ووظائفه وصوره وحجيته في الإثبات وكذا التصديق على التوقيعات الالكترونية في الفصل الأول وتناول في الفصل الثاني القواعد الجزائية التي رصدها المشرع الوطني والمقارن ضد مرتكبي جرائم التوقيع الالكتروني والمتمثلة فيما يلي:

الفصل الأول: الأحكام الوقائية لحماية التوقيع الالكتروني.

الفصل الثاني: الأحكام الجزائية لحماية التوقيع الالكتروني.

[1]- حسام محمد نبيل الشنراقي، جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، مصر، سنة، 2013، ص 13.

[2]- محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة الجديدة، مصر، 2003، ص 219.

الفصل الأول

الأحكام الوقائية لحماية التوقيع الالكتروني

فرض العصر الحالي إضفاء قدر معين من الحماية على التوقيعات الالكترونية في شقيها الوقائي الذي من شأنه منع ارتكاب جرائم الاعتداء على التوقيع الالكتروني قبل وقوعها تجنبا للأضرار الناشئة عن ارتكابها، أما شقها الجزائي يتمثل في القواعد الجزائية التي تطبق على كل من ثبت ضده ارتكاب مثل هذه الأفعال الماسة بالتوقيع الالكتروني.

وتتطلب دراسة القواعد الوقائية لحماية التوقيع الالكتروني البحث في الجوانب التقنية لحماية التوقيع الالكتروني، وأنماط الحماية التقنية للتوقيع الالكتروني وعلى ذلك فسوف نقسم هذا الفصل إلى مبحثين على النحو التالي:

المبحث الأول: الجوانب التقنية لحماية التوقيع الالكتروني.

المبحث الثاني: أنماط الحماية التقنية للتوقيع الالكتروني.

المبحث الأول: الجوانب التقنية لحماية التوقيع الالكتروني.

تنطلق الحماية التقنية من مبدأ أنه ليس هناك أفضل من الوسائل الوقائية المماثلة لطبيعة السلوك الإجرامي للحد من خطورته، ويتعين لوضع إستراتيجية وقائية لحماية التوقيع الالكتروني، الوقوف على مدلول الحماية التقنية للتوقيع الالكتروني التي يمكن الاعتماد عليها لتوفير حماية وقائية من مخاطر الاعتداء على التوقيع الالكتروني، وفي ضوء ذلك سوف نتناول في هذا المبحث مطلبين على النحو التالي:

المطلب الأول: مدلول الحماية التقنية للتوقيع الالكتروني.

المطلب الثاني: التصديق على التوقيعات الإلكترونية.

المطلب الأول: مدلول الحماية التقنية للتوقيع الالكتروني.

يعد التوقيع الالكتروني، العنصر الأساسي في ظهور التجارة الالكترونية التي كانت بحاجة إلى توقيع يتلاءم وطبيعتها قصد تضمين المعاملات الالكترونية وتوثيقها بصفة عامة والعقود المبرمة ضمن التجارة الالكترونية بصفة خاصة فقد أصبح اعتماد التوقيع الالكتروني ضرورة عالمية إذ سارعت معظم التشريعات إلى الاعتراف به، ما بين منظمين في قوانين خاصة كما هو الحال عليه في التشريع الفرنسي والمصري أو ضمن قانون التجارة الالكترونية مثل التشريع التونسي أو الأردني[1].

وتتعدد صور التوقيع الالكتروني بحسب الطريقة التي يتم بها التوقيع كما تتباين هذه الصور من حيث درجة ومستوى ما تقدمه من ضمان، حسب الإجراءات المتبعة في إصدارها وتأمينها والتقنيات التي تتيحها.

كما أن الثقة والأمان تفرضان وجود طرف ثالث محايد موثوق به وهذا الطرف يقوم بالتأكد من صحة صدور الإرادة التعاقدية الالكترونية لمن ينسب إليه التوقيع الالكتروني وهذا الطرف الثالث قد يكون مؤسسة حكومية أو غير حكومية ويسمى بجهة التوثيق[2]

[1]- يمينة حوحو، عقد البيع الالكتروني في القانون الجزائري، دار بلقيس للنشر والتوزيع، دار البيضاء، طبعة أولى الجزائر، 2016، ص 161.

[2]- Huet J, vers une consécration de la preuve et la signature électronique, D. 2000. DALLOZ, p 96

الفرع الأول: تعريف التوقيع الالكتروني.

يهدف التوقيع في القواعد التقليدية إلى تحديد هوية الشخص الموقع والتعبير عن إرادته وهو عنصر جوهري بوجود المحرر، وقد أخذ التوقيع عبر التاريخ صور مختلفة، ابتداء من التوقيع على الحجر أو الجلد أو الخشب ثم بخط اليد والحبر والبصمة وما إلى التوقيع الالكتروني.

فقد اختلفت المصطلحات الواردة بشأنه، فالبعض يسميه بمستندات الالكترونية مثل القانون الإماراتي والبعض الآخر يسميه رسالة بيانات كقانون الاونيسترال النموذجي والبعض الآخر بالإمضاء الالكتروني كما ورد في التشريع التونسي، أما المصطلح الشائع الاستعمال فهو مصطلح التوقيع الالكتروني كالقانون الفرنسي أو الأردني أو الجزائري أو المصري.

لذا يجدر بنا تحديد مدلول التوقيع الالكتروني في التشريعات المقارنة والمنظمات الدولية والإقليمية وطنية أو أجنبية.

أولا: تعريف التوقيع الالكتروني وفقا التشريعات والتوجيهات الدولية.

تختلف التعاريف التي اطلعت على التوقيع الالكتروني باختلاف الزاوية المنظور منها فالبعض يعرفه بناء على الرسائل التي يتم بها أو بحسب الوظيفة أو بناء على التطبيقات العملية له[1].

فقد تصدت أكثر من منظمة لتعريف التوقيع الالكتروني من خلال قوانين التجارة الالكترونية ومن خلال قوانين وصفت خصيصا للتوقيع الالكتروني، غير أننا سنتناول الحديث هنا عن منظمتين فقط هما: لجنة الأمم المتحدة لقانون التجارة الدولية المعروفة بالأونيسترال والاتحاد الأوروبي كمثال لمنظمة إقليمية، إذ أن باقي المنظمات التي حاولت تعريف التوقيع الالكتروني تأثرت بتعريف الأونيسترال[2]

[1]- محمد فواز المطالقة، الوجيز في عقود التجارة الالكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008، ص 172.

[2]- الأونيسترال: هي لجنة قانون التجارة الدولية للأمم المتحدة، وتظم في عضويتها غالبية دول العالم الممثلة لمختلف النظم القانونية الرئيسة، غرضها الأساسي هو تحقيق الانسجام والتلاؤم بين القواعد القانونية المنظمة للتجارة الالكترونية وتحقيق وحدة القواعد المتبعة وطنيا في التعامل مع مسائل التجارة الالكترونية.

أ- قانون الأونيسترال النموذجي بشأن التجارة الالكترونية لسنة 1996م:

لقد منح قانون الأونيسترال النموذجي بشأن التجارة الالكترونية، وسائل البيانات الالكترونية حجية في الإثبات، كما اعترف بالتوقيع الالكتروني وسوى بينه وبين التوقيع التقليدي[1].

غير أنه عند الاطلاع على مواد قانون الأمم المتحدة النموذجي بشأن التجارة الالكترونية نجد أنه لم يعرف التوقيع الالكتروني واكتفى في مادته السابعة بالإشارة إلى الشروط الواجب توافرها في التوقيع، حيث نصت الفقرة الأولى منها على أنه " عندما يشرط القانون وجود توقيع من شخص يستوفي ذلك الشرط بالنسبة لرسالة البيانات، إذ استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات[2]، كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشأت أو بلغت من اجله رسالة البيانات، إذ استخدمت طريقة لتعين هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات في ضوء كل الظروف بما في ذلك أي اتفاق متصل بالأمر"[3]

ترتكز هذه المادة على ضرورة قيام التوقيع الالكتروني بوظائف تقليدية للتوقيع العادي أي ما يسمى نهج النظير الوظيفي أو المعامل الوظيفي والتساوي الوظيفي هنا يقصد به المساواة من حيث وظيفة الدليل في الإثبات هذا ما ورد في الفقرة ب كما ارتكز أيضا على أنه ينبغي أن تكون طريقة التوقيع الالكتروني الواردة بالفقرة ب طريقة موثوق بها[4] لذلك نجد أن قانون الأمم المتحدة النموذجي للتجارة الالكترونية وضع القواعد الأساسية التي تقوم عليها التوقيع الالكتروني من خلال الاعتراف به ومساواته بالتوقيع التقليدي

ب-التوجيه الأوربي بشأن التوقيعات الالكترونية لعام 1999م:

لم تكن المجموعة الأوروبية بمنأى عن الاهتمام الدولي بتطوير القواعد القانونية التي تتلاءم وعصر المعلوماتية، بل بالعكس تماما فقد ساهمت في دعم الاتجاه الذي يقوم على تشجيع التجارة الالكترونية فيما بين دول الأعضاء وغيرها من الدول المتقدمة ولضمان الأمن والثقة في التبادل الالكتروني لبيانات

[1]- إيمان مأمون سليمان، الجوانب القانونية لعقد تجارة الكترونية، رسالة دكتوراه، جامعة المنصورة، مصر، 2006، ص 249.

[2]- رسالة البيانات: يقصد بها المعلومات التي يتم لنتاجها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية أو بصرية أو وسائل تقنية أخرى بما في ذلك تبادل البيانات الالكترونية، أو البريد الالكتروني أو التلكس أو النسخ البرقي.

[3]- خالد ممدوح إبراهيم، إبرام العقد الالكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر، 2008، ص 242.

[4]- راجع المادة 7 من قانون الأونيسترال النموذجي بشأن تجارة الكترونية الصادر في 1996.

تقدمت اللجنة الاقتصادية والاجتماعية في المجلس الأوروبي إلى البرلمان الأوروبي سنة 1997م بمبادرة أوروبية تتعلق بالتجارة الالكترونية لحماية الاتصالات الالكترونية باستخدام تقنيات التوثيق الالكتروني من خلال التوقيعات الرقمية والالكترونية.

وبالفعل فقد أصدر المجلس الأوروبي في 13 ديسمبر 1999م بشأن التوقيع الالكتروني يتكون هذا التوجيه من 28 حيثية و15 مادة وأربعة ملاحق، حيث جاء في مادته الأولى أن الهدف منه هو تسهيل استخدام التوقيعات الالكترونية والمساهمة بالاعتراف القانوني بهكدليل إثبات، وهو ما ينشئ إطارا قانونيا للتوقيعات الالكترونية وبذلك يكون هذا التوجه قد أفضى على التوقيع الالكتروني نفس الحجية القانونية في الإثبات الممنوحة للتوقيع التقليدي[1].

فقد قامت غالبية الدول الأوروبية في تعريفها للتوقيع الالكتروني بنقل التعريف الوارد بتوجيه اللجنة الأوروبية رقم 1999/93 ومن تلك الدول النمسا حيث صدر قانون خاص بالتوقيع الالكتروني عام 2000 وبلجيكا صدرت سنة 2001[2].

يتضح لنا مما سبق أن التوجيه الأوروبي رقم 1999/93 قد وضع تعريفا وصفيا للتوقيع الالكتروني أي أنه تبين مفهوما واسعا له، حيث جاء عاما وشاملا لجميع صور التوقيع.

ج- قانون الأونيسترال النموذجي الخاص بالتوقيعات الالكترونية لعام 2001م:

قامت لجنة الأمم المتحدة للقانون التجاري الدولي في دورتها الرابعة والثلاثين بوضع القانون الذي تعرض لتنظيم التوقيع الالكتروني الموثوق به والجهة التي تقوم بتحديده والواجبات التي يتحملها الموقع، وما يبذله من عناية حيال توقيعه والسلوك الذي يتعين أن يتبعه الطرف الذي يعول على هذا التوقيع، كما نظم، أوضاع مقدم خدمات التصديق أو التوثيق الالكتروني وشهادات التصديق التي يصدرها.

فقد نص في المادة الأولى على نطاق تطبيق قواعدهذا القانون[3] فنص على تلك القواعد تطبق حيثما تستخدم توقيعات الكترونية في سياق أنشطة تجارية.

---

[1] - Sébastien Fucini , Principe de loyauté: régularité du stratagème de constatation de la preuve public, édition daloz 2014 p 36.

[2] - عادل أبو هشيمة محمود حوته، عقود خدمات المعلومات الالكترونية في القانون الدولي الخاص، دار النهضة العربية، القاهرة، مصر، 2004، ص188.

[3] - بموجب نص المادة الأولى من هذا القانون فإن نطاق تطبيقه يقتصر فقط على استخدم التوقيعات الالكترونية في مجال أنشطة تجارية، والنشاط التجاري، وفقا لدليل هذا التشريع يشمل جميع الوسائل الناشئة عن كل العلاقات ذات طابع تجاري سواء تعاقدية أو غير تعاقدية.

عرفت المادة الثانية من قانون الأمم المتحدة النموذجي بشأن التوقيعات الالكترونية إلى تعريف التوقيع الالكتروني بأنه:" بيانات في شكل الكتروني مدرجة برسالة أو مضافة إليها أو مرتبطة بها منطقيا، بحيث يمكن أن تستخدم لبيان هوية الموقع بالنسبة إلى هذه الرسالة ولبيان موافقته على المعلومات الواردة في الرسالة[1].

نلاحظ من النص السابق أن قانون الاونيسترال بشأن التوقيعات الالكترونية لم يقيد مفهوم التوقيع الالكتروني، بل أن هذا النص يمكن أن يستوعب أي تكنولوجيا تظهر في المستقبل تعني بإنشاء توقيع الكتروني وهذا ما نصت عليه المادة الثالثة من ذات القانون.

ثانيا: تعريف التوقيع الالكتروني وفقا للتشريعات الأجنبية.

لقد تعددت التشريعات الأجنبية التي تناولت تعريف التوقيع الالكتروني منها القانون الفرنسي، القانون الأمريكي، والقانون الانجليزي، كما تعددت التشريعات العربية في تعريف التوقيع الالكتروني كالتشريع المصري، التونسي، الأردني، الجزائري وهذا ما سيتم دراسته على النحو الآتي:

1- القانون الفرنسي:

اصدر المشرع الفرنسي بالاعتراف بالتوقيع الالكتروني من خلال إصدار قانون رقم 230 لسنة 2000 بشأن تطويع قانون الإثبات لتكنولوجيا المعلومات والتوقيع الالكتروني[2] حيث تنص المادة 4/1316 المضافة بقانون 3 مارس 2000 على ما يلي:

"التوقيع الضروري لإتمام التصرف القانوني الذي يميز هوية من وقعه ويعبر عن رضائه بالالتزامات التي تنشأ عن هذا التصرف، عندما يكون الكترونيا فيجب أن يتم باستخدام وسيلة آمنة لتحديد هوية الموقع وضمان صلة بالتصرف الذي وقع عليه"[3].

إن التعديل الذي أجراه المشرع الفرنسي على القانون المدني القسم الذي احتوى على قواعد الإثبات لتكييفه مع تكنولوجيات المعلومات في القانون رقم 200-236 الصادر بتاريخ 2000/3/13 لم يحدد شكلا معينا لأداء التوقيع ولكنه ركز فقط وظيفتين للتوقيع[4]

---

[1]- قانون الأونيسترال النموذجي بشأن التوقيعات الالكترونية لسنة 2001.

[2]- عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، مصر، ص 423.

[3]- عبد الفتاح بيومي حجازي، المرجع السابق، ص 423.

[4]- Leclercq (jean), la signature électronique : lecture critique, technique et juridique, le décret du 30 mars 2001 relatif a la signature, p56.

ولقد تطرق الجزء الثاني من المادة السابعة للتوقيع الالكتروني فعرفه على أنه " وسيلة ممكنة لكشف الهوية تتضمن ارتباطا مع العقد المتصل بالتوقيع"

أما المرسوم رقم 273/2001 الصادر في 30 مارس 2001، الصادر تطبيقا لأحكام المادة 4/1316 من القانون المدني والخاص بالتوقيع الالكتروني، فقد فرق بين التوقيع الالكتروني العادي والتوقيع الالكتروني الآمن المتقدم.

2- في القانون الأمريكي:

حظي التوقيع الالكتروني بنصيب وافر الأهمية في التشريع الأمريكي على مستويين الاتحاد الفدرالي والولايات المتحدة في آن واحد، فقد صدر القانون الموحد للمعاملات الالكترونية لعام 1999م على مستوى الولايات المتحدة الأمريكية وقد عرف القسم 2-8 منه من التوقيع بأنه "صوت أو رموز أو عملية الكترونية ترفق أو تربط منطقيا بسجل يقوم بتنفيذها أو إقرارها شخص يقصد منها التوقيع على السجل[1].

أما القانون الفدرالي الأمريكي بشأن التوقيعات الالكترونية في التجارة العالمية والمحلية الصادر في 30 يونيو 2000 فعرف التوقيع الالكتروني بأنه " أصوات إشارات، رموز، أو أي إجراء آخر مرتبط به منطقيا، بنظام معالجة المعلومات الكترونيا ويقترن بتعاقد أو مستند أو محرر يستخدمه الشخص قاصدا التوقيع على المحرر أو المستند".[2]

أما المستند المحرر الالكتروني فقد عرفه هذا القانون كما يلي: "كل مستند ينشئ أو يرسل أو يستقبل أو يخزن بوسائل الكترونية.

لم يشترط القانون الفدرالي الأمريكي توفر خصائص معينة في التوقيع لكي تكون له حجية قانونية أي أنه يعترف بالتوقيع الالكتروني والمحررات الالكترونية ولا يشترط لذلك الحصول على شهادة توثيق أو تصديق، من جهة معينة.

[1]- خالد ممدوح إبراهيم، التوقيع الالكتروني، الدار الجامعية، ط 1، الإسكندرية، مصر، 2000، ص 41.

[2]- ازاد دزه يي، النظام القانوني للمصادقة على التوقيع الالكتروني، دار الفكر الجامعي، الإسكندرية، مصر، 2016، ص 50.

3- القانون الانجليزي:

نصت المادة 1/7 من قانون الاتصالات الانجليزي لعام 2000 على أنه في مسائل الإثبات القانوني يعتبر التوقيع المرتبط بأية وسيلة اتصالات الكترونية وأنه شهادة تفيد توقيع صاحبها إنهما مقبولان كدليل إثبات في أية منازعة تتعلق بالتوقيع أو البيانات[1]

كما وقد عرفته اللوائح المنظمة للتوقيعات الالكترونية البريطانية لعام 2002 التوقيع الالكتروني في المادة الثانية بأنه "يعني بيانات على شكل الكتروني تتصل بشكل منطقي ببيانات الكترونية أخرى أو تستخدم كوسيلة مصادقة.

فمعظم الدول الأعضاء في الاتحادالأوروبي قاموا بتعديل الإطار التشريعي الوطني لكي يتم تطويعها لتستجيب للتصرفات القانونية التي تتم عن طريق المستند الالكتروني [2]

ثانيا: تعريف التوقيع الالكتروني في التشريعات العربية.

اقتداء بالدول الغربية وبالقوانين الدولية، قامت الدول العربية بإصدار تقنيات خاصة بتنظيم التوقيع الالكتروني، وأخرى عدلت من قوانينها الخاصة بالإثبات من أجل مواكبة التقدم التكنولوجي ومنها.

1- القانون التونسي:

تعتبر تونس من الدول العربية ذات السبق في إصدار قانون التوقيع الالكتروني حيث صدر قانون التوقيع الالكتروني عام 2000 وهو القانون رقم 2000/83 الخاص بالتوقيع الالكتروني والتجارة الالكترونية، إلا أن المشرع التونسي لم يورد تعريفا خاصا بالتوقيع الالكتروني وإنما اكتفى بتنظيم أحكامه وذلك من خلال توضيح الإجراءات المتعلقة بالتشفير الخاصة بالتوقيع الالكتروني في المادة الثانية فقرة 6-

حيث تعرض المشرع التونسي إلى بيان معنى "منظومة أحداث الإمضاء ومنظومة التدقيق في الإمضاء

[1]- أيمن سعد سليم، التوقيع الالكتروني، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2004، ص62.

[2] - WILMS, Mélanges Jean Pardon, « De la signature au « notaire électronique ». La validation de la communication électronique », Bruxelles, Bruylant, 1996,p86

2-القانون المصري:

عرف المشرع المصري التوقيع في قانون التوقيع الالكتروني رقم 2004/15 أنه ما يوضع على محرر الكتروني ويتحقق في شكل حروف وأرقام أو رموز أو إشارات أو غيرها، ويكون به طابع منفرد ويسمح بتحديد شخص الموقع وتميزه عن غيره.

كما عرفه قانون التجارة الالكترونية المصري في المادة الأولى منه بأنه "حروف وأرقام ورموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتميزه عن غيره"[1]

وبمناقشة التعريفين المذكورين أعلاه تجد أن التعريف الخاص بالتوقيع الالكتروني في قانون التجارة الالكترونية المصري يعتبر هو الأفضل والأدق وذلك لأن التعريف الأول الخاص بقانون التوقيع الالكتروني جاء مقيدا فهذا التعريف ربط التوقيع الالكتروني بالوضع على محرر فقط.

3.القانون الجزائري:

لقد نص القانون الجزائري بالتوقيع الالكتروني في القانون المدني في المواد 323 مكرر1 إلى 327، وكذلك ضمن المرسوم التنفيذي رقم 07-162 الصادر في 2007/05/30 المعدل والمتمم للمرسوم التنفيذي رقم 01-123 والمؤرخ في 2001/05/09 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية فقد نصت المادة 323 مكرر من القانون المدني الجزائري المستحدثة بالقانون رقم 05-10 والمؤرخ في 2005/07/20.[2]

ما يلي "ينتج الإثبات بالكتابة من تسلسل حروف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها أو طرق إرسالها".

[1]- راشد بن حمد البلوشي، التوقيع الالكتروني والحماية الجزائية المقررة له، دراسة في القانون العماني والقانون المقارن، منشورات الحلبي الحقوقية، طبعة أولى، بيروت، لبنان، 2018، ص 25.

[2]- قانون رقم 10/05 المؤرخ في 20 جويلية 2005، المعدل والمتمم للأمر رقم 75-58المؤرخ في 26 -09-1975 والمتضمن القانون المدني العدل والمتمم ج ر ، رقم 44 المؤرخة في 26-06-2005.

كما نصت المادة 03 من المرسوم التنفيذي رقم 07-162 [1] الصادر في 2007/05/30 المعدل والمتمم للمرسوم التنفيذي 01-123 والمؤرخ في 2001/05/09 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات السلكية واللاسلكية ما يلي:

"التوقيع الالكتروني هو معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر و323 مكرر 01 حيث أنه اعتبر التوقيع الالكتروني المؤمن هو توقيع الكتروني يعنى بالمتطلبات الآتية:

- يكون خاصا بالموقع.
- يتم بوسائل يمكن أن يحتفظ بها الموقع تحت مراقبته الحصرية.
- يضمن مع الفعل المرتبط بمهامه بحيث يكون أي تعديل لاحق للفعل قابل للكشف.
- كما وقد عرف المشرع الجزائري التوقيع الالكتروني في نص المادة 02 من القانون رقم 04/15 المتعلق بالتوقيع والتصديق الالكترونيين على انه "بيانات في شكل الكتروني،مرفقة أو مرتبطة منطقيا ببيانات الكترونية أخرى،تستعمل كوسيلة توثيق"
- وبصدور القانون رقم 04/15 المؤرخ في 11 ربيع الثاني عام 1436 هـ الموافق ل أول فبراير سنة 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني نلاحظ أن المشرع الجزائري اقر بالتوقيع الالكتروني كوسيلة توثيق وكان أكثر وضوحا في ظل هذا القانون مقارنة بالمرسوم التنفيذي رقم 162/07 المتعلق بنظام الاستغلال المطبق على أنواع الشبكات الخدمات المواصلات السلكية واللاسلكية.

الفرع الثاني: وظائف وخصائص التوقيع الالكتروني.

لقد أدى استغلال وسائل تقنية المعلومات في إبرام العقود المختلفة وتبادل البيانات إلى ظهور حقيقته ملموسة ذات طابع مادي تتمثل في التوقيع الالكتروني الذي حظي بالاعتراف به من قيل جميع التشريعات غير أن خذا الأخير يثير عدة إشكالات حول مدى اعتراف القانون بهذه الآلية الجديدة في ميدان الإثبات، ولكي يمكن الاعتماد والأخذ به من قبل جهة رسمية يتطلب ذلك وجود مجموعة من

[1]- مرسوم تنفيذي رقم 162/07 يعدل ويتمم المرسوم 01-123 المتعلق بنظام الاستغلال المطبق على كل أنواع الشبكات بما في ذلك اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية اللاسلكية،رقم 37 المؤرخة في 03 يونيو2007.

الشروط والخصائص بالتوقيع الإلكتروني والتي هي موضوع حديثنا، وعليه سنتطرق إلى: وظائف التوقيع الالكتروني ثم خصائصه ثانيا.

أولا:وظائف التوقيع الالكتروني

اعتبارا للأهمية الكبرى التي يكتسبها التوقيع الإلكتروني سنحاول إبراز الوظائف التي يؤديها وهي كالآتي

أ-مدى تحديد التوقيع الالكتروني لهوية الشخص الموقع

حتى يقوم التوقيع بوظيفته، فلابد أن يكون للتوقيع علامة مميزة لشخصية الموقع عن غيره وتضمن تحديد هويته وقد أكد هذا الشرط قانون الاونيسترال النموذجي الخاص بالتوقيعات الالكترونية حيث نصت المادة 1/أ إذا استخدمت طريقة لتعيين هوية ذلك الشخص وأيضا المادة الثانية أ من قانون الأونيسترال بشأن التوقيعات الالكترونية لعام 2001 ما يلي: "يجوز أن تستخدم لتعيين هوية الموقع"[1]

هذا وقد نصت المادة 2 فقرة2 من قانون 15-04 بأن الشخص الموقع هو "شخص طبيعي يحوز بيانات إنشاء التوقيع الالكتروني ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي، أو المعنوي الذي يمثله[2] وبالتالي فإنه بتوافر هذا الشرط في التوقيع الالكتروني يؤدي إلى اتجاه نية الموقع على المحرر بمضمونه ويكون شاهدا على نيته بالالتزام بمضمون العقد الموقع عليه.

من الضروري أن يكون التوقيع دالا ومحددا لشخص الموقع ليتحقق بذلك دوره في الإثبات.

1- التعبيرعن إرادة الموقع:

ذكرنا سابقا أن التوقيع بشكل عام يعرف على أنه بمثابة تعبير عن إرادة الموقع بمضمون التصرف القانوني، وهذا ما أكدته محكمة النقض المصرية، حيث قررت بأن ثبوت صحة التوقيع بعدم

[1]- خالد ممدوح إبراهيم، المرجع السابق، ص 110.

[2]- راجع المادة 2 فقرة 2 من القانون رقم 15-04 المتعلق بتنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات بجمهورية مصر العربية.

إنكارهصراحة كافية لإعطاء الورقة حجيتها في أن صاحب التوقيع قد ارتضى بمضمونها والالتزام بها ومؤداه إعطاء الورقة حجيتها.[1]

ولعل هذا الشرط يعتبر من الشروط المشتركة بين التوقيع الكتابي والتوقيع الالكتروني حيث يستوي في ضرورة توفر هذا الشرط أن يكون التوقيع كتابيا حرر بخط اليد على الورق وأن يكون الكترونيا سواء كان هذا التوقيع رموزا، أرقاما، إشارات بحيث توقع على بيانات محرر الكتروني.[2]

2- إثبات حضور صاحب التوقيع

بالرغم من أن التوقيع الالكتروني لا يعني بالضرورة الحضور المادي والجسدي للأفراد في مجلس العقد وقت إبرام العقد أو التصرف القانوني، إلا أن هناك من يرى بأن استعمال البطاقة الالكترونية وإدخالها في المكان المناسب بجهاز الصرف الآلي وإدخال الرقم السري ثم تدوين قيمة المبلغ المراد سحبه على الجهاز يعد دليلا على الحضور المادي للشخص ذاته لأن الرقم السري لا يعرف إلا صاحبه.[3]

ثانيا: خصائص التوقيع الالكتروني

يتميز التوقيع الالكتروني بخصائص أساسية ومتميزة عن التوقيع الكتابي كونه يتم كليا أو جزئيا عبر وسائط إلكترونية من خلال أجهزة الكمبيوتر أو عبر شبكة الانترنت ومن بين الخصائص التي يتميز بها ما يلي:

أ- يوفر الخصوصية:

أي حماية البيانات هذا الاستخدام غير مشروع، ونعني بالخصوصية أن البيانات المتوفرة فقط للأشخاص المسموح لهم الاطلاع عليها بعبارة أخرى عدم الاطلاع عليها من قبل الآخرين الغير مخول لهم الاطلاع على مضمون السند الموقع الكترونيا سوى الشخص المرسل له[4]ويتم حفظ البيانات الخاصة بالتوقيع الالكتروني على بطاقة ذكية وتكون محمية برقم سري، وتشفيرها أثناء إرسالها وهي إحدى مزايا التوقيع الالكتروني التي تهدف إلى التأكد من أن الشخص المقصود هو الوحيد الذي اطلع على المستند المر

[1]- محكمة النقض المصرية النقض مدني، جلسة 05 يونيو 2001، الطعن رقم 564 المشار إليه في محلية المحاماة عدد 2 سنة 2002م، ص 70.

[2]- راشد حمد البلوشي، المرجع السابق، ص 31.

[3]- فيصل سعيد الغريب، التوقيع الالكتروني وحجيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، مصر، 2005، ص 216.

[4]- Jeff C. Dodd and James A. Hernandez, contracting in cyberspace, avril 1998, p 17.

ب-يوفر التعرف على المستخدم:

تتم عملية التحقق من هوية الأشخاص والتعرف على مصادر البيانات عن طريق كلمات الشر والبطاقات الذكية أو عن طريق شهادة التصديق الالكتروني المصدرة من جهة تصديق الكتروني وكلما زادت الحاجة لدفة تحديد الهوية يتم اللجوء إلى جمع عدة وسائل وزيادة تعقيد وسيلة التحقق من هوية المستخدم.[1]

ج- يوفروحدة البيانات:

هي عملية حماية البيانات ضد التغيير أو التعريف عنها ببيانات أخرى، وتتم هذه العملية باستخدام تقنية تشفير البيانات ومقارنة ببصمة الرسالة المرسلة لبصمة الرسالة المستقبلة –عدم تغيير البيانات أثناء نقلها، وأن مستقبل الرسالة يمكنه معرفة ذلك عند تلقي رسالته، حيث حصل أي تغيير أو تعديل على المستند أثناء إرساله اعتبر تزويرا.[2]

الفرع الثالث: صور التوقيع الالكتروني وحجيته في الاثبات:

أولا-صور التوقيع الالكتروني.

لم ينص المشرع الجزائري على صور التوقيع الالكتروني كما وقع ذلك في أغلب التشريعات الأوروبية أو العربية مع أن تنظيمها يعد من المسائل الضرورية في ميدان المعاملات الالكترونية وفي الحقيقة صور التوقيع الالكتروني تتعلق بمسألة أنظمة توثيق التوقيع الالكتروني والمرتبطة بتكنولوجيا المعلومات والاتصالات التي أوجدت عدة أشكال من أنظمة التوقيع الالكتروني ومن بين صور التوقيع الالكتروني ما يلي:

أ-التوقيع بواسطة الرقم السري ببطاقة ممغنطة.

تعتبر هذه الصورة الأكثر انتشارا في التعاملات الالكترونية، خاصة في المعاملات البنكية حيث درجت البنوك على إصدار بطاقات ذكية مصحوبة برقم سري يتمثل في أرقام وحروف ويطلق عليه الرقم الشخصي المميز PIN حيث تتم مطابقة هذا الرقم السري برقم سري مخزن سابقا في ذاكرة الحاسب الآلي

[1]- لالوش راضية، أمن التوقيع الالكتروني، رسالة ماجستير في القانون، فرع القانون الدولي للأعمال،كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012، ص 37.

[2]- صلاح عبد الحكيم المصري، متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية، رسالة ماجستير في إدارة الأعمال، كلية التجارة، الجامعة الإسلامية غزة، 2007، ص 24-25.

المقدم للخدمة المعلوماتية فإذا تطابق الرقمان كان التوقيع تاما، وبذلك يكون الشخص مخولا بدخول إلى الموقع الالكتروني أو النظام المصرفي[1].

ب-التوقيع البيومتري.

يعرف التوقيع البيومتري بأنه "التحقق من شخصية الموقع باعتماد على مجموعة من الخواص الفيزيائية والطبيعية والسلوكية التي يتصف بها ذلك الشخص"

فالتوقيع في هذه الصورة يعتمد على الصفات الفيزيائية والطبيعية والسلوكية للإنسان تختلف من شخص إلى آخر، تتميز هذه الصفات بالثبات النسبي ومن شأنه أن يجعل لها صفة الحجية في التوثيق والإثبات، حيث تعتبر هذه الصورة منصور التوقيع الالكتروني، العلمية الحديثة والمتطورة، وهي ضمن تكنولوجيات البصمات والخواص الحيوية والطبيعية[2].

ج-التوقيع بالقلم الالكتروني.

يعد التوقيع الالكتروني بواسطة القلم الالكتروني من أهم التوقيعات الالكترونية المستخدمة عبر الانترنت إذ هو توقيع يعتمد على استعمال أرقام، رموز سرية من قبل المستخدم من خلال الحاسب الآلي باستعمال علم التشفير القائم على المفتاح العام والخاص قصد تضمين سرية البيانات والمعطيات وسلامتها وتحديد مصدر مرسلها[3].

وتعتبر هذه الصورة من صور التوقيع الالكتروني أفضل الصور على الإطلاق والأكثر انتشارا وذلك لما توفره هذه الطريقة أو الصورة من أمان وثقة وضرورية في المعاملات الالكترونية خصوصا في التجارة الالكترونية[4].

ثانيا: حجية التوقيع وفقا للتشريعات المنظمة للإثبات الالكتروني.

في مطلع العقد الأخير من القرن الماضي وبعد تعميم استخدام شبكة الاتصالات الحديثة الانترنت على الأشخاص، أخذت هذه الشبكة بالتحول بوتيرة متسارعة إلى سوق تجاري عالمي مجرد من الهيكل المادي أي خال من الورق ونظرا لاختلاف مقومات التجارة الالكترونية عن مقومات التجارة التقليدية،

[1]- ثروت عبد الحميد ، التوقيع الالكتروني ماهيته، مخاطره، كيفية مواجهته ومدى حجيته في الإثبات، دار النهضة العربية، القاهرة، مصر، 2002، ص 62.

[2]- إبراهيم الدوسقي أبو الليل، الجوانب القانونية للتعاملات الالكترونية، مجلس البحث العلمي، جامعة الكويت، 2002، ص 158.

[3]- يمينة حوحو، المرجع السابق، ص 184.

[4] - Vidal G, cours de droit criminel et de science pénitentiaire, 2eme, paris, 2010.p 75.

فلم يعد في ظل التجارة الالكترونية دعامات ركائز ورقية تثبت عليها الكتابة التقليدية أو يظهر عليها توقيع خطي الأمر الذي أدى إلى ظهور محاولات عديدة على المستوى الدولي والإقليمي لاكتشاف السبل الكفيلة لإعطاء الثقة في التوقيع الالكتروني ووضع أساس يضمن الاعتراف بحجيته في الإثبات وهذا ما سنتناوله في هذا الفرع.

أ-الاعتراف التشريعي بحجية التوقيع الالكتروني في التشريعات الدولية.

حظي التوقيع الالكتروني باهتمام دولي كبير فمنحت له مختلف التشريعات الحجية القانونية في الإثبات وهذا ما سنتطرق له كالآتي:

1- منح التوقيع الالكتروني الحجية في الإثبات وفقا لقوانين الأونيسترال

تنص المادة 1/6 من قانون "الأونيسترال" بشأن التوقيعات الالكترونية على أنه "حيث ما يشترط القانون وجود توقيع من شخص، يعد ذلك شرطا مستوفيا في رسالة البيانات إذا استخدم توقيع الكتروني موثوقا به بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات في ضوء كل الظروف بما في ذلك اتفاق ذي صلة[1].

وفقا لهذا النص يعد التوقيع الالكتروني صالحا لإنشاء الالتزامات حينما يتطلب القانون وجود توقيع على مستند معين، يشترط أن يكون هذا التوقيع الالكتروني موثوق به[2].

2- منح التوقيع الالكتروني الحجية القانونية وفقا لتوجيهات الاتحاد الأوروبي.

اعتبر الاتحاد الأوروبي إيجاد نظام قانوني بالتوقيع الالكتروني من الأولويات الأساسية وقد تم تشكيل لجنة خبراء في القانون والاقتصاد، أنيطت بها مهمة الإجابة عن الأسئلة التي يطرحها قطاع التجارة الالكترونية وفي نهاية أعمالها تمكنت من الخروج بعدة مقترحات واستنتاجات أولية ذات أهمية بالغة منها أن الانترنت ليست فضاء لعدم التقنين، إذ تجد تنظيمه بأحدث القوانين والعمل على صياغة قانون إطار

[1]- عيسى غسان ربضي، القواعد الخاصة بالتوقيع الالكتروني، دار الثقافة للنشر والتوزيع، عمان، طبعة أولى، 2005، ص 172.

[2]- الفقرة 3 من المادة 6 من قانون الاونيسترال، بشأن التوقيعات الالكترونية لسنة 2001م.

مشترك بين الدول الأوروبية بخصوص تنظيم مؤسسة التوقيع الالكتروني جميع دول الاتحاد الأوروبي آخذين بعين الاعتبار المصالح الداخلية لكل دولة[1].

وذلك في الفقرة الأولى من المادة الخامسة من هذا التوجيه على أنه " على الدول الأعضاء مراعاة التوقيع الالكتروني المتقدم المستند إلى شهادة تصديق الكتروني والمنشأ بوسيلة آمنة".

يحقق الشروط القانونية للتوقيع بالنسبة للمعلومات المكتوبة الكترونيا، بذات الحجية لتي يحققها التوقيع اليدوي بالنسبة للمعلومات المكتوبة يدويا أو المطبوعة على الورق.

يكون مقبولا كدليل أما القضاء.

ومن خلال هذا النص يتضح لنا أن التوجيه الأوروبي أضفى على التوقيع الالكتروني نفس الحجية القانونية في الإثبات الممنوحة للتوقيع التقليدي.

ب-منح التوقيع الالكتروني الحجية القانونية في الإثبات وفقا للتشريعات الوطنية

1-التشريعات الغربية.

-القانون الفرنسي:

انسجاما مع التوجيهات التي رسمها القانون المشترك للاتحاد الأوروبي، حول التوقيع الالكتروني سعت فرنسا إلى إدخال تعديلات هامة على مستوى قوانينها سواء القانون المدني أو مدونة حماية المستهلك.

-على مستوى القانون المدني:

تبنت فرنسا بمقتضى المرسوم 2000/203 الصادر في 13 مارس 2000[2]التوقيع الالكتروني في مجال تكنولوجيا المعلومات والاتصالات الحديثة، بعد تعدل المواد 1315 إلى 1348 من القانون المدني الفرنسي حيث نصت المادة 4/1316 منه على أن التوقيع ضروري لإتمام العقد القانوني ولتحديد هويته من وصفه، كما يكشف عن رضاء الأطراف بالالتزامات الناشئة عن العقد...، حينما يكون التوقيع الكترونيا فإنه يكمن في استخدام طريقة جاهزة لتحديد الهوية بما يضمن ارتباطه بالعقد الذي وضع عليه التوقيع.

[1]- المصطفى فارس، الإثبات الرقمي، الحجية القانونية للسندات الالكترونية، مكتبة رشاد للتوزيع والنشر، الطبعة الأولى، المغرب، 2015، ص 86.

[2]-القانون الفرنسي رقم: 2001/272 الصادر بتاريخ 30 مارس 2000 المتعلق بالتوقيع الالكتروني المعدل والمتمم للمادة 136 من القانون المدني الفرنسي، الجريدة الرسمية، عدد 77، الصادرة بتاريخ 21 مارس 2001.

كما أقر القضاء الفرنسي بصلاحية التوقيع الالكتروني وحجيته في الإثبات من خلال حكم صدر بتاريخ 08 نوفمبر 1989 عن محكمة النقض الفرنسية، أقر بصلاحية التوقيع الرقمي الذي يتم بواسطة شخص من خلال الرقم المستخدم في البطاقات الرقمية وهذا بالنسبة للاتفاقات المتعلقة بالإثبات.

وتكون الثقة في الواقع الالكتروني والتي يستمد منها حجيته الإثبات مفترضة عندما تراعي الشروط التي يتولى تحديدها مرسوم يصدر عن مجلس الدولة الفرنسي[1].

من خلال ما سبق يمكن القول أن المشرع الفرنسي لم يفرق بين التوقيع التقليدي والتوقيع الالكتروني حيث يكون لكل منهما نفس الحجية القانونية في الإثبات طالما كان هذا التوقيع يميز صاحبه، ويتم بإجراءات آمنة تضمن سرية بيانات التوقيع.

-على مستوى مدونة حماية المستهلك.

عرفت الفقرة 16 من المادة 121 من مدونة حماية المستهلك المعدلة لتعاقد الكتروني عن بعد بكونه "كل بيع لمال أو منقول أو اخذ خدمة من غير حضور ذاتي أو مباشر للأطراف، وذلك بين المستهلك ومنتج وبائع، الذين يستعملون وسيلة أو عدة وسائل للاتصال عن بعد الانترنت، الفاكس الهاتف لإنجاز ذلك العقد.

وبإدخال هذا التعديل على مدونة حماية المستهلك تم حل الإشكالات التي يطرحها التعاقد عن بعد، فلم يقتصر على مجرد تبادل المعلومات الكترونيا وإنما اشترط أن يتم تأكيد رغبة المستهلك بوثيقة كتابية[2].

2-في القانون الأمريكي:

أوردت المادة 101 من الباب الأول الذي جاء بعنوان السجلات والتوقيعات الالكترونية في التجارة الالكترونية من التشريع الفدرالي الأمريكي بشأن التوقيعات الالكترونية والتجارة الالكترونية، قاعدة عامة تتعلق بصحة وقانونية المحررات حيث نصت الفقرة أ على أنه رغما عن أي تنظيم أو قانون في أيه ولاية أو أية قاعدة قانونية في أي قانون في أية معاملات مالية، سواء في داخل الولايات أو في التجارة الأجنبية، يجب مراعاة أنه عقد خاص بالمعاملات المالية لا ينكر أثره القانوني أو حجيته أو قابليته للتنفيذ بسبب استخدام التوقيع الالكتروني أو السجل الالكتروني في الكتابة أو صياغته.

[1]- سعيد سيد قنديل، التوقيع الالكتروني، دار الجامعة الجديدة، الإسكندرية، مصر ،2006، ص 58.

[2]- المصطفى فارس، المرجع السابق، ص 91.

يلاحظ أن التشريع الفدرالي الأمريكي لم يشترط في التوقيع الالكتروني ضوابط فنية أو تقنية معينة كما لم يستلزم توثيق التوقيع الالكتروني من جهة تصديق الكتروني معتمدة[1].

3-التشريعات العربية:

قامت التشريعات العربية مثلها مثل التشريعات الغربية يمنح التوقيع الالكتروني الحجية في الإثبات، سنتعرض لمختلف هذه التشريعات فيما يلي:

-التشريع التونسي:

بموجب قانون المبادلات والتجارة الالكترونية التونسي رقم 83 لسنة 2000 تم إقرار الحجية القانونية في الإثبات للتوقيعات الالكترونية والسندات الالكترونية أسوة بالتوقيع التقليدي للمحررات العادية ولم يعط المشرع التونسي الحرية المطلقة لأي شخص في الحصول على توقيع الكتروني وقد اعترف المشرع التونسي بالحجية الكاملة للتوقيع الالكتروني في الإثبات وهذه الحجية تعادل تماما حجية التوقيع المكتوب على السندات التقليدية[2].

-القانون الأردني:

أورد المشرع الأردني مادتين في قانون المعاملات الالكترونية رقم 85 لسنة 2001 ساوى بينهما في الحجية التوقيع الالكتروني والتوقيع التقليدي، حيث نص في المادة7أ "يعتبر السجل الالكتروني والعقد الالكتروني والرسالة الالكترونية والتوقيع الالكتروني منتجا للآثار القانونية ذاتها المرتبطة على الوثائق والمستندات الخطية والتوقيع الخطي بموجب أحكام التشريعات النافذة من حيث إلزامها لأطرافها وصلاحيتها في الإثبات، ونصت المادة 10 على أنه "إذا استوجب تشريع نافذ توقيعا على المستند أو نص على الترتيب أثر على التوقيع فإن التوقيع الالكتروني على السجل الالكتروني يفي بمتطلبات ذلك التشريع".

-القانون المصري:

ووفقا للقانون المصري رقم 15 لسنة 2004 بشأن التوقيعات الالكترونية نستطيع أن نقول أنه قد دخل من التعاملات الالكترونية من دون خوف وتردد في الأخذ بالوسائل الحديثة في مجال إثبات المعاملات الالكترونية ومنحها الحجية القانونية في الإثبات فقد نصت المادة 15 من القانون نفسه "الكتابة الالكترونية والمحررات الالكترونية في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة

[1]- لالوش راضية، المرجع السابق، ص 81.

[2]- أزاد دزه بيي، المرجع السابق، ص 178.

للكتابة والمحررات الرسمية والعرفية" ومن ثم كررت نفسها فيما يأتي: "يتمتع التوقيع الالكتروني والكتابة الالكترونية والمحررات الالكترونية بالحجية في الإثبات إذا توافرت الشروط الآتية:

-ارتباط التوقيع الالكتروني بالموقع وحده دون غيره.

-سيطرة الموقع وحده دون غيره على الوسيط الالكتروني.

-إمكانية كشف أي تعديل أو تبديل في بيانات التوقيع الالكتروني.

ومن الملاحظ أن هذه الشروط هي نفسها المنصوص عليها في المادة 3/2 من قانون التوقيع الالكتروني النموذجي لسنة 2002[1].

-في القانون الجزائري:

لقد استجاب المشرع الجزائري للتغيرات التي طرأت على وسائل الاتصالات والإعلام واستعمالها في المعاملات، حيث سار على ما نهجته تشريعات العالم من الاعتراف بالكتابة الالكترونية التي دعت الأمم المتحدة إليه من خلال لجنة أونيسترال التابعة لها وفي هذا الصدد نص المشرع الجزائري في المادة 323 مكرر1 من القانون المدني المعدل والمتمم بالقانون 15-10 الصادر في 2015/07/20 على أنه "يعتبر الإثبات بالكتابة في الشكل الالكتروني كالإثبات بالكتابة على الورق[2].

بشرط أمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها" كما جاء في نص المادة 327 من نفس القانون ما يلي: "يعتبر العقد العرفي صادرا مما وقعه مالم يذكر صراحة ما هو منسوب إليه من خط أو إمضاء".

ويعتبر التوقيع الالكتروني وفق الشروط المذكورة في المادة 323 مكرر 01 أعلاه "ومن خلال هذين النصين يكون المشرع الجزائري قد تبنى صراحة الكتابة الالكترونية وأقر المساواة بين الحجية المقررة للكتابة على الورق عندما تستجيب لمتطلبات المادة 323 مكرر وهي أن تكون محددة الهوية وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها، هذا يعني أن الكتابة لا تعتبر دليلا إذا اشتملت على توقيع صاحبها وأن تكون تحت سيطرته الحصرية، وأن أي تعديل أو تغيير في بياناته يكون قابلا للكشف، ولكي تتحقق تلك الشروط يجب أن يتم إنشاء التوقيع الالكتروني وفق البيانات المحددة والمتمثلة في إجراءات توثيق التوقيع منها استخدام تقنيات خاصة التي تحمله توقيعا موثوقا به، فتصدر بشأنه شهادة تصديق

[1]- أزاد دزه يي، المرجع السابق، ص 176-177.

[2]- المادة 323 مكرر 01 من القانون المدني رقم 15-10 المؤرخ في 2005/07/20م منشور بالجريدة الرسمية رقم 44، ص 25.

الكترونية من جهة مختصة بذلك والموثوق بها حينئذ يمكن القول أنه يكشف حجية الإثبات شأنه شأن الكتابة التقليدية وقد سبق وأن قلنا أن المشرع الجزائري قد تبنى ازدواجية التوقيع الالكتروني أي التوقيع الالكتروني العام والبسيط والتوقيع الالكتروني المؤمن أو المتقدم، ومن جهة أخرى اعترف بحجية التوقيع الالكتروني كورقة عرفية دون الورقة الرسمية والتي تبقى خاضعة للقواعد العلمية إلا أن بعض التشريعات الأجنبية لم تضع هذا التمييز، واعترفت بحجية الكتابة الالكترونية العرفية والرسمية معا[1].

حجية التوقيع الالكتروني العام والمؤمن

رغم أن معظم التشريعات أخذت بمبدأ الحياد تجاه تقنيات التكنولوجيا المتاحة لتحقيق حجية التوقيع الالكتروني، إلا أن الأمر استقر على وجود نوعين من التوقيع الالكتروني العام أي البسيط، أو التوقيع الالكتروني المؤمن، لكن هذه الازدواجية نتج عنها إشكالية متمثلة في مدى مساواة التوقيع الالكتروني العام بالتوقيع الالكتروني المؤمن، خصوصا أن هذا الأخير يصدر بشأن شهادة التصديق الالكتروني التي تقر بصحة التوقيع الالكتروني وسلامته من أي تعديل أو تزوير.

-حجية التوقيع الالكتروني العام:

قد يكون التوقيع الالكتروني توقيعا عاما بمعنى بسيط لاستخدم فيه تقنية خاصة لتأمينه وتوثيقه كما سبق وأن بينا، وبالرجوع إلى نص المادة 223 مكرر 01 من القانون المدني الجزائري التي جاء فيها "ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها أو طرق إرسالها" بمعنى أن التوقيع الالكتروني يتخذ هذه الأشكال والتي يمكن فهمها وقراءتها هو التوقيع الالكتروني العام والبسيط، أي ذلك التوقيع الذي لم يتم وفقا للشروط المنصوص عليها في المادة 03 من المرسوم 07-162 وهي أن يكون التوقيع الالكتروني خاصا بالموقع وأن يتم إنشاؤه بوسائل يمكن أن يحتفظ بها الموقع تحت رقابته الحصرية وأن يضمن من الفعل المرتبط به صلة بحيث يكون أي تعديل لاحق للفعل قابل للكشف فهو لا يستفيد من القرينة المنصوص عليها بهذه المادة كما أن التوقيع الالكتروني العام أو البسيط هو التوقيع الذي لم يصدر بشأنه شهادة مصادقة الكترونية

[1]- يمينة حوحو، المرجع السابق، ص 206.

من الجهة المؤهلة لذلك، أو أصدرت بشأنه شهادة مصادقة عامة حينئذ يكون لمن يتمسك به أن يثبت شروط الأمان والحفظ والسلامة المطلوبة منه.

هذا ويعتد بالتوقيع الالكتروني العام والبسيط متى كان صادرا من الشخص محدد الهوية وفي حالة النزاع عليه إثبات أن توقيعه كان معدا ومحفوظا في ظروف سليمة وآمنة وفي كل الحالات تقود السلطة التقديرية للقاضي في تقدير حجية التوقيع الالكتروني البسيط.

-حجية التوقيع الالكتروني المؤمن:

منح المشرع الجزائري للتوقيع الالكتروني للمؤمن الحجية الكاملة في الإثبات مثله مثل التوقيع التقليدي كورقة عرفية يترتب عليه جميع الآثار القانونية، عندما تتوفر لديه الشروط القانونية المطلوبة، عندئذ يستفيد التوقيع الالكتروني من الحجية بأنه خاص بالموقع دون غيره وإن إنشائه قد يتم بوسائل احتفظ بها تحت رقابته الحصرية دون سواه، وأن يضمن مع الفعل المرتبط به صلة، بحيث يكون أي تعديل أو تغيير لاحقا لفعل قابلا للكشف عنه، فمسألة حجية التوقيع الالكتروني من قوتها مرتبط بدرجة الوسائل التقنية المستعملة وبمدى نجاحها في توفير الأمان وصحة التوقيع الالكتروني وسلامته وأصبح التوقيع الالكتروني المؤمن يحقق وظائف أقوى من الوظائف التي يحققها التوقيع اليدوي، فضلا عن السرعة والتوقيع عن بعد[1].

المطلب الثاني: التصديق الالكتروني

تعتمد التجارة الالكترونية في إجراءاتها على شبكة مفتوحة كما أن غالبية العقود التي تتم بين أطرافها تعد من العقود المبرمة بين غائبين، وذلك بسبب اختلاف المكان وزمان التعاقد وغياب العلاقة المباشرة بين أطراف التعاقد، إذ أنهم في أغلب الأحيان لم يدخلوا في علاقات مع بعضهم البعض من قبل.

لذلك فإن توافر عنصري الثقة والأمان في هاتين الحالتين ليس مطلوبا بل ضروريا لتطوير التجارة الالكترونية وتنمية المبادلات الاقتصادية، ذلك ارتأت التشريعات الدولية والإقليمية والوطنية إيجاد وسيط طرف ثالث وظيفته توطيد العلاقات وتوثيقها بين الأشخاص الذين يعتمدون على الوسائط

[1]- يمينة حوحو، المرجع السابق، ص 212-213.

الالكترونية[1]، وإصدار شهادة تسمى شهادة التصديق الالكتروني، وذلك بعد التحقق من هوية ومضمون التصرف وسلامته من العيوب[2].

وبناءا على ما تقدم ماذا نقصد بالطرف الثالث؟ وكيف يمكن للأطراف المتعاقدة أن تبسط ثقتها عليه؟ بمعنى ماذا يقدم للأطراف المتعاقدة لكي يثقوا به؟

وبيان المزيد عن الجهة المختصة بإصدار شهادات التصديق الالكتروني سيحدث في الشروط والواجبات الملقاة على هذه الجهة، وماهية الشهادة الالكترونية التي تقدمها ومدى مسؤوليتها عن الإخلال بالواجبات المفروضة عليها وعليه سنقسم هذا المطلب إلى فرعين الأول: الجهة المختصة بإصدار شهادة التصديق الالكتروني، والثاني: خصوصيات شهادة التصديق الالكتروني..

الفرع الأول: الجهة المختصة بإصدار شهادة التصديق الالكترونية شهادة التوقيع الالكتروني:

إن الثقة والأمان لدى أطراف العقد الالكتروني هما من أولى الأمور التي يتعين توافرها في هذا النوع من التعاقد ولكي تتوافر هذه الثقة والأمان المستهدفان فإن الأمر يستلزم وجود طرف ثالث محايد سواء كان شخصا طبيعيا أم شخصا معنويا، وذلك حتى يضمن سلامة المحرر الالكتروني من العبث والاحتيال، ويؤمن عملية التوقيع الالكتروني وذلك بالتحقق من شخصية المتعاقدين.

أولا: تعريف الجهة المختصة بإصدار شهادات التصديق الالكتروني:

لقد اختلفت المصطلحات بشأن الجهات المختصة بإصدار شهادات التصديق الالكتروني فمنها ما يطلق عليها بمصطلح "سلطة الإشهار" ويعرفها بأنها "هيئة عامة أو خاصة تسعى إلى ملئ الحاجة الملحة لوجود طرف ثالث موثوق، يقدم خدمات أمنية في التجارة الالكترونية، بأن يصدر شهادات تثبت صحة حقيقة معينة متعلقة بموضوع التبادل الالكتروني لتوثيق هوية الأشخاص المستخدمين بهذا النوع من التوقيع الرقمي، وكذلك نسبة المفتاح العام المستخدم إلى صاحبه[3].

ومنها ما يطلق عليها بمصطلح "مؤدي الخدمة" كما هو وارد في نص المادة 03 من المرسوم 07-162 الجزائري، كما ورد في الفصل الثاني من القانون التونسي أو جهات التصديق كما جاء في نص المادة 01 من قانون التوقيع المصري أو "جهة التوثيق" كما جاء في قانون المعاملات الالكترونية الأردني.

---

[1]- عيسى غسان ربضي، مرجع سابق، ص 112.

[2]- سامي علي عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية ، مصر، 2007، ص 320.

[3]- عايض راشد المري، مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود التجارية، رسالة دكتوراه في الحقوق ، جامعة القاهرة، مصر1988، ص 100.

"يعرف مقدم خدمات التصديق الالكتروني بأنه "هيئة أو مؤسسة عامة أو خاصة تستخرج شهادات الكترونية، وتكون هذه الشهادة بمثابة سجل الكتروني يؤمن التوقيع الالكتروني ويحدد هوية الموقع، ومعرفة المفتاح العام وتعتبر شهادة التصديق بمثابة بطاقة هوية الكترونية تستخرج من شخص مستقل ومحايد ومرخص له بمزاولة هذا النشاط"[1].

كما يعرف أيضا على أنه "كل شخص طبيعي أو معنوي يستخرج الشهادات الالكترونية ويقدم الخدمات الأخرى المرتبطة بالتوقيعات الالكترونية، ويضمن تحديد هوية الأطراف المتعاقدة والاحتفاظ بهذه البيانات لمدة معينة، ويلتزم باحترام القواعد المنظمة لعمله، والتي يتم تحديدها بمعرفة السلطة المختصة[2].

استخدم قانون الأمم المتحدة النموذجي بشأن التوقيعات الالكترونية لسنة 2001م اصطلاح مقدم خدمات التصديق ووفقا للمادة 02/هـ/ التي تطرقت إلى تعريف مقدم خدمات التصديق فإنه يقصد به، "شخص يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الالكترونية[3].

كما ذهب القانون الإماراتي إلى التعريف ذاته والذي عرفها بأنها " أي شخص أو جهة معتمدة أو معترف بها، تقوم بإصدار شهادات التصديق الالكترونية أو أية خدمات أو مهام تتعلق بالتوقيع الالكتروني"[4].

بينما الفصل الثاني من الباب الأول من القانون التونسي رقم 83 لسنة 2000م بشأن المبادلات والتجارة الالكترونية حدد مفهوم مصطلح مزود المصادقة الالكترونية بأنه "كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة ويسدي خدمات أخرى ذات علاقة بالإمضاء الالكتروني"

كما أنشأ المشرع التونسي "الوكالة الوطنية للمصادقة الالكترونية" واعتبرها مؤسسة عامة، تتمتع بالشخصية المعنوية والاستقلال المالي وتخضع في علاقاتها مع الغير إلى التشريع التجاري التونسي ومعترف بها بتونس العاصمة، وقد حدد في الفصل التاسع من الباب الثالث من القانون السابق أهداف هذه الوكالة منها:

- السهر على مراقبة احترام مزود خدمات المصادقة الالكترونية للقانون.

---

[1]- لالوش راضية، مرجع سابق، ص 106.

[2]- سامي علي حامد عياد الجريمة المعلوماتية وإجرام الانترنت ،دار الفكر الجامعي ،الإسكندرية ،مصر 2007 ، ص 322.

[3]- خالد ممدوح إبراهيم، مرجع سابق، ص 173.

[4]-إبراهيم الدوسقي أبو الليل، مرجع سابق، ص 56.

- إصدار وتسليم وحفظ شهادات المصادقة الالكترونية.
- إبرام اتفاقيات الاعتراف المتبادل الخاص بمزودي خدمات التصديق الالكتروني مع الأطراف الأجنبية[1].

هذا ويتعين على كل من يرغب بممارسة نشاط مزود خدمات المصادقة الالكترونية الحصول على ترخيص مسبق من الوكالة الوطنية للمصادقة الالكترونية ويشترط للحصول على هذا الترخيص توافر العديد من الشروط[2].

أما قانون المعاملات الالكتروني الأردني رقم 85 لسنة 2001 لم يورد أي تعريف للجهة المختصة بإصدار شهادات التصديق الالكترونية، حيث خول المشرع الأردني لمجلس الوزراء بإصدار الأنظمة والأحكام التي تحدد الجهة التي تشرف على ترخيص مقدمي خدمات التصديق، وطرق إجراء إصدار الشهادات، وسائر الأمور المرتبطة بها[3].

أما قانون التوقيع الالكتروني المصري رقم 15 لعام 2004 فقد جاء خاليا من ثمة تعريف لجهة التوثيق الالكتروني، وأنه كان حظر مزاولة نشاط إصدار شهادات التصديق الالكتروني إلا بعد الحصول على ترخيص بذلك من الهيئة المختصة وهي هيئة تنمية صناعة تكنولوجيا المعاملات وفقا للإجراءات والضمانات التي تحددها اللائحة التنفيذية كما وضع عقوبة جنائية في حالة مخالفة ذلك فقد أقر المشرع المصري العديد من الاختصاصات لهيئة تنمية صناعة تكنولوجيا المعلومات أهمها منح وتجديد تراخيص مزاولة نشاط خدمات التوقيع الالكتروني، متابعة ومراقبة نشاط مقدمي خدمات التصديق الالكتروني[4] الذين يعهد إليهم إنشاء منظومة التوقيع الالكتروني، تحديد معاييرها، ضبط مواصفاتها الفنية، إصدار شهادة تصديق الكتروني وكذلك التصديق على المعاملات الالكترونية كما ألزم المشرع المصري على ضرورة الحصول على ترخيص من الهيئة قبل مزاولة أي نشاط، ويكون لهيئة تنمية صناعة تكنولوجيا المعلومات كامل السلطة في إلغاء الترخيص عند مخالفة شروط الترخيص[5].

أما المشرع الجزائري قد جاء تعريفه لمؤدي خدمات التصديق الالكتروني في الفقرة 16 من المادة 03 من المرسوم التنفيذي الجزائري رقم 67-162 المؤرخ في 30 ماي 2007 الجهات المختصة في التصديق

[1]- الفصل التاسع من نفس القانون.

[2]- الفصل الخامس عشر من الباب الرابع من نفس القانون.

[3]- المادة (48/ب) من القانون الأردني رقم 2001/85 بشأن المعاملات الالكترونية.

[4]- المادة (04) من القانون المصري رقم 15 لسنة 2004 بشأن تنظيم التوقيع الالكتروني.

[5]- المادة 26 من قانون التوقيع الالكتروني المصري رقم 15/ 2004 والمادة 23 من اللائحة التنفيذية لهذا القانون.

الالكتروني بما يلي: "مؤدي خدمات التصديق هو كل شخص في مفهوم المادة 08-08 من قانون رقم 03-2000 المؤرخ في 2000/5/8" وبالرجوع إلى نص المادة 05 فقرة 08 من القانون رقم 03-2000 المؤرخ في 2000/5/8 والمتعلق بالقواعد العامة المرتبطة بالبريد والمواصلات السلكية واللاسلكية فقد عرفت موفر الخدمة بأنه "كل شخص معنوي أو طبيعي يقدم خدمة مستعملا وسائل المواصلات السلكية واللاسلكية"[1].

كما نظم المرسوم التنفيذي رقم 07-162 المذكور نشاط التصديق الالكتروني بإخضاعه لنظام الترخيص المنصوص عليه في المادة39 من القانون 03-2000 وقد نفت المادة 03 من المرسوم التنفيذي 07-162 على أنه يخضع لترخيص تمنحه سلطة الضبط للبريد والمواصلات السلكية واللاسلكية إنشاء واستغلال خدمات التصديق الالكتروني.

وبالرجوع إلى نص المادة 39 من القانون رقم 03-2000 المؤرخ في 2000/12/5 فإنها تنص على أنه "يمنح ترخيص الضبط لكل شخص طبيعي أو معنوي يلتزم باحترام الشروط التي تحددها سلطة الضبط في مجال إنشاء واستغلال الشبكات أو تقديم الخدمات الخاضعة لنظام الترخيص، هذا وفقا لنص المادة 03 من المرسوم نفسه 67-162 فقد يكون مؤدي خدمات التصديق أجنبيا أي من جنسية أجنبية، لكن عليه أن يستجيب للشروط المطلوبة قانونا.

أما المشرع الفرنسي فقد أطلق عليه اسم المكلف بخدمة التوثيق الالكتروني بموجب المادة رقم 1 الفقرة 11 من المرسوم رقم 2001/272 الصادر بتاريخ 2001/3/30 بأنه" كل شخص يصدر شهادات الكترونية أو يقدم خدمات أخرى متعلقة بالتوقيع الالكتروني.

ثانيا: الشروط الواجب توفرها في الجهة المختصة بإصدارشهادات التصديق الالكترونية

لابد من توافر بعض الشروط في كل شخص سواء أكان طبيعيا أم معنويا يتقدم بطلب إلى الجهة المختصة، للحصول على ترخيص لممارسة مهنة إصدار شهادات التصديق الالكترونية، وذلك لتحقيق مدى معين من الأمان والثقة في التوقيع الالكتروني، ولإثبات أنه محل ثقة بممارسة مهنة إصدار شهادات التصديق الالكترونية[2].

[1]- يمينة حوحو، مرجع سابق، ص 190.

[2]- ثروت عبد الحميد ، مرجع سابق، ص 162.

ومن هذه الشروط الشخصية كما هو وارد في قانون المبادلات والتجارة الالكترونية التونسي، إذ اشترط على مزود خدمات المصادقة الالكترونية، سواء كان شخص طبيعي أو ممثلا قانونيا لشخص معنوي، والذي يرغب في الحصول على ترخيص لتعاطي نشاط مزود خدمات المصادقة توافر الشروط التالية:

1- أن يكون من ذوي الجنسية التونسية منذ خمس أعوام على الأقل.

2- أن يكون حاصلا على شهادة الأستاذية أو ما يعادلها.

3- أن يكون مقيما بالبلاد التونسية.

4- أن يكون متمتعا بالحقوق المدنية والسياسية ونقي السوابق القضائية.

5- أن لا يتعاطى نشاطا مهنيا آخر[1].

أما بالرجوع إلى المشرع الجزائري فإنهأحكام المادة 34 من القانون رقم 15-04 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، تحديد الشروط التي يجب على كل طالب ترخيص لتأدية خدمة التصديق الالكتروني أن يستوفيها، ويتعلق الأمر ب الشروط الآتية:

- أن يكون خاضعا للقانون الجزائري للشخص المعنوي أو الجنسية الجزائرية للشخص الطبيعي
- أن يتمتع بقدرة مالية كافية.
- أن يتمتع بمؤهلات وخبرة ثابتة في ميدان تكنولوجيا الإعلام والاتصال للشخص الطبيعي أو المسير للشخص المعنوي
- أن لا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع نشاط تأدية خدمات التصديق الالكتروني.

ومن الشروط الأخرى التي يجب توافرها بالجهة المختصة بإصدار شهادات التصديق الالكترونية، شروط يمكننا القول أنها شروط فنية كأن يكون الشخص الطبيعي أو الممثل المعنوي ذا كفاءة مهنية في ممارسة نشاط إصدار شهادات التصديق كأن يكون مهندس تقنيات حديثة أو من مبرمجي الحاسبات الالكترونية أو أن تكون لديه خبرة مهنية بمجال عمله، وهذا الشرط هو أحد المتطلبات الأساسية التي حددها التوجيه الأوروبي للجهة المختصة بإصدار شهادات التصديق.

[1]- عيسى غسان ربضي، مرجع سابق، ص 124.

فالمادة 2 من الملحق الثاني التابع للتوجيه الأوروبي بشأن التوقيعات الالكترونية، الذي ينظم المتطلبات الخاصة بالمكلفين بخدمة التوثيق الذين يصدرون شهادات موصوفة، تنص على أنه يجب على المكلفين بخدمات التوثيق "الاستعانة بموظفين متمتعين بالمعارف النوعية والخبرة والتوصيفات الضرورية لتوريد الخدمات وعلى الأخص الاختصاصات على مستوى الإدارة والمعارف المتخصصة تكنولوجيا في التوقيعات الالكترونية".

هذا ولم ينص المشرع الجزائري عليها ضمن المرسوم 07- 162 لكن أشار إليها في المادة 03 فقرة 11 من المرسوم نفسه بقوله لأن "مؤديا للخدمات على التصديق الالكتروني يقدم خدمات مطابقة لمتطلبات نوعية خاصة" ويقصد بالنوعية الخاصة مجموعة المؤهلات المذكورة والتي تحدد في الغالب من خلال التنظيم وبالرجوع إلى القانون الفرنسي مثلا نجد أن المادة 02 من المرسوم 2001-272 المؤرخ في 2001/03/30 المتعلق بالتوقيع الالكتروني قد حددت تلك المؤهلات منها أن خدماته موثوق بها "وأن يمسك سجلا الكترونيا يقيد كل الشهادات المصادقة الالكترونية إذ يوظف إطارات مختصة في مجال المصادقة الالكترونية بما في ذلك استعمال تقنيات مخصصة ومناسبة في توثيق المعطيات وسلامتها، واتخاذ كل الإجراءات التي من شأنها تجنيب كل التحريف والتزوير متى توافرت كل المؤهلات في الجهة التي تزيد مزاولة الخدمات الالكترونية تستفيد حينئذ من شهادة تأهيل للقيام بخدمات التصديق الالكتروني.

وقد عرفت المادة 03 فقرة 10 من المرسوم التنفيذي الجزائري أهلية مؤدي الخدمات الالكترونية بأنه "الوثيقة التي تثبت من خلالها بأن مؤديا لخدمات التصديق الالكتروني يقدم خدمات مطابقة لمتطلبات نوعية خاصة"

ولم يعرف المشرع الجزائري تلك الوثيقة عكس المشرع الفرنسي الذي جاء مجمل تعريفه لها في المادة 01 فقرة 12 من مرسوم 2001-272 بأنها قرار صادر من الغير وهو هيئة التأهيل تصرح أو تشهد بأن مؤدي خدمة المصادقة الالكترونية يزود الخدمات الالكترونية بالشروط المطلوبة الخاصة بالتأهيل، أما في تونس فهي الوكالة الوطنية للمصادقة الالكترونية.

ثالثا: اختصاصات مؤدي خدمات التصديق الالكتروني

مع تعدد التشريعات التي نظمت أحكامهم نشاط الجهة المختصة بإصدار شهادات التصديق الالكترونية، اختلفت الالتزامات التي يجب على هذه الجهة التقيد بها من التشريع الآخر، إلا أنه توجد التزامات مشتركة بين هذه التشريعات وهي:

أ- التأكد من صحة البيانات المدونة في شهادة التصديق الالكترونية

إن أهم اختصاص يسند لمؤدي خدمات التصديق الالكتروني هي عملية التصديق الالكتروني التي تهدف إلى ضمان صحة البيانات الالكترونية وسلامتها والتأكد من هوية الموقع وصحة توقيعه وسلطاته في التوقيع[1]، حيث جاء نص المادة 03 فقرة 10 من المرسوم التنفيذي الجزائري رقم 07-162 ما يلي: يسلم شهادات الكترونية أو يقدم خدمات أخرى في مجال التوقيع الالكتروني، معنى هذا أن مؤدي خدمات التصديق إلى جانب تسليمه لشهادات المصادقة الالكترونية فهو يقوم بأداء خدمات أخرى مرتبطة بالتوقيع الالكتروني وهي متنوعة مثل حفظ الوثائق الالكترونية واتخاذ التدابير اللازمة لتوفير الحماية لها وفقا للشروط والضوابط المنصوص عليها قانونا أي أن يقوم بالتحقق من التوقيع الالكتروني قد تم تنفيذه من شخص معين ومحدد.

فبفضل التصديق الالكتروني يمكن تحديد هوية المتعامل وربط معطيات تعامله مع ضمان سلامة هذه المعطيات وصحتها بواسطة شهادة التصديق الالكتروني[2].

ب- الالتزام بالسرية

ويقصد بالسرية الحفاظ على البيانات ذات الطابع الشخصي المقدمة من العميل إلى الجهة المختصة بإصدار شهادات التصديق الالكترونية، ولقد أوصى التوجيه الأوروبي بشأن التوقيعات الالكترونية في المادة 1/8 دون الاعتماد بأن تتعهد بأن تلتزم الجهات التي تصدر شهادات التصديق الالكترونية بالحفاظ على كل البيانات ذات الطابع الشخصي[3] وقد تبنت التشريعات الوطنية ما نص عليه التوجيه الأوروبي قد نص الفصل 15 من قانون المبادلات الالكترونية الفرنسي على "يتعين على مزودي خدمات المصادقة الالكترونية وأعوانهم المحافظة على سرية المعلومات الواردة فيه ويمنع عليه استعمالها خارج المصادقة الالكترونية"[4].

ج- إلغاء أو إيقاف العمل بشهادة التصديق.

تلتزم الجهة المختصة بإصدار شهادات التصديق الالكترونية بإلغاء أو إيقاف شهادة التصديق في حالة وجود سبب يقيني يوجب ذلك، فقد يتضح لهذه الجهة وجود تغيير جوهري في بيانات شهادة

[1]- عيسى غسان ريضي، مرجع سابق، ص 132.

[2]- يمينة حوحو، ، مرجع سابق، ص 196.

[3]- ثروت عبد الحميد ، مرجع سابق، ص 165.

[4]- عيسى غسان ريضي، مرجع سابق، ص 134.

التصديق الالكترونية، كما لو علمت بتزوير الوثائق المقدمة لها من ذوي الشأن لإصدار شهادة التصديق، أو تبين لها من جراء تحرياتها أن الشخص الذي صدرت الشهادة باسمه فقد أهليته أو أفلس أو فقد وظيفته وتتعقد مسؤولية هذه الجهة إذا لم تتخذ الإجراءات اللازمة لإلغاء أو تعليق الشهادة الالكترونية[1].

الفرع الثاني: شهادة التصديق الالكترونية

لقد تعددت وظائف جهات التصديق الالكتروني، وذلك على نحو عرضناه سالفا وكان من أهم تلك الوظائف هو قيامها بإصدار التصديق الالكتروني ونظرا لأهمية تلك الشهادة كونها أهم دور تقدمه جهات التوثيق من ناحية ومن ناحية أخرى، كونها أهم دور قدمه جهات التوثيق من ناحية أخرى كونها بتت الثقة والأمان لدى المتعاملين عبر الانترنت، فقد ارتأينا أن نتعرض لها في هذا الفرع من حيث مفهومها وبياناتها وأنواعها وكذا وظائفها[2].

أولا: تعريف شهادة التصديق الالكتروني.

نظرا لأهمية شهادة التوثيق الالكترونية في مجال التجارة الالكترونية وخاصة في مجال الإثبات سارعت العديد من التشريعات التي نظمت التوقيع الالكتروني بتعريف هذه الشهادة مبينة المقصود بها.

فقد اختلفت المصطلحات بشأن هذه الشهادة متأثرة بالمصطلحات المستعملة في عالم الانترنت وتكنولوجيا الإعلام فقد تسمى بالشهادة الالكترونية أو شهادة رقمية أو بشهادة الثقة الرقمية أو شهادة التوثيق.

فقد عرفها قانون الأونيسترال النموذجي بشأن التوقيعات الالكترونية فقد حدد مفهومها على أنها "تعني رسالة بيانات أو سجلا آخر يؤكد الارتباط بين الموقع وبيانات إنشاء التوقيع"[3].

أما التوجيه الأوروبي لسنة 1999 فقد ميز في المادة 02 منه في الفقرتين التاسعة والعاشرة ما بين الشهادة الالكترونية البسيطة والشهادة الالكترونية الموصوفة المؤكدة، وعرفتها على أنها "الشهادة الالكترونية التي تربط البيانات الخاصة بفحص التوقيع الالكتروني والشخص المعين وتؤكد هوية هذا الشخص أما الشهادة الثانية فهي شهادة مؤهلة تستوفي الشروط أو المتطلبات المنصوص عليها في الملحق. 01

[1]- Mechal Jaccard, problème juridique les transactions sur le réseaux, édition 2000.، p3

[2]- Adel Brahim, signature électronique et droit, édition Ms،Tunisie, 2004, p23

[3]- المادة 02 فقرة ب من قانون الأونيسترال النموذجي بشأن التوقيعات الالكترونية لسنة 2001م.

وتقدم بواسطة مقدم خدمات التصديق المستوفي للمتطلبات المنصوص عليها في الملحق02"[1].

كما عرف القانون التونسي رقم 2000/83 بشأن المبادلات والتجارة الالكترونية شهادة التصديق الالكترونية في الباب الأول بأنها:

"الوثيقة الالكترونية المؤمنة بواسطة الإمضاء الالكتروني للشخص الذي أصدرها والذي يشهد من خلالها أثر المعاينة على صحة البيانات التي تتضمنها".

أما المشرع الأردني: فقد عرفها على أنها " وثيقة الكترونية على شكل شهادة رقمية تصدر عن جهة التصديق الالكتروني تثبت نسبة المعطيات للموقع.

أما المشرع المصري: فقد بين المقصود بشهادة التصديق الالكتروني معرضا إياها في المادة الأولى فقرة 09 من قانون التوقيع الالكتروني رقم 15-04" بأنها الشهادة التي تصدر من جهة مرخص لها بالتصديق وتثبيت الارتباط بين الموقع وبيانات إنشاء التوقيع[2].

وكذا نجد أن المشرع الجزائري حدد المقصود بشهادة التصديق الالكتروني في المادة 03 فقرة 08 من المرسوم التنفيذي رقم 07-162 بقولها "هي وثيقة في شكل الكتروني تثبت الصلة بين معطيات فحص التوقيع الالكتروني والموقع.

ونجد أيضا المادة 03 مكرر 7 من المرسوم الجزائري رقم 07-162 عرف شهادة المصادقة الالكترونية على أنها وثيقة تصدرها جهة التصديق الالكتروني، تدل على الربط بين صاحبها ومضمونها، فتكون تلك الوثيقة في شكل الكتروني مخزن في شكل بيانات رقمية حسب تقنية محددة سلامتها من التغيير أو التزوير أو استعمالها من الغير[3].

كما تعرف أيضا على أنها مستند يصادق على معلومات معينة مدرجة فيه، أو ترتبط به ارتباطا منطقيا[4].

هذا ويتعين أن تحتوي شهادة التصديق الالكتروني على بيانات إلزامية كما تأخذ نموذجا معينا أو تستعمل لمدة محددة وفي مجالات مختلفة قصد تحقيق وظائف محددة.

---

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص 217.

[2]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 103.

[3]- يمينة حوحو، مرجع سابق، ص 198.

[4]VinezoSins, digital Europe international Lawer, Decembre 2000, p 64.

ثانيا: البيانات الإلزامية لشهادة المصادقة الالكترونية.

يجب أن تتضمن شهادة التصديق الالكترونية جملة من البيانات الإلزامية والضرورية لكي تكون لها حجية قانونية في الإثبات، ولقد اختلفت التشريعات المقارنة في تحديد هذه البيانات فقد نصت المادة 20 من قانون التوقيع الالكتروني المصري على أن "تحدد اللائحة التنفيذية البيانات التي يجب أن تشتمل عليها شهادة التصديق الالكتروني".

1- شخصية مقدم خدمة التوثيق والدولة التي نشأ بها لممارسة اختصاصه.

2- اسم الموقع الفعلي، صاحب الشهادة.

3- ميزة خاصة للموقع حسب الاستعمال الذي منحت الشهادة لأجله.

4- تحديد المفتاح العام.

5- تحديد مدة صلاحية الشهادة من بدايتها وحتى نهاية صلاحيتها.

6- الرقم التسلسلي الخاص بالشهادة.

7- التوقيع الالكتروني لمقدم خدمة التصديق الالكتروني.

8- حدود استخدام الشهادة عند الطلب.

9- تحديد قيمة الصفقات التي يمكن استخدام الشهادة بشأنها.

وهذه البيانات بعضها يكون لازم والآخر اختياري أو قد أتاحت التوجيهات الأوربية لمقدم خدمات التصديق وضع شروط تعد قيد على استخدام الشهادة أو يشترط في ذلك أن يكون بإمكان الطرف المتعامل مع صاحب الشهادة العلم بها، وأجازت المادة 03/08 من التوجيهات الأوربية بمقدم خدمات التصديق الالكتروني وضع اسم مستعار على الشهادة مع إمكانية التحقق من هوية الموقع[1].

هذا وقد نص التشريع الجزائري أيضا على البيانات التي يجب أن تشملها الشهادة كما هو منصوص عليه في التشريع المقارن فنجد مثلا المادة 06 فقرة 01 من المرسوم التنفيذي الفرنسي رقم 2001-272 المؤرخ في 2001/03/30 نص على مجموعة من البيانات الإلزامية التي يجب أن تحتويها شهادة المصادقة الالكترونية الموصوفة ويمكن حصر هذه الشروط الشكلية كما يلي:

[1]- إيمان مأمون أحمد سليمان، الجوانب القانونية للتجارة الالكترونية، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، قسم القانون التجاري، مصر 2006، ص 321.323.

تحديد هوية صاحب الشهادة سواء الحقيقية أو الالكترونية وكذا طبيعته القانونية إن كان ممثلا عن شخص آخر.

- هوية مزود خدمة المصادقة الالكترونية.
- عناصر التدقيق في إمضاء صاحب الشهادة.
- مدة صلاحية الشهادة.
- الرقم التعريفي للشهادة.
- وصف شهادة بأنها مؤمنة[1].

-شهادة التصديق الالكتروني:

عرفتها المادة 7/1 من اللائحة التنفيذية لقانون التوقيع الالكتروني بأنها: "الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع" والغرض من إصدار جهات التصديق الالكتروني للشهادة هو الشهادة والإقرار بصحة التوقيع الالكتروني ونسبته لمن أصدره وأنه مستوفي لجميع الشروط والمعايير الفنية والتقنية التي نص عليها قانون التوقيع الالكتروني ولائحته التنفيذية[2].

ب-هذا ونجد أيضا أن المشرع الجزائري قد تبنى أيضا أنواع شهادة التصديق الالكتروني وهذا على النحو الآتي:

- **شهادة المصادقة الالكترونية العامة والموصوفة:**

لقد تبنى المشرع الجزائري مفهومين للتوقيع الالكتروني وهما التوقيع الالكتروني العام أو المسمى أيضا بالبسيط والتوقيع الالكتروني المؤمن ونتيجة لذلك يوجد شهادة المصادقة الالكترونية العامة أو البسيطة وشهادة الكترونية مؤمنة والتي سماها المشرع الجزائري شهادة الموصوفة، ومن ثم فإن شهادة التصديق الالكتروني هي الأخرى تكون إما:

1- شهادة مصادقة الكترونية عامة:

[1]- يمينة حوحو، مرجع سابق، ص 200.

[2]- محمد أمين الرومي، النظام القانوني للتوقيع الالكتروني، دار الكتب القانونية، مصر ،2007، ص55.

إن شهادة المصادقة الالكترونية العامة أو البسيطة هي الشهادة المنصوص عليها في المادة 3 مكرر 8 من المرسوم التنفيذي 07-162 "هي وثيقة في شكل الكتروني تثبت الصلة بين معطيات فحص التوقيع الالكتروني والموقع"[1] إذ هي شهادة صادرة من جهات المصادقة الالكترونية المتنوعة، وتثبت الصلة بين معطيات التوقيع الالكتروني والموقع فتحدد هوية الشخص الموقع وتثبت الارتباط لمعطيات التوقيع الالكتروني به.

ثالثا: أنواع شهادة المصادقة الالكترونية:

لقد اختلفت أنواع الشهادات المتعلقة بالمصادقة الالكترونية في التشريعات المقارنة.

فنجد أن المشرع المصري حددها بأربعة صور وهي:

- **شهادة فحص بيانات إنشاء الموقع الالكتروني:**

نصت المادة 01/20 من اللائحة التنفيذية لقانون التوقيع الالكتروني على تعريفها شهادة فحص بيانات التوقيع الالكتروني على أنها: " شهادة تصدرها الهيئة نتيجة الفحص والتحقق من صحة بيانات إنشاء التوقيع الالكتروني، فيمكن أن يتقدم ذوي الشأن بطلب لهيئة تنمية صناعة تكنولوجيا المعلومات للفحص والتأكد من صحة بيانات التوقيع الالكتروني مقابل مبلغ يحدده مجلس إدارة الهيئة[2].

- **شهادة فحص التوقيع الالكتروني:**

نصت المادة 1/21 من اللائحة التنفيذية لقانون التوقيع الالكتروني المصري على تعريف شهادة فحص التوقيع الالكتروني وهي "شهادة تصدرها الهيئة بنتيجة فحصها لسلامة وصحة التوقيع الالكتروني وهذه الشهادة يجوز تقديمها بناءا على طلب من ذوي الشأن لهيئة تنمية صناعة تكنولوجيا المعلومات مقابل رسم تحدده الهيئة ويمكن للهيئة أن تعهد للغير بتقديم الخدمة تحت إشرافها ولكن تصدر الهيئة في كافة الأحوال شهادة فحص التوقيع الالكتروني[3].

- **شهادة اعتماد جهات التصديق الالكتروني الأجنبية:**

نصت المادة 1/22 من اللائحة التنفيذية لقانون التوقيع الالكتروني على تعريف شهادة اعتماد جهات التصديق الالكتروني الأجنبية بأنه: "شهادة تصدرها هيئة تنمية صناعة تكنولوجيا المعلومات باعتماد

[1]- المادة 03 مكرر 08 من المرسوم التنفيذي 07-162 السالف الذكر.

[2]- حسام محمد الشنراقي، مرجع سابق، ص 107.

[3]-سعيد سيد قنديل، التوقيع الالكتروني، دار الجامعة الجديدة، الإسكندرية، مصر، 2006، ص 59.

جهات التصديق الالكتروني الأجنبية وما تصدره هذه الجهات من شهادات التصديق الالكتروني النظيرة للشهادات الصادرة داخل مصر.

وتختص الهيئة باعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الالكتروني بمقابل تحدده ثم تقوم بعد ذلك بإصدار شهادة تفيد اعتماد هذه الجهة باعتبارها من جهات التصديق الالكتروني بمصر، وبذلك تصبح لها نفس الحجية القانونية المقررة للشهادات الوطنية بمصر[1].

2- شهادة المصادقة الالكترونية الموصوفة:

نصت المادة 03 مكرر 09 من نفس المرسوم على أن شهادة المصادقة الالكترونية الموصوفة بأنها: "الشهادة الالكترونية التي تستجيب لمتطلبات محددة" أي أن شهادة التصديق الالكتروني الموصوفة هي الناتجة عن التوقيع الالكتروني المؤمن الذي يستجيب لمتطلبات محددة، أي تلك المتطلبات المنصوص عليها في المادة 03 فقرة 03 فتقوم بتقديم الدليل بطريقة موثوقة وقد سبق وأن قلنا أن المشرع الجزائري لم ينص على البيانات التي يجب أن تحتويها شهادة المصادقة الالكترونية سواء عامة أو خاصة ونذكر أن ما جاء به المشرع الفرنسي ضمن المرسوم رقم 2001-272 المؤرخ في 2001/03/30 حيث نصت المادة 06 مكرر 01 إلى 11 على أن البيانات الإلزامية خاصة التي يجب أن تشملها شهادة مصادقة.

- الإشارة إلى أن الشهادة صادرة بغرض المصادقة الالكترونية.
- تحديد هوية مزود الخدمة، وإن كان أجنبيا تحديد الدولة التي ينتمي إليها.
- تحديد اسم الموقع أو اسمه المستعار.
- تحديد صفة الموقع حسب استعمال تلك الشهادة.
- تحديد مدة بداية صلاحية الشهادة ونهايتها.
- رقم تعريف الشهادة.
- توقيع خاص بمزود خدمة المصادقة الالكترونية.
- بيان يحدد شروط استعمال الشهادة خصوصا تحديد المبلغ الأقصى للمبادلة التي من اجلها صدرت الشهادة[2].

رابعا: مجال الشهادة ومدة استخدامها

[1]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 108.

[2]- يمينة حوحو، مرجع سابق، ص 204،203.

يتعين كذلك أن تتضمن شهادة المصادقة الالكترونية الغرض من إنشائها ومجال استعمالها، فقد تكون بغرض إثبات وفاء الكتروني أو بغرض إثبات دين تم بطريقة الكترونية أو بغرض إثبات تعاقد الكتروني.

فمجال استعمالها يكون في التصرفات التي يمكن إجراؤها عبر الشبكة وبطريقة الكترونية، ومن جانب آخر فإن شهادة المصادقة الالكترونية هي شهادة محددة من حيث المدة حيث تتضمن معلومات تخص مدة صلاحية الشهادة لأن الشهادة الالكترونية ليست شهادة محددة المدة وإنما صلاحية استعمالها محددة بمدة زمنية معينة تبتدئ من تاريخ كذا وتنتهي بكذا[1].

خامسا: وظائف شهادة المصادقة الالكترونية:

تؤدي شهادة التوثيق الالكتروني أدوار متعددة فإلى جانب وظيفة تحديد هوية صاحبها "identification"وكذلك تحديد سلطاته وأهليته وأوصافه المهنية مثال ذلك أنها تمكن من التحقق من أن هذا الشخص هو بالفعل صيدلي أو محامي أو غير ذلك[2]. وبذلك فإنه من خلال شهادة التوثيق الالكترونية تتلاشى مخاطر إبرام العقد من أطراف ناقصة الأهلية أو من غير ذي صفة.

كذلك تثبت شهادة التوثيق الالكترونية أن التوقيع صحيح حيث تمنحه الحجية الكاملة كما تثبت أن بيانات الرسالة الموقع عليها صحيحة ولم يطرأ عليها أي تغيير أو تبديل.

وتمكن هذه الشهادة أيضا من معرفة المفتاح العام من خلاله يتم التأكد من المعلومات المرسلة، نظرا للارتباط بين هذا المفتاح والمفتاح الخاص.

كما تثبت وجود ارتباط بين زوج مفاتيح العام والخاص وبين الشخص الذي تحققت شخصيته.

إن إبرام العقد الالكتروني من خلال اللجوء لجهات التوثيق والحصول على شهادة التوثيق الالكتروني يضمن عدم إنكار أي من الطرفين لتوقيعه على العقد حيث يتم التوقيع من خلال المفتاح الخاص الذي

[1]- لقد نص الفصل 17 من قانون التجارة الالكترونية التونسي على ما تتضمنه شهادة المصادقة الالكترونية ومن بينها مدة صلاحية الشهادة ومجالات استعمالها، وهو ما نصت عليه أيضا المادة 20 من اللائحة التنفيذية لقانون 2004 المصري الخاص بالتوقيع الالكتروني.

[2]-إيمان مأمون أحمد سليمان، المرجع السابق، ص 325.

يثبت شخصية الموقع ويؤكد رضاه وقيامه بالتوقيع أو ادعاءه بأن صلب العقد قد تم تعديله أو تغييره وذلك لتوثيقه من تلك الجهات.

هذا ويمكن إجمال دور شهادة التوثيق الالكتروني في أنها سجل معلوماتي موقع بإمضاء الكتروني يحقق هوية مصدر الشهادة ويحقق هوية الموقع ويعطي مفتاحه العام مما يعني أنها بطاقة هوية الكترونية ذات حجية قانونية في الإثبات.

كما اشترطت التوجيهات الأوروبية الصادرة في13 ديسمبر 1999 وجود هذه الشهادة حتى يمنح التوقيع الالكتروني حجية وصلاحية إبرام العقد الالكتروني وإثباته.

وفي الولايات المتحدة الأمريكية نص القانون بالتوقيع الالكتروني والتصرفات الرقمية على استخدام هذه الشهادات[1].

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص 226-227.

المبحث الثاني: أنماط الحماية التقنية للتوقيع الالكتروني

تتعدد صور الحماية التقنية للتوقيع الالكتروني بحسب الطريقة التي يتم بها هذا التوقيع، كما تتباين هذه الصور من حيث درجة الثقة ومستوى ما تقدمه من ضمان، بحسب الإجراءات المتبعة في إهدارها وتأمينها، والتقنيات التي تتيحها[1].

ومن ثم فإن تقييم جدوى وسيلة الحماية التقنية ترتبط بمدى استيعابها لعناصر من المعلومات والتي تلخص في الآتي:

1-السرية: وتعني التحقق من أن المعلومات لا يتسنى الاطلاع عليها لغير المخول له بذلك[2].

2-تكامل البيانات: ونعني أن الرسالة البيانات تكون بمنآى عن أي عبث بأي جزء من محتواها[3].

3-التوثيق: أي ضرورة وجود آلية للاحتفاظ برسالة البيانات بحيث يمكن الرجوع إليها عند الحاجة.

4-عدم الإنكار: ويعني ذلك ضرورة إسباغ الحجية في الإثبات على مضمون التصرف محل الرسالة، بحيث لا يكون بوسع الموقع عليها إنكار توقيعه[4].

ومن ناحية أخرى، فيجب أن تتوافر آلية يكون من شأنها تحقق طرفي التعاقد من أن التوقيع المنسوب للطرف الآخر قد صدر عن يد محبة دون أن يداخله شبهة تناول من حجيته، ومن صور الحماية، التشفير وكذا استخدام أدوات القياس الحيوي وهذا الأمر يتطلب الوقوف على موقف التشريعات المقارنة من هذا الأمر وسوف نتناول ما تقدم بالبحث كل في مطلب مستقل على النحو التالي:

المطلب الأول: حماية التوقيع الالكتروني بواسطة التشفير

تعتبر وسيلة تشفير الرسائل الالكترونية إحدى وسائل حماية سلامة وسرية المعلومات المرسلة عبر شبكة عامة، فالتشفير يعتبر أفضل تقنية لحماية البيانات من أي تعديل غير مرغوب فيه، حيث يتم باستخدام أدوات ووسائل وأساليب لتحويل المعلومات بهدف إخفاء محتوياتها أو الحيلولة دون تعديلها أو استخدامها الغير مشروع.

---

[1]- ثروت عبد الحميد، مرجع سابق، ص54.

[2]- Lionel (b), internet et commerce électronique, 2eme édition, Delmas 2001, p 67.

[3]- منير ممدوح محمد الجنبهي، أمن المعلومات الالكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2005، ص13.

[4]- محمد عبيد الكعبي، الحماية الجنائية للتجارة الإلكترونية، رسالة دكتورة في الحقوق ، جامعة عين شمس، القاهرة، مصر، 2007، ص 105.

الفرع الأول: تعريف التشفير

إن مفهوم التشفير والترميز ليس بمستحدث في استخدام التشفير في الكتابة موجود منذ زمن وكان يستخدم غالبا في الأغراض العسكرية والاستخباراتية، أما في مجال الانترنت فقد استخدم التشفير لخدمة أغراض الشخصية للأفراد، وتستخدم في المراسلات العادية لتحديد هوية مرسلها وتستخدم في المصادقة على مضمونها والتأكيد على سلامتها، وعدم المساس بها، ونظرا لأهميته فقد حظى باهتمام العديد من التشريعات الغربية أو العربية ومن بين التشريعات التي اهتمت بتنظيم وتحديد أسلوب التشفير منها على سبيل المثال.

أولا: التعريف القانوني للتشفيرفي البلدان الغربية

يعتبر نظام التشفير أكثر تقدما في الدول الغربية، حيث أصبحت جلّ المعاملات اليومية في هذه الدول تتم عبر الوسائل الالكترونية، وبالتالي اعتماد نظام التشغيل لاستفاء السرية عليها، نتناول تعريفه في تشريعات مختلف الدول الغربية كما يلي:

1-القانون الفرنسي:

صدر أول مرسوم فرنسي بشأن التعامل بوسيلة التشفير بتاريخ 18 أفريل 1939 ثم صدر تعديل له بالمرسوم الصادر في 18 أبريل 1982، ثم صدر القانون الفرنسي رقم 9/1170 بتاريخ 29 ديسمبر 1990 حيث تضمنت المادة 27 منه على تعريف التشفير بأنه "كل الأعمال التي تهدف إلى تحويل معلومات أو إشارات واضحة باستخدام وسائل مادية أو معالجة آلية إلى معلومات أو إشارات غامضة للغير، أو إلى إجراء العملية العسكرية عبر وسائل مادية أو معلوماتية مخصصة لهذا الغرض[1].

سمح هذا القانون للمشروعات الصغيرة والأفراد باستخدام التشفير بعد أن كان مقصورا على المجالات العسكرية والحكومية فقط، وبتاريخ 24 فبراير 1998 صدر المرسوم رقم 98/101 الذي وضع الضوابط المتعلقة باستخدام التشفير

كما أنه وبموجب القانون رقم 616 بتاريخ 2001/07/11 أدخلت تعديلات على المادة 28 من قانون تنظيم الاتصالات الفرنسي لسنة 1990 تجيز تصدير وسائل التشفير التي تؤمن وظيفة السرية لرسالة المعلوماتية، وهذا التعديل التشريعي كان بناءا على توصيات البرلمان الأوربي بتاريخ 2000/06/22 التي ترمي إلى إلغاء القيود القائمة على تبادل تقنيات ومنتجات التشفير فيما بين الدول أوروبية الإعفاء.

[1]-سمير حامد عبد العزيز جمال، التعاقد عبر تقنيات الاتصال الحديثة، دار النهضة العربية ،القاهرة ،مصر ،2006 ، ص19.

أما الفترة الأولى من المادة 28 فقد عرفت أدوات التشفير ووسائله في مجال المعلوماتية بأنها "أعمال ترمي عبر اتفاقية سرية إلى تحويل معلومات أو إشارات غامضة، أو القيام بالعملية المعاكسة وذلك باستخدام وسائل أو برامج مخصصة لهذه الغاية[1].

2-في المملكة المتحدة:

صدر عام 2002 قانون جديد للتحكم في الصادرات لكي يحل محل قانون الاستيراد والتصدير وسلطات الجمارك لعام 1939، وهذا القانون الجديد ينظم إجراءات الحصول على رخص لتصدير المنتجات المشفرة والبرمجيات من المملكة المتحدة.

ويحتوي الملحق 01 من القانون البريطاني لعام 2002 على استثناء عام فيما يتعلق بإتاحة البرمجيات بصفة عامة دون قصد.

كما أن هناك تكنولوجيات محددة أخرى استثناها الملحق رقم "1" وهي البطاقات الشخصية الذكية ومعدات البث الإذاعي أو التلفزيوني المدفوع والذي يضمن تكنولوجيا فك الشفرة للصوتيات والمرئيات[2].

ثانيا: التعريف القانوني للتشفير في البلدان العربية

اقتداء منها بالدول الغربية قامت بتنظيم التشفير، وسنتناول تعريف التشفير في مختلف تشريعات الدول العربية فيما يلي:

1-القانون التونسي:

انفرد المشرع التونسي في نصوصه عن باقي التشريعات العربية الخاصة بالتجارة الالكترونية بتعريف التشفير في الفصل الثاني من الباب الأول من القانون رقم 83 سنة 2000 في شأن المبادلات والتجارة الالكترونية حيث نص على أن التشفير هو: استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومات بدونها[3].

كما نص أيضا على بعض الشروط التي يجب مراعاتها عند استعمال التشفير، حيث جاء الفصل الثالث من نفس القانون على أنه:" يخضع استعمال التشفير في المبادلات والتجارة الالكترونية عبر

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص164.

[2]- سمير حامد عبد العزيز جمال، المرجع السابق، ص 56.

[3]-محمد أمين الرومي المحامي، النظام القانوني للتوقيع الالكتروني، دار الكتب القانونية، مصر، سنة 2008، ص31.

الشبكات العمومية للاتصالات إلى التراتيب الجاري بها العمل في ميدان الخدمات ذات القيمة المضافة للاتصالات.

هذا وقد نص الفصل 48 من القانون رقم 2000/83 في حالة الاعتداء على البيانات المشفرة على أنه:"يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية المتعلقة بإمضاء غيره بالسجن لمدة تتراوح بين ستة أشهر وعامين وبخطية تتراوح بين 1000 و10000 دينارا أو بإحدى العقوبتين[1].

2-القانون المصري:

اصدر المشرع أيضا التشفير البيانات والمعلومات التي يتم تدوينها أو التعامل عليها من خلال الوسائط الإلكترونية، وذلك كأسلوب يحقق تأمين المعاملات التجارية وبالتالي ازدهارها رغم أن قانون التوقيع الإلكتروني المصري رقم 2004/15 جاء خاليا من تعريف التشفير، إلا أنه ترك هذه المسؤولية المسألة ليتم تنظيمها بأحكام اللائحة التنفيذية للقانون بتنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعية تكنولوجيا المعلومات، وذلك بوضع القواعد والضوابط الخاصة بتشفير المحررات والبيانات الالكترونية وكذلك وضع القواعد الخاصة بتشفير التوقيع الالكتروني وبيانات الائتمان وغيرها من البيانات التي يتم تحريرها أو نقلها أو تخزينها على وسائط الكترونية، وفقا للمعايير الفنية والتقنية المنصوص عليها في اللائحة التنفيذية للقانون والمشار إليها في الملحق الفني والتقني لهذه اللائحة[2].

عرفت المادة 9/1 من اللائحة التنفيذية لقانون التوقيع الالكتروني التشفير بأنه:" منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيا بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة"

كما عرفت المادة 10/1 من اللائحة نفسها شفرة المفتاحين العام والخاص بأنه:" تقنية شفرة المفتاحين العام والخاص هي منظومة تسنح لكل شخص طبيعي أو معنوي بان يكون لديه مفتاحين منفردين أحدهما عام ومفتاح إلكترونيا والثاني خاص يحتفظ به الشخص ويحفظه في درجة عالية من السرية"

[1]-وائل أنور بندق، موسوعة القانون الإلكتروني وتكنولوجيا الاتصال، دار المطبوعات الجامعية، الإسكندرية، 2007، ص51.

[2]-أنظر الفقرة (أ) و(ب) من الملحق الفني والتقني للائحة التنفيذية لقانون التوقيع الالكتروني المصري رقم 15 سنة 2004.

عرفت نفس اللائحة كل من المفتاحين العام والخاص وكذلك المفتاح الشفري الجذري التي تستخدمه جهات التصديق الالكتروني لإنشاء شهادات التصديق وبيانات إنشاء التوقيع الالكتروني، حيث نصت الفقرات 13/12/11 من المادة الأولى من اللائحة التنفيذية على ما يلي:

المفتاح الشفري العام: أداة إلكترونية متاحة للكافة، تنشأ بواسطة عملية حساسة خاصة وتستخدم في التحقق من شخصية الموقع على المحرر الالكتروني والتأكد من وجه وسلامة محتوى المحرر الالكتروني الأصلي[1]

المفتاح الشفري الخاص: أداة الكترونية خاصة بصاحبها، تنشأ بواسطة عملية خاصة وتستخدم في وضع التوقيع الالكتروني على المحررات الالكترونية ويتم الاحتفاظ بها على بطاقة ذكية ومؤمنة.

المفتاح الشفري الجذري: أداة إلكترونية تنشأ بواسطة عملية حسابية وتستخدمها جهات التصديق الالكتروني لإنشاءاتها ذات التصديق الالكتروني وبيانات إنشاء التوقيع الالكتروني"

يرى جانب من الفقه في هذا الخصوص أن التوقيعات الرقمية يستعان بها على نطاق واسع، وذلك أنها أكبر وسيلة لتحقيق مستوى الثقة المطلوبة بين الأطراف في المعاملات التجارية من حيث الفعالية وإمكانية التطبيق، حيث تنشأ التوقيعات الرقمية باستخدام علم التشفير، أما استخدام الشفرة غير المتماثلة أو المفتاح العام[2]. حيث نصت المادة الثالثة من اللائحة التنفيذية لقانون التوقيع الالكترونية رقم 15 لسنة 2004 على أنه:

"تجب أن تتضمن منظومة تكوين بيانات إنشاء التوقيع الإلكتروني المؤمنة الضوابط الفنية والتقنية اللازمة وعلى الأخص ما يلي:

1/أن تكون المنظومة مستندة إلى تقنية شفرة المفتاحين العام والخاص وإلى المفتاح الشفري الجذري الخاص بالجهة المرخص لها والذي تصدره لها الهيئة وذلك كله وفقا للمعايير الفنية والتقنية المشار إليها في الفقرة أ من الملحق الفني والتقني لهذه اللائحة.

2/أن تكون التقنية المستحدثة في إنشاء مفاتيح الشفرة الجذرية لجهات التصديق الالكتروني من التي تستعمل مفاتيح تشفير بأطوال لا تقل عن 2048 حرف الكترونيbit "

[1] - Williams David and john Benamati,Technology foundations & e-business applications, university new yourk, 2003, p 285.

[2]-Lorna brazel,Electronic Signatures and Identities Law and Regulation, 2008,p50.

3-القانون الجزائري:

لم يرد تعريف التشفير بصلب القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين كما وقع ذلك في أغلب التشريعات الأوربية أو العربية من أن تنظيمه يعد من المسائل الضرورية في ميدان المعاملات الإلكترونية، وإنما نص فقط على أنظمة التشفير في المادة 2 بند 8-9 من القانون 15-04 والتي تتمثل في:

1-مفتاح التشفير الخاص: هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي.

مفتاح التشفير العمومي: هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الالكتروني وتدرج في شهادة التصديق الإلكتروني[1].

نلاحظ مما سبق تفاوت التشريعات المنظمة للتجارة الإلكترونية في مواقفها من تنظيم أحكام التشفير بين من نظمها جزئيا وبين من انتشار إليها بصورة عرضية وبين من أغفلها تماما.

ثالثا: التعريف الفقهي للتشفير

تناول الفقه تعريفا للتشفير، حيث عرفه إبراهيم الدوسقي أبو الليل فيقول "بأنه تغيير في البيانات عن طريق تحويلها إلى رموز أو إشارات لمنع الغير من معرفتها أو تعديلها"[2].

كما عرفه ماجد راغب الحلو:"بأنه عبارة عن أرقام مطبوعة لمحتوى المعاملة التي يتم توقيع عليها بالطريقة نفسها باستعمال مفاتيح سرية"[3].

"يرى ليونالبوشرباغ "LIONEL BOUCHURBERG" بأنه مجموعة من التقنيات التي تهدف إلى حماية المعلومات بأفضل استعمال بروتوكولات سرية، تجعل البيانات مشفرة غير مفهومة لدى الغير بواسطة البرامج المخصصة لذلك[4].

يتضح لنا من التعاريف الواردة سواء التشريع أو الفقه تتفق على اعتبار التشفير بأنه عملية تحويل المعلومات إلى رموز غير مفهومة لمنع الغير من الاطلاع عليها أو فهمها، لهذا تنطوي عملية التشفير أساسا على تحويل النصوص العادية إلى نصوص مشفرة ومن المعلوم أن الانترنت تشكل في هذه الأيام الوسط

[1]-مادة 2 بند 8-9 من القانون رقم 15-04 المتعلق بالتوقيع الإلكتروني والتصديق الإلكتروني المصري السالف الذكر.

[2]-إبراهيم الدوسقي أبو الليل، مرجع سابق، ص180.

[3]-ماجد راغب الحلو، العقد الإداري الإلكتروني، تأليف: رحيمة الصغير ساعد نمديلي، دار الجامعة الجديدة، 2007، ص37.

[4]-Edward h.j. d, digital signature and electronic contacts, 2004,p 156.

الأضخم لنقل المعلومات ولا بد من نقل المعلومات الحساسة مثل الحركات المالية بصيغة شفرة للمحافظة على سلامتها وتأمينها وتستخدم في ذلك المفاتيح في التشفير الرسائل الإلكترونية وفك تشفيرها، وتستند هذه المفاتيح إلى صيغ رياضية معقدة المسماة بالخوارزميات وتعتمد قوة وفعالية التشفير على عاملين أساسيين هما: الخوارزمية وطول المفتاح مقدار البث bit[1].

الفرع الثاني: أنظمة تشفير التوقيع الالكتروني

مع انتشار القرصنة وسرقة المعلومات الشخصية في كل أنحاء العالم من خلال شبكة الانترنت، لا ينكر أحد مدى أهمية التشفير في حماية البيانات المرسلة والتي يتم إخضاعهاإلى أحد النظامين، النظام الأول النظام المتماثل والثاني هو النظام اللامتماثل أو النظام المزدوجوهذا ما سنتناوله في هذا الفرع كالتالي:

أولا: التشفير بالمفتاح المتماثل:

ويقصد به المفتاح الخاص clé privée والمسمى بنظام تقنية التشفير المتماثل حيث يعتمد هذا النوع من التشفير على معيار تشفير البيانات وفيه يستخدم كل من المرسل والمستقبل ذات المفتاح السري في تشفير رسالة البيانات وفك تشفيرها[2].

وفي حال إنشاء المفتاح يتم الاتفاق بين الطرفين في البداية على كلمة المرور حيث يتم إعداد كلمات مرور طويلة فالمفتاح الذي يتم إنشاؤه للمرور يمكن أن يتضمن حروفا كبيرة وصغيرة ورموزا أخرى بحسب ما ينتج عن الخوارزمية التي يتم إنشاؤها بين طرفي التشفير، وفي حال إدخال كلمة المرور يتم تحويل عبارة المرور إلى عدد ثنائي يتم فهمه من قبل أجهزة الحاسب وفي حال إرسال الرسالة إلى الطرف الآخر، فإنه من الضروري أن تتم قراءة الرسالة التي وصلت إلا أن قراءة الرسالة بالوضع الذي تم استلامها به يكون صعبا وغير ممكن، لان الرسالة المشفرة لا يمكن فهم ما تحتويه من رموز وإشارات ولإزالة الغموض وبيان الرسالة على شكلها الأصلي يتم استخدام كلمة المرور المستخدمة في التشفير والتي تشكل المفتاح الثنائي الذي يتولى عملية التشفير وتحويل النص المشفر إلى شكله الأصلي المفهوم[3].

---

[1]- يمينة حوحو، مرجع سابق، ص187.

[2]-حسام محمد نبيل الشنراقي، مرجع سابق، ص639.

[3]-محمد فواز محمد المطالقة، عقود التجارة الإلكترونية، أركانه، إثباته، حماية تشفير التوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، طبعة أولى، 2006، ص64.

وما يعاب على هذه الطريقة إمكانية تسرب المفتاح السري الوارد أثناء التبادل بين الطرفين ويمكن اقتحامه واستعماله من قبل لصوص أو قراصنة أو أي شخص آخر غير مرخص باستعماله[1].

وفيما يلي الشكل رقم 02 الذي يبين لنا آلية التشفير التماثلي.

ثانيا: التشفير اللامتماثل:

من استخدام النوع السابق للتشفير وعدم نجاحه تم البحث عن بديل يحل محله ويؤدي الغاية المرجوة منه على أفضل وجه، وتم التوصل إلى نوع جديد ألا وهو التشفير اللامتماثل، حيث اكتشفت هذه الطريقة في الولايات المتحدة الأمريكية عام 1978 ثلاثة علماء في الرياضيات[2] وهم rivest، Shamir and edeman على عكس التشفير المتماثل الذي يستخدم مفتاح واحد فإن هذا النوع من التشفير يستخدم مفتاحين اثنين تربط بينهما علاقة رياضية متينة، ويدعى هذان المفتاحان بالمفتاح العام public key والمفتاح الخاص peivatkey[3] ويكون المفتاح الخاص معروفا لدى جهة واحدة فقط أو شخص واحد فقط وهو المرسل ويستخدم لتشفير الرسالة وفك شفرتها، أما المفتاح العام فيكون معروفا لدى أكثر من شخص أو جهة ويستطيع المفتاح العام فك شيفرة الرسالة التي تتم تشفيرها بالمفتاح الخاص بذلك، ويتم تأمين هذا النظام عن طريق بروتوكول الطبقات الأمنية secure socket layers SSL.

حيث يساعد هذا البروتوكول على التحقق من المفتاح العام والتأكد من سلامة رسالة البيانات وعدم تحريفها أثناء نقلها عبر شبكة انترنت.

ثالثا: نظام المفتاح العام المزدوج

يتم تشفير التوقيع الإلكتروني بالمفتاح الخاص للمرسل وبعد ذلك تشفير الرسالة كاملة بواسطة المفتاح العام للمرسل إليه، وبعد ذلك يستخدم المستقبل مفتاحه الخاص ويسترجع به الرسالة الأصلية.

وهناك حاجزان من التشفير لحل شفرة التوقيع الالكتروني.

الأول: يستخدم المفتاح العام للمرسل لحل شفرة التوقيع الخاص بالمرسل والتي يتم تشفيرها بالمفتاح الخاص.

[1]-ازاد دزه يي، مرجع سابق، ص92.

[2]-محمد فواز المطالقة، المرجع السابق، ص124.

[3]-خالد ممدوح إبراهيم، المرجع السابق، ص158.

الثاني: وهو محتوى الرسالة، يستخدم المستقبل مفتاحه الخاص لفك شفرة الرسالة التي تم تشفيرها بمفتاح المستقبل العام.

ويضمن بذلك سلامة الرسالة من أي عبث أو لعب أو تعديل من قبل الغير، بهذه الطريقة تكون شخصية الموقع ومتن الرسالة موضع الثقة الكاملة[1].

رابعا: أقسام التشفير

ينقسم علم التشفير إلى ثلاثة أقسام هي:

1-الكتابة المشفرة الطبيعية:

تتضمن الكتابة المشفرة الطبيعية أنواع مختلفة من الطرق، والطرق الأكثر شيوعا هي حالة تستخدم الإحلال أو تبديل الحروف أو الكلمات، ومن الطرق الطبيعية أيضا طريقة التشفير المسماة بفن الاختزال وهي اختفاء المعلومات ضمن معلومات أخرى كصورة مثلا وبصفة عامة تشير الكتابة المشفرة الطبيعية إلى أي طريقة لا تعدّل القيمة باستعمال عملية رياضية

2-الكتابة المشفرة الرياضية:

تتعامل الكتابة المشفرة الرياضية مع القضايا المتعلقة باستعمال العمليات الرياضية على الحروف أو الرسالة، الأكثر شيوعا هي حالة تسمى الهامش وهي عبارة عن عملية حسابية تتم على الرسالة وتحولها إلى قيمة عددية.

ولا يمكن أن تستعمل لاشتقاق معنى الرسالة، وهذا العدد يمكن أن يرسل بالرسالة إلى المستلم، الطرف الآخر يمكن أن يستعمل دالة الهامش نفسها لتقرير أن الرسالة موثوق بها، إذا قيمة الهامش مختلفة، فهذا يدل على أن الرسالة عدّلت بطريقة ما، هذه العملية معروفة كذلك بحساب المجموع.

3-الكتابة المشفرة الكمية:

الكتابة المشفرة الكمية هي طريقة جديدة نسبيا من التشفير، قبل 2002 تطبيقها كان محدودا على عمل المختبر وربما بعض التطبيقات الحكومية السرية، هذه الطريقة تعتمد على خصائص أصغر جزئيات عرفت ومن الممكن الآن صنع شفرات مستحيلة الكسر باستخدام الطرق الكمية[2].

[1]-ازاد دزه يي، مرجع سابق، ص152.

[2]-خالد ممدوح إبراهيم، مرجع سابق، ص154، 155.

الفرع الثالث: الكيفية التقنية لتشفير التوقيع الإلكتروني

تقسم البيانات المراد تشفيرها إلى حروف نبضات ويتم تشفير كل حرف على حدة باستخدام مفتاح شفرى واحد، أو تقسم البيانات المراد تشفيرها إلى حروف ويتم تشفير كل حرف على حدة باستخدام مفتاح شفري مختلف وهذا الأسلوب له عدة تقنيات وهي:

أولا: الأساليب التقنية للتشفير

***شفرة الإحلال:** وفيها يتم تحويل حروف البيانات المراد تشفيرها إلىحروف أخرى وذلك باستخدام مفتاح معين متفق عليه.

***شفرة الاستبدال**: وفيها يتم التبديل في الحروف المراد تشفيرها، أي في البيانات التي تحتفظ بنفس حروفها ولكنها تكون غير مرئية ويتم ذلك باستخدام مفتاح معين متفق عليه[1].

***شفرة الإنتاج**: وهي عبارة عن مزيج من شفرة الإحلال وشفرة التعديل أي أن البيانات تمر بعدة مراحل من التشفير للحصول على الصورة المشفرة في النهاية[2].

شفرة الأسية: حيث يتم التشفير باستخدام معادلو رياضية أُسية بعد تحويل الحروف إلى أرقام باستخدام جداول ثم يتم إعادتهاإلى صورة حروف بعد التعويض في هذه المعادلة.

***شفرة حقيبة الظهر:**

تتم عملية التشفير باستخدام معادلة رياضية معقدة لحصول على أعلى درجات السرية والصعوبة في حال هذه الشفرة بواسطة أي شخص دخيل على النظام وغير مصرح له بتداول البيانات التي تم تشفيرها[3].

[1]-أيمن عبد الحفيظ، حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة، العدد 20 يناير 2004، ص332.

[2]- إبراهيم الدوسقي أبو الليل، مرجع سابق، ص125.

[3]-حسام محمد نبيل الشراقي، مرجع سابق، ص642.

ثانيا: مستويات التشفير

توجد عدة مستويات للتشفير، فقد يكون على مستوى الإرسال أو على مستوى التنقل أو التصفح، كما قد يكون على مستوى التطبيق أو التنفيذ، وأخيرا التشفير على مستوى الملفات، وسنتطرق لدراسة كل هذه المستويات على النحو التالي:

أولا: التشفير على مستوى الإرسال:

يتم في هذا المستوى تشفير جميع المعلومات والبيانات بين نقطة الإرسال ونقطة الاستقبال ويتم عن طريق الشبكات الافتراضية الخاصة[1] وهي شبكات جزئية من شبكة الانترنت، تقوم فيه إحدى المنشآت أو المشروعات بتخصيصه لخدمتها عن طريق إحاطته باحتياطات التأمينية المطلوبة لإرسال واستقبال المعلومات من خلاله بشكل آمن، أي تبادل المعلومات والبيانات بشكل آمن على شبكة الانترنت، ويتم عن طريق تشفير جميع البيانات والمعلومات من نقطة الإرسال إلى نقطة الاستقبال[2].

ثانيا: التشفير على مستوى التصفح أو التنقل

وفقا لهذا المستوى يتم تشفير جميع الاتصالات بين نوافذ الشبكة وأحد برامج التصفح أو أحد مقار المعلومات أو المواقع الموجودة عليها، مما يؤدي إلى حماية البيانات أثناء انتقالها، وقد أعلنت شركة نت سكيب "Net scape" أحد البروتوكولات التأمينية عام 1995 وهو بروتوكول المعروف باختصار SSL وتنصرف مهمة هذا البروتوكول نحو تشفير جميع الاتصالات على النحو المذكور سابقا، الأمر الذي يقلل من فرصة نسخ أو وصول البيانات إلى أيدي أي شخص غير مرغوب فيه وقصر وصولها للمستقبل النهائي، مما قد يعطي هذا الأمر شكلا من أشكال الثقة والائتمان للعملاء، لان المعلومات والبيانات الخاصة بهم بما فيها أرقام بطاقة الائتمان، لن تكون متاحة سوى للتاجر، أو المنشأة أو المؤسسة المراد التعامل معها عن طريق هذه الشبكة دون غيرها.

عندما يرغب أحد المستهلكين في شراء سلعة عن طريق الانترنت، فيقوم بالدخول على الموقع أو الصفحة الخاصة بالمؤسسة المراد التعامل معها CWEBSITE وبعد اختيار الشيء المراد شراءه، يدخل إلى القناة أو الطريق الآمن لإتمام عملية الشراء، مما يؤدي إلى انتقال قنوات الاتصال والإرسال بين نافذة

[1]-أحمد محمد الهواري، عقود التجارة الالكترونية، مركز البحوث والدراسات أكاديمية شرطة دبي، الإمارات العربية المتحدة، فقرة 26-28 أفريل 2003، ص 25-30.

[2]- قدري عبد الفتاح الشهاوي، أدلة مسرح الجريمة، الأساليب التقنية المتقدمة، علما وقانونا وتحليلا وفنا وعملا وتطبيقا، منشأة المعارف، الإسكندرية، 2002ص 417- 419.

شبكة المعلومات ومقر المعلومات أو يتغير بداية اسم مقر المعلومات HTTPإلى[1] HTTP بروتوكول SSL قد بدأ عمله أثناء إتمام الصفقة التجارية وبمجرد وصول تلك البيانات إلى مقر المعلومات يتم حل الشفرة بواسطة برنامج خاص لاستدراج أمر الشراء، ويعتبر هذا البروتوكول الأكثر انتشارا واستخداما[2].

يوجد بروتوكول آخر لتأمين البيانات أثناء انتقالها بين أحد نوافذ شبكة الانترنت واحد مقر المعلومات أو يسمى هذا النظام ببروتوكول الاتصال الآمن s-http[3] ويختلف هذا النظام عن نظام نت سكيب للتأمين، في أن النظام الأول، نظام بروتكول الاتصال الآمن s-http يقوم بحماية البيانات المنقولة ذاتها بينما النظام الثاني – بروتوكول SSL مهمته حماية قناة الاتصال أثناء انتقال البيانات من المرسل إلى المستقبل.

ثالثا: التشفير على مستوى التطبيق أو التنفيذ

يتم فيه تشفير طلب الشراء وعملية الدفع عبر شبكة online وهو نظام تأمين المعاملات الالكترونية set[4] ويعتبر هذا النظام من أهم البروتوكولات المتعلقة بالنواحي التي ظهرت في مجال منظومة التجارة الالكترونية.

ويتطلب العمل بنظام set فتح حساب بنكي لكل من البائع والمشتري بأحد البنوك المستخدمة له، واستخدام المشتري لأحد برامج التصفح نوافذ شبكة المعلومات المدعم لنظام set واستخدام البائع لمقر المعلومات server يدعم هو الآخر ذلك النظام.

ثانيا: الطرق التقنية لكسر التشفير

هناك طرق كثيرة لكسر الشفرات أو الرموز وهي:

أ-تحليل التكرار:

[1]- بعد ظهور نظام الويب العالمي (WWW) وكانت الحادية إلى لغة تسمح بربط مواقع الويب الموصولة بشبكة فيما بينها بالتجول داخلها، وهنا ظهر بروتوكول HTTP تعمل على حمل ونقل المعلومات والبيانات مباشرة بين الأطراف.

[2]- قدري عبد الفتاح الشهاوي، المرجع السابق، ص419- 420.

[3]- اختصارات Securehypertexte transport Protocol البروتوكول الآمن والعالمي المدى في نقل البيانات، أنظر: عمر خالد الزرقيات، عقود تجارة الالكترونية، عقد البيع عبر الانترنت، ط1، دار الجامعة للنشر والتوزيع، الأردن، 2007.

[4]-اختصار Secureélectronique transaction بروتوكول الإخفاء المزدوج والدفين الآمن، أنظر: قدري عبد الفتاح الشهاوي، مرجع سابق، ص412.

يتضمن النظر إلى الرسالة المشفرة لتحديد وجود أي نمط متكرر، فعلى سبيل المثال في اللغة الانجليزية يتكرر الحرفين TLE فمثلا الكلمات That،the ، and،i هي كلمات شائعة جدا ومحل التشفير يبحث عن هذه الأنواع من الأنماط ومع مرور الوقت، قد يكون قادرا على استنساخ الدالة التي استعملت لتشفير البيانات، هذه العملية يمكن أن تكون بسيطة جدا أحيانا أو رما قد تأخذ كثيرا من الجهد.

ب-**أخطاء خوارزمية:** الخوارزمية هي عملية أو مجموعة من الأوامر لأداء مهمة أوامر في عالم الحاسبات استخدم للقيام بعمليات تكرارية والتي تعطي أحيانا نتائج غير متوقعة الأمر الذي يؤدي إلى الكشف عن خوارزمية التشفير.

ب-**الخطأ البشري:** أحد الأسباب الرئيسية لنقاط ضعف التشفير، إذا أرسل بريد الكتروني باستعمال التشفير وشخص آخر أرسله بدون تشفير الرسائل المستقبلية.

ج-**الهندسة الاجتماعية:** هذه الحالة يمكن أن تكون نتيجة خطأ أو يمكن أن يكون سببها الحوافز الشخصية مثل الطمع المال والمعتقدات السياسية دافعا قويان، الناس يمكن أن يرتشو لإعطاء معلومات[1].

نلاحظ أن نجاح التشفير يقتصر على كون كل المعلومات والمفتاح الذين يراد تشفيرهما محميين من المخاطر الأخرى، فمثلا وجود الفيروسات أو البرامج التجسس على جهازك سيؤدي إلى كشف كلمة المرور، أو يؤدي إلى تخريبها لذا التشفير عملية تجري موازنة لها عملية أخرى وهي إمكانية الخرق والكشف عن المفاتيح، وهذا الصراع بدأ بين الطرفين منذ ظهورهما ويستمر هذا النهج، على الرغم من وجود طرائق تشفير متينة وقوية لا يسهل اختراقها، ومع ذلك تبقى عملية التشفير الطريق الأمن لإجراء العمليات بين الأطراف، وهو طريق متمتع بالصفة القانونية في بيئة الكترونية وبواسطة تقنيات ووسائل اتصال حديثة وتكنولوجية.

المطلب الثاني: حماية التوقيع الالكتروني بواسطة أدوات القياس الحيوي

يعتبر التشفير من أهم السبل الوقائية لإسباغ الحماية على التوقيع الالكتروني وإزاء ذلك بات ملحا أن تتوافر آلية يكون من شأنها تحقق ضرفي التعاقد من أن التوقيع المنسوب للطرف الآخر قد صدر عن إرادة صحيحة منه ودون أن يداخلها شهة تنال من حجيته، ومن صور الحماية الفنية للتوقيع الالكتروني استخدام أدوات القياس الحيوي والتي تتم من خلال استخدام أساليب علمية متطورة تدخل ضمن

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص156-157.

تكنولوجيا البصمات والخواص الحيوية والطبيعية وهي تعتمد على الخصائص الفيزيائية والطبيعية والسلوكية للأفراد والتي تعتمد على بصمة الإبهام أو حدقة العين أو بصمة الصوت أو أنماط الأوعية الدموية[1] وهذا ما سنتناوله على النحو التالي:

الفرع الأول: المسح الضوئي للشبكة والقزحية[2].

توفر التقنيات المتطورة اليوم استخدام أنماط من قزحية العين والحدقة ولون العينين والشبكية التي تميز بصفات متنوعة فريدة لدى كل شخص، لتحقق من هوية ذلك الشخص.

ونظام تمييز قزحية العين يتم باستخدام آلة تصوير فديو مرئية لجذب انتباه حدقة العين، وبطريقة أخذ بصمات الأصبع نفسها ومن خلالها تقوم البرامج المتخصصة بإجراء المقارنة بين البيانات الناتجة وتلك البيانات المخزنة والمحفوظة لديها لتحديد الهوية[3].

وتنشأ المشاكل في تلك التقنيات المتطورة التي يمكنها أن تقوم بتضييع عدسات لاحقة مشابهة لقريحة عين شخص معين وبالتالي يمكن إنتاج شكل مشابه ورخيص ويمكن أن يطبق ببساطة وطبقا لرؤية بعض المختصين في الأنظمة البيومترية التي تحدد شبكة العين وطبقة الأوعية الدموية التي تقع خلف العين.

وهذه الصورة يمكن أن تكون واضحة جدا ويصعب أن تجذب الانتباه وأثناء تسجيل المستعمل يجب أن يركز على هذه النقطة، بينما تؤخذ تلك الصورة بشكل دقيق جدا وتخزن في آلة التصوير لأداء عملها بشكل صحيح أو أن أفضل أمن عام يمكن أن يستنتج باستعمال هذه الأنظمة البيومترية التي تعتمد على العين أساسها قزحية وشبكة العين بشكل آلي.

لا يتخذ شخصان في نمط واحد للوعاء الدموي للشبكة[4] حتى فيما بين التوائم المتماثلة، ولهذا فإنها توفر وسيلة لتحديد هوية الشخص يمكن الوثوق بها ونمط الوعاء الدموي لشبكة يتغير تغيرا طفيفا مع الوقت.

---

[1] - Nehadalhussban, admissibility of electronic signature in and It's Legal Effect , A Comparative Study in the Jordanian Laws, university of Jordanian, December, 2005, p30.

[2] -محمد علي سويلم، الحماية الجنائية للمعاملات الالكترونية بين الجوانب الإجرائية والأحكام الموضوعية، دراسة مقارنة لقانون تنظيم التوقيع الالكتروني وتكنولوجيا المعلومات، دار المطبوعات الجامعية، الإسكندرية، طبعة أولى سنة 2018.

[3] - محمد سعيد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الالكترونية، رسالة دكتوراه حقوق، عين الشمس، القاهرة، 2005، ص195.

[4] - الشبكة: طبقة رقيقة تقع في الجزء الخلفي من العين، وهي التي تستشعر الضوء وتنقل إشارات من خلال العصب البصري إلى المخ، ومن المعروف أن كل إنسان ينفرد بشكل مختلف من الأوعية الدموية، وهو ما يسمى باسم....الوعاء الدموي للشبكة.

وأنظمة المسح الضوئي لشبكة تستخدم آلة تصوير لتفحص عين الإنسان وتمسح الشبكة ضوئيا، ونمطيا، يؤخذ مسح دائري للشبكية على 360 درجة باستخدام مصدر للضوء ذي كثافة منخفضة وقارئ بصري لتحقق من أنماط الأوعية الدموية بالشبكة، وتستغرق هذه العملية عشر ثوان، ثم تترجم هذه المعلومات إلى عدد من النقاط المرجعية عن طريق وسائل مثل الخوارزميات المحددة مسبقا قبل أن يتم تحويلها إلى قالب يعبر عنه رقميا ويمكن تخزينه بغية إجراء مقارنة مستقبلية[1].

وفي أجهزة المسح الضوئي الموجودة حاليا يطلب من الشخص أن يقرب عينه من جهاز المسح، وإن ينزع النظارة أو العدسات اللاصقة التي تبت أن الناس لا يستخدمونها كثيرا ونتيجة لذلك فإن أجهزة المسح الضوئي للشبكة يتم تطويرها الآن حتى تسمح لمسح الضوئي أن يعمل عن بعد وألا يتأثر بوضع الشخص لنظارة الطبية أو العدسات اللاصقة[2].

المسح الضوئي للقزحية هو من الطرق الرئيسية الأخرى للقياسات الحيوية والبيولوجيا الإحصائية التي تتعلق بالعين والقزحية هي عضو داخلي يقع خلف القرنية والرطوبة المائية للعين، ويمكن رؤيتها من الخارج على شكل الجزء الملون في العين الذي على طبقات عديدة ومشخصات مميزة.

ونسيج القزحية الذي يؤدي إلى الأنماط السابقة، عبارة عن تركيب ليفي معقد ويعرف باسم الشبكة الدمعية ويتكون خلال المراحل الأخيرة من الحمل.

وينتهي تطوره قبيل الولادة، ووظيفة هذا النسيج هي تصريف الرطوبة المائية من العين، ومن المفهوم أن نمط كحل قزحية فريد في قياسه حتى بين التوائم المتماثلة، والنماذج التي تمثلها القزحية لا تتغير مع العمر، ومن المعروف أن الشبكة الدمعية تفسد خلال الدقائق التي تعقب الوفاة.

ويتطلب نظام المسح الضوئي للقزحية، أن يجلس المستخدم في وضع يرى فيه بنفسه انعكاس عينية على الجهاز، ويمكن حينئذ أن تلتقط آلة التصوير التلفزيونية صورة لقزحيته والأجزاء التي لا تقدم بيانات ذات مغزى مثل العين والأهداب وما إلى ذلك، ويمكن حجبها حتى لا تتداخل مع تكويد بيانات القزحية، وبعد ذلك تطبق تقنيات معالجة الإشارة.

وتسمى باسم مرشحات Gabor على هذه الصورة لاستخراج البيانات القائمة على تموجات شبكة المجاري الدمعية، ويمكن للمستخدم أن يجري عليه المسح من مسابقة تصل إلى قدمين أو ربما يحتاج

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص81.

[2]- محمد أحمد نور حسيبة، مدى حجية التوقيع الالكتروني في عقود التجارة الالكترونية، رسالة دكتوراه حقوق، القاهرة، 2005، ص99.

إلىأن يقترب ليكون على مقربة محدودة، ويعتمد ذلك على نوعية الجهاز ويحتاج المستخدم أن ينظر في الجهاز لبرهة يسيرة[1].

ولكي تحل المشاكل المستقبلية لمنتحلي شخصية المستخدمين الذين يحاولون خداع أجهزة المسح الضوئي وذلك بحمل صورة ضوئية لقزحية الشخص المعنى، فإن بعض أجهزة المسح الضوئي تحتوي على مصدر للضوء وتقيس اتساع عين الإنسان وذلك لضمان أن ما يقوم الجهاز بمسحه ضوئيا هو العين الحقيقية لشخص.

وعموما فإن أجهزة استخدام حدقة العين تعين الخواص البيولوجية لعين المتمثلة في الشرايين والعلامات الموجودة في الشبكة ثم تحيل على ذاكرة الحاسب الذي يتصل بجهاز مزود بشرائح الكترونية صغيرة الحجم، والذي يقوم بدوره بتحديد هوية الأشخاص عند التعامل من خلال التقاط صورة للعين ومضاهاتها بما هو مخزن في الذاكرة وبالتالي سمح لصاحب البصمة بالدخول على البرنامج وتلك الطريقة تعرف ايريكس كود[2].

الفرع الثاني: تمييز الصوت voice

تختلف خصائص الأشخاص في الذبذبات الصوتية من حيث درجتها ونوعها فالقياسات الحيوية للصوت تستفيد من الصفات المميزة لصوت الشخص وبعض هذه المميزات يحددها السلوك والبعض الآخر تحددها الوظائف وتحلل أجهزة القياسات الحيوية ديناميكيات الموجات مثل طول القناة الصوتية وشكل تجويف الفم والأنف بإضافة إلى النبرات ونطق الحروف ويمكن بعد ذلك أن ترقم هذه الموجات بغية إنشاء التوقيع الالكتروني"[3].

وأجهزة التقاط القياسات الحيوية للصوت سهلة الاستخدام، ويشعر المرء بصفة عامة براحة أكثر عند التحدث في الميكروفون على أن ينظر إلى شعاع من الضوء عند أخذ المسح الضوئي لشبكية ولمنع استخدام تسجيل الصوت لخداع الجهاز، فإن معظم الأجهزة تتطلب الترددات العالية والمنخفضة للعيون للمناظرة بينهما والتي يصعب على عديد من وسائل التسجيل أن تقلدها جيدا.

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص82.

[2]- عبد الفتاح بيومي حجازي، مرجع سابق، ص133.

[3]- خالد ممدوح إبراهيم، مرجع سابق، ص83.

ويلاحظ أنه مهما تبلغ مهارة التقليد الصوتي فلا يمكن تقليد أصوات أشخاص معينين وفي المقابل، فقد يعاني الشخص من مشاكل فيزيولوجية مثل الإصابة "بالبرد أو التهاب الحنجرة" الذي قد ينتج عنه إنتاج بيانات القياس الحيوي للصوت المختلف عن التوقيع الطبيعي لشخص نفسه، وأيضا فإن الشخص يتغير بمرور الزمن وهو ما قد يحد من الاستفادة من هذه التقنية بغية إنشاء توقيع الكتروني[1].

فقد تم اكتشاف حالات احتيال باستخدام البصمة الشخصية المقلدة وعدم استطاعة بعض أجهزة التحقق البصرية المصنوعة من رقائق السيليكون من كشفها أو تمييزها، كما أن التكلفة المرتفقة نسبيا التي يتطلبها وضع نظام آمن في شبكة المعلومات باستخدام وسائل بيومترية حددت من انتشاره إلى درجة كبيرة وجعلته قاصرا على بعض الاستخدامات المحدودة[2].

الفرع الثالث: بصمات الأصابع والشكل الهندسي لليد

تتكون بصمات الأصابع من تنوعات وتجاويف احتكاكية، وهي تميز أصابع الشخص بخطوط متشابكة وهذا النمط عبارة عن حلقات وتقوسات مع سمات صغيرة من التنبؤات والتجاويف وحتى الأمن من أكثر منتجات القياسات الحيوية الحالية نجاحا عظيما من حيث المبيعات هي تلك التي تعتمد على بصمات الأصابع وتقدر منتجات تمييز بصمة الأصبع بأنها المسئولة عن أكثر من 70% من إجمالي المبيعات الخاصة بتقنيات البيولوجيا الحيوية[3].

أولا: بصمة الأصبع

تعتبر بصمات الأصبع الأداة المميزة لأي شخص، حيث أن الطبيعة الفريدة لبصمات أصابع الشخص تجعل التوقيع بواسطتها يبدو طبيعيا، وأن استخدمت لذلك عدة برامج وتقنيات الكترونية.

ومن جهة أخرى، فإن التطبيق العملي يتم بأخذ بصمات الأصابع عن طريق وضع الأصبع على ماسح ضوئي صغير الحجم يقرأها ويحولها بما تتضمنه من نتوءات وتجاويف وانحناءات إلى مجموعة بيانات، ويرسلها إلى الحاسب الالكتروني المتصل به حيث يتم تشفيرها باستخدام خوارزميات خاصة تسمى خوارزميات البصمة الالكترونية، وإن استخدام هذه الخوارزميات ينتج توقيعا الكترونيا فريدا بطريقة أسرع من القيام بعملية التشفير اللامتناظر، وفي المرحلة التالية فإن البيانات المخزنة لديه عن طريق

[1]-MARTIN H, La signature électronique : comment la technique répond elle aux exigences de la loi , gazette du palais, 2000, p 46

[2]-أيمن سعد سليم، مرجع سابق، ،ص22.

[3]- محمد أحمد نور حسيبة، مرجع سابق، ص105.

بصمات الأصابع وفي أغلب الأحيان قد يكون هناك معلومات إضافية يجب أن تكون متوفرة، مثل الاسم أو الرمز المستعمل وبالتالي فإن المرور يكون مسموحا به فقط إذا كان هناك تطابق.

وتعمل أنظمة القياسات الحيوية التي تستخدم بصمة الأصبع في تحديد الهوية عن طريق وضع الشخص أصبعه على ماسح ضوئي صغير، وهذا الماسح الضوئي يأخذ قراءة بصمة الأصبع بصورة ضوئية، أو باستخدام الموجات فوق الصوتية، أو أية وسيلة أخرى من وسائل قراءة الشكل الهندسي لبصمة الأصبع، ويتصل بالكمبيوتر الذي يأخذ المعلومات من الماسح الضوئي[1].

وأهم السمات الخاصة بالبصمة هي النقاط لتي تأتي فيها خطوط بصمة الأصبع المتعددة معا أو تغير اتجاهها، وتتحدد مع تصنيف الخطوط مثل التنبؤات والتجاويف والحلقات الدائرية وما إلى ذلك وتحول هذه السمات إلى شكل رقمي، وفي العادة لا تظهر صورة بصمة الأصبع إلا مجموعة من البيانات فقط، بينما قد يؤثر وضع اليد وحركتها خلال عملية المسح الضوئي على مخرجات البيانات.

وتحتوي الأجهزة الحديثة على مرشحات خوارزمية مدمجة تزيل هذه الآثار إلى حد بعيد وخالية من أي إصابة.

ثانيا: الشكل الهندسي لليد

أما فيما يتعلق بالشكل الهندسي لليد، فإن الهندسة ثلاثية الأبعاد ليد الشخص تقوم على حجمها، وشكلها، وطول الأصبع، وتفاصيل أخرى، وهي بذلك تقدم معلومات وافية ذات طابع فردي يمكن استخدامها كوسيلة من وسائل القياسات الحيوية لتحديد الهوية، ويمكن للمعلومات التي تجمع من تحليل شكل يد الشخص المعني أن تترجم رقيما وتستخدم كأساس لتوقيع الالكتروني.

وتعمل الأجهزة القياسية للقياسات الحيوية الخاصة بالشكل الهندسي لليد عن طريق وضع الشخص المعني يده على سطح عاكس، وعندئذ يتم التقاط صورة باستخدام مجس شحنات متصل بمجموعة من المرايا، وينتج عن ذلك معلومات ثلاثية الأبعاد تعتمد على الشكل الهندسي لليد، وهذه العلامات الاسترشادية لضمان أن كل شخص يضع يده في وضع ثابت يمكن استخدام هذه الطريقة بشكل مناسب حسب الرغبة لضمان أن الشخص حي.

ويؤخذ على هذه الطريقة، أن اليد البشرية وإن كانت متنوعة إلى حد بعيد إلا أنها ليست فريدة ولهذا فإنه عند استخدام أنظمة الشكل الهندسي لليد عندما يكون التحقق من الصحة مطلوبا، يثور الشك

[1]- خالد ممدوح إبراهيم، مرجع سابقن ص86.

حول ما إذا كانت البيانات الناتجة عن أجهزة الشكل الهندسي لليد مناسبة لاستخدام توقيع الكتروني، كما أن هذه الأجهزة ذات تكلفة مرتفعة بالمقارنة بأجهزة تمييز بصمة الأصبع وأجهزة المسح الضوئي للقزحية ويمكن أيضا أن تتأثر البيانات بإصابة اليد بالجرح، وتورمها، وعند التزيين بالحلي[1]

ثالثا: ديناميكيات التوقيع بخط اليد:

إن الأشكال المرئية للتوقيع بخط اليد هي –بلا جدال- الأكثر شيوعا في الاستخدام في تحديد الهوية وظلت كذلك لآلاف من السنين، واليوم نجد التوقيع على كل بطاقات الائتمان والبنوك المستخدمة، وهذه الطريقة الأساسية التي تنعقد بها العقود الشكلية المكتوبة وبالرغم من أن المزور يمكنه تقليد الشكل المرئي للتوقيع، إلا أن كل شخص له طريقة منفردة يوقع بها على الوثيقة.

والتحدي الذي يواجه أنظمة القياسات الحيوية هو أن تلتقط كلا من التوقيع المكتوب والطريقة المكتوب بها، وبهذا المعنى فإن التقاط التوقيع المكتوب باليد يختلف من محددات الهوية الأخرى التي تستخدم القياسات الحيوية في أنها ليست طريقة فسيولوجية في تحديد هوية الشخص، بل هي طريقة سلوكية.

وهذه الأجهزة تذهب إلى ما وراء الطريقة البسيطة "للقلم الضوئي" التي تم شرحها أعلاه، وفي هذه الطريقة أيضا يتم تسجيل شكل التوقيع، ويلتقط الجهاز سرعة كتابة يد الموقع، والتقاط التي يرفع فيها القلم عن سطح الورقة، والضغط الطي يستعمله الموقع وغير ذلك من الأساليب الحركية، وبتطبيق ذلك فإن تلك الأجهزة تجعل التوقيع باستخدام القياسات الحيوية أكثر صعوبة في التزوير، فلا يتعين فقط على المزور أن يقلد توقيع الضحية بدرجة عالية من الدقة والتشابه بل يجب أن يقلده أيضا بأسلوب حركة يده نفسها في التوقيع، ولا يتوقع أن يكون ذلك ممكنا في إهمال كثيرة.

رابعا: أنماط الأوعية الدموية[2].

هناك إضافة حديثة نسبيا ألحقت بقائمة طرق القياسات الحيوية، وهي تحليل أنماك الدموية كوسيلة من وسائل تحديد الهوية وبالتالي فإن اتساع مكان وتوزعي الأوردة يعتقد أنه فريد، فالأجهزة التي تستخدم القياسات الحيوية لأنماط الأوعية الدموية هي نمطيا مثل تلك القائمة على قياس اليد، وتتطلب

[1] -Alain Bensoussan, la signature électronique, premier réflexion après la publication de la directive du 13 décembre 1999 et la loi 13 mars 2000 ,p253.

[2] - محمد أحمد نور حسيبة، المرجع السابق، ص110 .

أيضا الشخص يده على قارئة المنحنيات التي تأخذ القراءة عن طريق المسح الضوئي بالأشعة تحت الحمراء ويقوم بترقيم هذه المعلومات إلى أرقام، وعلى الرغم من أن المسح الضوئي يعمل بموجات تحت الحمراء فإن الجروح الخارجية لن تؤثر على التوقيع المراد إنشاؤه.

حيث أن هذه الأجهزة قد طرحت مؤخرا في الأسواق، إلا أنها إلى حد ما يصعب تقديرها إذا كانت هذه التقنية سوف تناسب عملية إنشاء توقيعات الكترونية آمنة، نستطيع مواجهة من يحاولون التزوير في المستقبل عند محاكاة أنماط بشكل الأوعية الدموية للشخص.

فصلا عن فعالية تلك التقنية تتأثر بعوامل مثل السن، والمشاكل الطبية المتعلقة بالأوعية الدموية، وأيضا الأجهزة الحالية كبيرة الحجم إلى حد ما مقارنة بنظيراتها المستخدمة في مجالات القياسات الحيوية الأخرى، التي رسخ استعمالها، بيد أنه مع التقدم التكنولوجي، فقد يزيد استخدام أنماط الأوعية الدموية في إنشاء التوقيع الالكتروني[1]

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص88.

الفصل الثاني

الجرائم الماسة بمنظومة التوقيع الالكتروني

مع تعاظم التجارة الالكترونية عبر الانترنت، وتطور تقنيات الاتصال ظهرت جرائم الانترنت، وهي تلك الجرائم ذات التأثير الكبير على التجارة الالكترونية وعمليات التبادل التجاري والصفقات، والمعاملات التجارية والمالية عبر الانترنت والتي تعوق بسهولة إتمام العمليات التجارية الالكترونية، ولما كان التوقيع الالكتروني من أهم عوامل إتمام تلك الصفقات والمعاملات التي تتم دون توفير الثقة له وحمايته من كافة صور الاعتداء عليه، وهذه الحماية لا يتصور تمامها وتحققها إلا بتجريم أفعال الاعتداء عليه في القانون، وتأكيدا لحرص مشرعي الدول المختلفة على وضع الضمانات الكفيلة بحرية التجارة الالكترونية وإصباغ الحماية الجنائية على المستند الالكتروني تم تجريم أفعال الاعتداء على التوقيع الالكتروني فبرغم من أهمية التدابير الوقائية للحد من هذه الأفعال المجرمة، إلا أن ذلك لن يؤدي إلى منع ارتكابها لذلك كان ضروريا أن نتناول في هذا الفصل إضافةإلى التدابير الوقائية تنظيما للجزاء الجزائي لمن تسول له نفسه الاعتداء على التوقيع الالكتروني.

وفي ضوء ما تقدم سوف نقسم دراسة هذا الفصل إلى مبحثين على النحو التالي:

المبحث الأول: الجرائم التقليدية الماسة بالنظام المعلوماتي للتوقيع الالكتروني.

المبحث الثاني: الجرائم المستحدثة الماسة بالنظام المعلوماتي للتوقيع الالكتروني وبياناته.

المبحث الأول: الجرائم التقليدية الماسة بالنظام المعلوماتي للتوقيع الالكتروني

تتمثل المصالح المحمية في شرعية تداول البيانات وسريتها وخصوصيتها وإصباغ الحجية على التوقيع الالكتروني وحماية التوقيع الالكتروني تعني في حقيقة الأمر حماية محتوى وصحة بيانات منظومته الالكترونية من أي فعل من الأفعال الإجرامية الماسة بأمنه وثقته بين المتعاملين به وكذا حجيته في المعاملات التجارية كما هو الحال بالنسبة لجريمة تزوير التوقيع الالكتروني، جريمة إتلاف التوقيع الالكتروني، جريمة الحصول على توقيع الكتروني بوسائل احتيالية وغيرها من الجرائم التي سنتطرق لها في هذا المبحث على النحو التالي:

المطلب الأول: الجرائم الاعتداء بالمحل التوقيع الالكتروني

المطلب الثاني: الجرائم الاعتداء على حجية التوقيع الالكتروني

المطلب الأول: الجرائم الماسة بالمحل الالكتروني:

نتعرض في هذا المطلب إلى الحماية الموضوعية للمحل الالكتروني، والاهتمام بجرائم الأموال، وهي البيانات التي تتناول الذمة المالية، وإذا ما تم تناول تلك الحماية فلابد من التعرض لها في بعض الجرائم التي تمس الذمة المالية، وسنحدد في هذا المطلب الجرائم المرتكبة بشكل متكرر وسنخص بدراستنا السرقة والنصب وخيانة الأمانة وتوضيح أركان الجريمة المادية والمعنوية والشرعية، وبناءا على ما تقدم سنقسم هذا المطلب إلى ثلاث فروع التالية:

الفرع الأول: جريمة السرقة الالكترونية:

جريمة السرقة الالكترونية بصورة عامة تعتبر من الجرائم التقليدية وتعد من أخطر الجرائم التي ينصب محلها على المال، وتؤدي إلى حرمان صاحب الحق بصورة كلية.

أما في المجال المعلوماتي فالوضع يختلف، حيث أن محل الجريمة هنا يختلف عنه في الجريمة بصورتها التقليدية، فمحلها هنا المعلومات والبيانات الموجودة داخل النظام المعلوماتي أو داخل الحاسب الآلي، والمحفوظة داخل الدعامات المادية، على اعتبار أن المال إما أن يكون ذا طبيعة مادية بحتة، وإما يكون ذا طبيعة مادية يحتوي في مضمونه على قيمة حقيقية معنوية[1].

ولغاية إيضاح هذه الجريمة سوف نتناولها من خلال مجموعة من النقاط الضرورية.

[1]- يوسف بن سعيد الكلباني، الحماية الجزائية للبيانات الالكترونية في التشريعين العماني والمصري، دار النهضة العربية، الطبعة الأولى، مصر، 2017، ص 86.

أولا: تعريف جريمة السرقة.

تعد جريمة السرقة من جرائم الاعتداء على الملكية والحيازة، فهي تؤدي إلى إخراج المال من حيازة صاحبه أو حائزه أو إدخاله في حيازة شخص آخر بدون وجه حق وهي أكثر الجرائم وقوعا وخطورة وصلة بالحياة العملية مقارنة مع غيرها من الجرائم[1].

أ- **لغة:** "بأنها أخذ الشيء في الخفاء وتطلق مجازا على الشيء المسروق سرق منه مالا، كما يطلق مجازا على السمع متخفيا، إذ يقال، استرق السمع ومنه قوله تعالى: "إلا من استرق السمع.....شهاب مبين"[2].

ب-**فقها:** تعرف السرقة في مفهومها الواسع بأنها: "اختلاس مال منقول مملوك للغير بغية تملكه وعرفها الفقه بأنها اعتداء ملكية المنقول وحيازته بنية تملكهن وذهب البعض الآخر في تعريفهم لمفهوم السرقة على أنها اختلاس مال منقول مملوك للغير بغية التملك"[3].

أما في المجال المعلوماتي فقد انقسم الفقه إلى اتجاهين:

الاتجاه الأول يذهب بالنسبة لبيانات عبر الانترنت أو من يقوم بسرقة البيانات فإنه يقر بأخذ نسخة من البيانات أو المعلومات أو برامج معينة وإدخالها في حيازته.

بناء على هذا فإن السرقة لهذا المعنى تتعارض وتعريف السرقة المنصوص عليها في التشريعات العقابية وفي إمكانية أن تكون البيانات أو البرامج محلا للسرقة لأنها أشياء غير محسوسة وغير مادية في حين يذهب الاتجاه الثاني إلى أن جريمة السرقة بمفهومها التقليدي يمكن أن تقع على البرامج والمعلومات وبالتالي تخضع لذات أحكام جريمة السرقة فالركن المادي يتمثل في أخذ نسخة من المعلومات أو البرامج دون إذن صاحبها أو علمه أي أن السرقة هي عبارة عن استيلاء على المعلومات والبيانات دون علم وإرادة صاحبها الشرعي سواء كانت مخزنة على أشرطة ممغنطة أو اسطوانات مدمجة[4].

وبين هذين الاتجاهين رأى البعض إلى حصر نطاق مفهوم هذه الجريمة حيث عرضها على أنها "الاستيلاء غير المشروع على الأرقام والمعلومات الخاصة بالبطاقات الائتمانية المملوكة للغير عبر شبكة المعلومات يهدف الحصول على السلع والخدمات"

---

[1]- دلخار صلاح الدين بوتاني، الحماية الجنائية الموضوعية للمعلوماتية، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، مصر، 2016، ص 76.

[2]- سورة الحجر، الآية رقم 18.

[3]- شمسان ناجي صالح الخيلي، الجرائم المستحدثة بطرق غير مشروعة لشبكة الانترنت، دار النهضة العربية، القاهرة، 2009، ص 172.

[4]- يوسف بن سعيد الكلياني، مرجع سابق، ص 77.

ونحن نرى إلى أن مفهوم سرقة البيانات الالكترونية من الممكن أن تأخذ بذات المفهوم التقليدي بجريمة السرقة إلا أنه يتوسع في تحديد المحل الذي ينص عليه هذه الجريمة المتعلقة بالبيانات الالكترونية.

وعليه يمكن تعريف سرقة البيانات الالكترونية على أنه عبارة عن الاستيلاء على البيانات أو المعلومات بواسطة اختراق أنظمة الحاسب الآلي أو المواقع الالكترونية وحيازتها بطريقة تمكن الغير من حرمان صاحب الحق منها والبعض من مكوناتها، وذلك بدون علم وعلى غير إرادة مالكها أو حائزها[1].

ثانيا: الركن المادي الاختلاس المعلوماتي في جريمة السرقة الالكترونية:

إن الفعل المادي لسرقة أي فعل الاختلاس يتكون من عنصرين هما: العنصر الموضوعي المادي الذي يتمثل في الاستيلاء على الحيازة على نحو يؤدي لإخراج الشيء من حيازة المجني عليه وإدخاله في حيازة أخرى والعنصر المعنوي المتمثل في عدم رضا المالك أو الحائز.

ووفقا للمفهوم التقليدي لفعل الاختلاس عرف البعض الاختلاس المعلوماتي بأنه "الاستيلاء على المعلومات والبيانات دون علم وإرادة صاحبها الشرعي"[2].

1- فعل الاختلاس:

إن الطبيعة المعنوية للمعلوماتية أثارت خلافات في الفقه حول مدى إمكانية ورود فعل الاختلاس على المعلوماتية المعالجة آليا فانقسم إلى اتجاهين:

أ- **الاتجاه الأول:** يرى أنصار هذا الاتجاه في عدم خضوع المعلوماتية لفعل الاختلاس للاختلاف الواضح في الطبيعة بينهما، فالمعلومات ذات طبيعة معنوية، بينما الاختلاس ذو طبيعة مادية، ويسوق أنصار هذا الاتجاه إلى عدة حجج منها:

– المعلوماتية لا تعد قبيل الأشياء وكونها يتم الحصول عليها إما عن طريق الالتقاط السمعي أو البصري أو بطريقة إعادة نسخها على دعامات يملكها الجاني ذاته[3].

[1]- أيمن عبد الله فكري، جرائم نظم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2007، ص 523.

[2]- دلخار صلاح بوتاني، مرجع سابق، ص 86.

[3]- عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيا، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2009، ص 301.

– أن الاختلاس اللازم لقيام جريمة السرقة غير متحقق في إطار المعلوماتية فالاختلاس بمعناه المعروف يؤدي إلى إخراج المال من حيازة مالكه أو حائزه أو إدخاله في حيازة الجاني، بينما في حالة المعلوماتية فإن مالك أو حائز المعلومات لا يفقدها بل كل ما في الأمر هو ازدياد عدد المطلعين عليها.

– إن من غير المتصور اختلاس شيء معنوي غير مادي على استغلال من دعامته، ومرد ذلك طبيعته، الشيء الذي تقتضي حيازته داخل دعامة معينة وفي هذا الغرض تتحقق جريمة السرقة بمفهومها التقليدي بخروجه من حيازة صاحبه إلى حيازة الجاني، بينما المعلومات الموجودة على شاشة الحاسب الآلي فلا تصلح محلا للسرقة[1].

ب-**الاتجاه الثاني:** وفق أنصار هذا الاتجاه فإن المعلوماتية تخضع لفعل الاختلاس، معتمدين في ذلك علىالتوسع في مفهوم الاختلاس، حيث تغطي حالات الاختلاس الوقتي لشيء بنية استعماله وإعادته بعد فترة زمنية قصيرة ومن ثم تجريمها لعمليات النسخ أو نقل المحتوى المعلوماتي ويستند هذا الاتجاه على عدة حجج.

– إن المعلوماتية قابلة للتحديد والقياس مثل الطاقة الكهربائية، فمن الممكن قياسها عن طريق كمية المعلومات بالشريط أو الأسطوانة ويمكن قياسها عن طريق الشريط أو الفكرة المعبرة عنها أيضا[2].

– الاختلاس ليس له طبيعة واحدة بل يتفق وطبيعة المحل الذي يرد عليه، فإذا كان المحل شيئا غير مادي معنوي فإن الاستيلاء عليه سيكون بالطرق غير المادية تبعا إلى ذلك، والمعلوماتية كونها خلقا فكريا فإن الاختلاس الذي يرد عليها سيكون من نفس طبيعتها، أي حيازة فكرية للشيء المعلوماتي[3].

2- ركن محل الاختلاس المعلوماتي.

وفقا للمفهوم التقليدي لجريمة السرقة فإن محل الاختلاس يجب أن يكون مالا منقولا وأن يكون مملوكا للغير تبعا لذلك فإن محل السرقة المعلوماتية هو مال معلوماتي مملوك لغير الجاني والمعروف أن جريمة السرقة المعلوماتية إنما تنص على المعلوماتية وعليه لبيان ركن المحل فيها لابد أن تبين ما مدى اعتبار المعلومات مالا منقولا مملوكا لغير الجاني أ ملا، وذلك من خلال ما يلي:

– أن يكون محل السرقة المعلوماتية مالا: مدى اعتبار المعلومات محل سرقة المعلوماتية مالا:

---

[1]- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الطبعة الثانية، دار النهضة العربية، القاهرة، 2011-2012، ص 28.

[2]- المرجع نفسه، ص 29.

[3]- هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية المنعقد بـ 25 أكتوبر 1993، القاهرة، مصر، ص 310.

إن القيمة الاقتصادية التي تتمتع بها المعلومات جعل منها قيمة مالية قابلة للتملك والاستغلال وهذه القيمة تتعاظم يوما بعد يوم، مما أصبح من غير المقبول التغاضي عن أهميتها في ظل اعتماد المجتمع عليها في شتى المجالات، الأمر الذي اقتضى إسباغ وصف المال على المعلومات.

– أن يكون محل السرقة المعلوماتية مالا منقولا مدى اعتبار المعلومات محل جريمة السرقة المعلوماتية من قبيل المنقولات

من المعلوم أن النصوص الجنائية الخاصة بالسرقة لا توفر الحماية الجنائية سوى الأموال المنقولة، والتي تعني وفقا للمفهوم التقليدي أية مادة كونية غير بشرية قابلة للنقل من مكان لآخر سواء كانت صلبة أو سائلة أو غازية أي أن تكون ذات طبيعة مادية[1] بيد أن القضاء قد وسع من مفهوم المنقول واتجه إلى القول أنه "لا يقتصر وصف المال المنقول على ما كان جسما متحيزا قابلا للوزن طبقا لنظريات الطبيعة، بل هو يتناول كل شيء مقوم قابل للتملك والحيازة والنقل من مكان إلى آخر"[2].

هذا ما دفع جانبا من الفقه إلى إضفاء وصف المنقول على المعلومات، وذلك بناءا على قابليتها للانتقال من مكان إلى آخر وإمكانية حيازتها والإطلاع عليها من خلال شاشة الحاسب الآلي، دون اشتراط انتقال المحتوى والهيكل، فالانتقال هنا يكون ذهنيا، أي بمجرد تشغيل الحاسب الآلي ورؤية المعلومات على شاشته تنتقل هذه المعلومات إلى ذهن هذا المتلقي[3] على اعتبار المنقولات تختلف بحسب طبيعتها فيما يتعلق بطريقة انتقالها، فمنها ما ينتقل باليد كالبضائع، وما ينتقل بالتدوين عن طريق الفاكس، ومنها ما ينتقل عبر الدوائر أو الالتقاط الذهني كالمعلومات.

– ونحن بدورنا مع من ذهب إلى إسباغ وصف المنقول على المعلومات المعالجة آليا كونها شيئا قابلا للانتقال دون أن يطرأ عليها تلف سواء عن طريق الدعامة المادية المخزونة أو عن طريق عمليات النسخ واللصق أو الإرسال سواء نفي أصلها كما في النسخ والإرسال أو لم يبق الأصل كما في النقل عن طريق الأمر.

والجدير بالذكر أن اعتبار المعلومات من قبيل المنقولات لا يعني إمكانية اعتبارها محلا للاختلاس في جريمة السرقة، وبخاصة ضمن فكر الاتجاه المعارض لوقوع الاختلاس على المعلومات والتي تقضي حسب رأيهم انتقال المال من حيازة الشخص إلى آخر أي حرمانه منها، فهو قد لا يتحقق في إطار المعلوماتية كما في

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص 104.

[2]- دلخار صلاح بوتاني، مرجع سابق، ص 90.

[3]- هدى حامد قشقوش، مرجع سابق، ص57.

حال نسخ المعلومات مع بقاء الأصل، فمنقول يكتسب هذه الصفة لإمكانية نقله من مكان إلى آخر وليس لإمكانية اختلاسه من عدمه[1].

- أن يكون محل السرقة المعلوماتية مالا منقولا مملوكا للغير مدى صلاحية المعلومات لتكون محلا لملكية الغير.

من المتفق عليه أن جريمة السرقة لا تقع إلا على شيء مملوك لشخص غير الجاني، سواء كان طبيعيا أو معنويا، وقد اختلفت الآراء حول المعلومات كمحل لسرقة المعلوماتية ما إذا كانت تصلح لأن تكون ملكا للغير، فذهب رأي إلى أن المعلومات لا يمكن أن تكون ملكا لأحد، بدعوى أن المعلومات هي نتاج فكري حر لا يمكن أن يكون ملكا لأحد، بدعوى أن المعلومات هي نتاج فكري حر لا يمكن أن يكون ملكا لأحد، فالأفكار حرة مطلقة لا فضل لأحد بمفرده في إيجادها بل هي خلاصة تجارب أشخاص متعددين، غير أنه هناك رأي آخر يرى إمكانية أن تكون المعلومات محل ملكية للغير، فهي ليست مجرد فكرة وإنما مجموعة أفكار أنشأت عنها شيء معنوي، وهو ما يؤكده وجود معلومات ذات قيمة اقتصادية كبيرة يتم الاحتفاظ بها بعيدا عن متناول الجميع.

ونحن بدورنا نؤمن بصلاحية المعلومات لأن تكون محلا لملكية الغير، فالمعلومة عند تخليقها أو استخدامها من قبل شخص فإنه يكون المسيطر عليها، ويمكن رفض إذاعتها، وهذه العلاقة بين المعلومات وصاحبها هي علاقة قانونية، وهي علاقة الحائز بما يحوزه وتنطبق عليه قاعدة الحيازة في المنقول سند الملكية، أضف إلى ذلك أن المعلومات أصبحت في مصاف الأموال الاقتصادية المهمة كما سبق بيانه.

ثالثا: الركن المعنوي لجريمة السرقة المعلوماتية.

تقوم جريمة السرقة المعلوماتية على ركن معنوي يتمثل أساسا في القصد الجنائي الذي بدوره يرتكز على عنصري العلم والإرادة بحيث يتعين على الجاني أن يدرك أنه يختلس مالا مملوكا لغيره وأن إرادته تتجه إلى إحداث ذلك السلوك أو يتمثل ذلك في جريمة سرقة البيانات عند انتهاك الأنظمة الآلية التي تحوي أرقاما سرية، مما يدل على سوء نية مرتكب الفعل ويظهر القصد الجنائي عندئذ في فترة البقاء غير المشروع، ولكن لربما يشكل عبء الإثبات في هذه الحالة عقبة في توافر هذا القصد من عدمه.

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 90.

أما بخصوص القصد الجنائي الخاص في جريمة السرقة هو يتمثل في "نية تملك الشيء" مما يعني أن جريمة السرقة من الجرائم العمدية التي تتطلب قصدا جنائيا خاصا يتمثل في نية تملك الشيء المسروق[1] ويستدل على توافر هذا القصد من خلال القرائن والأدلة.

وقد قضت، محكمة النقض المصرية "أن القصد الجنائي" في جريمة السرقة ينحصر في قيام العلم عند الجاني وقت ارتكاب الجريمة أنه يختلس المنقول المملوك للغير رغم إرادة مالكه بنية أن يمتلكه هو نفسه[2].

ويذهب القضاء الفرنسي إلى أن انتهاك النظام الأمني الخاص بالأنظمة الالكترونية يعتد به كسوء نية وقصد سرقة منفعة حتى ولو كانت نية التملك وقتية التي تتوافر بمجرد ارتكاب الشخص عمل من أعمال التصرف والتي يظهر فيها بمظهر المالك[3].

واشترطت بعض القوانين المقارنة توافر نية التملك في جريمة السرقة حيث استخدم قانون العقوبات الفرنسي في المادة 1/311 تعبير "من اختلسبسوء نية.

وكذلك فإن القانون الإنجليزي استخدم مصطلح سوء النية للتعبير عن نية التملك حين نص في قانون السرقة لسنة 1968 "يعتبر الشخص مرتكبا للسرقة إذا استولى لنفسه بسوء نية على أموال تنتمي إلى الغير بنية حرمان هذا الأخير بشكل دائم منه[4].

والسرقة هنا يترتب عليها حيازة الغير لنسخة من البيانات والمعلومات دون أن تؤدي إلى حرمان صاحبها ممن حيازتها أو التصرف فيها، كما يوجد رأي فقهي يرى أن القصد الجنائي الخاص المتمثل في نية التملك لا يتوافر في حالة الالتقاط الذهني للبيانات والمعلومات أو سماها وبرر ذلك بأن الجاني لم يقصد حرمان الحائز القانوني لها وإنما شاركه في الانتفاع بها من خلال الإطلاع عليها، فإثبات القصد الجنائي هو مزيج من إثبات الوعي بملابسات الفعل المجرم واتجاه الإرادة إلى تحقيق النتيجة المتوقعة من جراء هذا الفعل.

ولهذا فإن عناصر القصد الجنائي بعنصرية العام والخاص تتوافر في الشخص مرتكب جريمة سرقة البيانات الالكترونية.

---

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص 305.

[2]- مجموعة أحكام محكمة النقض رقم 15 لسنة 1964/06/23، ص 66.

[3]- خالد ممدوح إبراهيم، مرجع سابق، ص 306.

[4] -" a person is guilty of theft if the dishonesty appropriates property belonging to another with the intention of depriving the other of it: and "thief" and "steal" shall de construed accordingly".

خامسا: موقف القوانين العقابية من جريمة السرقة المعلوماتية:

تتجلى العقبة الأساسية أمام تطبيق نصوص قوانين العقوبات التقليدية على جريمة السرقة المعلوماتية في أن هذه النصوص قد صيغت في وقت كان يعتد فيه بالأشياء المادية، وضعت لحمايتها من صور الاعتداء المألوفة وقتها الأمر الذي تصعب معه مواجهة أفعال التعدي التي تقع في الوقت الحالي على عناصر ومكونات المعلوماتية ذات الطبيعة المعنوية، كما أن تطبيق هذه النصوص قد يتعارض أحيانا والطابع الخاص للوسائل المعلوماتية المستحدثة والمستخدمة في تنفيذ الجريمة[1]، وفي سبيل تخطي هذه العقبة وتوفير الحماية الجنائية للمعلوماتية التي غدت ذات أهمية اقتصادية كبيرة التجأت بعض الدول إلى إصدار تشريعات خاصة لمواجهة هذه الجرائم المعلوماتية والبعض الآخر إلى تعديل قوانينها العقابية القائمة كي تتلاءم مع أنماط السلوك الإجرامي المستحدث وعليه سوف نبين فيه موقف بعض القوانين العقابية العربية الأجنبية.

موقف بعض القوانين العربية

تباينت القوانين العقابية العربية فيما بينها في نطاق توفير الحماية الجنائية الموضوعية من جريمة السرقة المعلوماتية ففي الوقت الذي أصدرت فيه بعض الدول تشريعات تتضمن نصوصا خاصة لمواجهة جريمة السرقة المعلوماتية، التجأت دول أخرى إلى تعليل النصوص الخاصة بالسرقة في قوانينها القائمة كي تتلاءم مع السمات المستحدثة لجريمة السرقة المعلوماتية، بينما البعض الآخر من الدول أبقت على النصوص الجنائية القائمة والخاصة بجريمة السرقة.

ففي قانون دولة الإمارات العربية المتحدة: على الرغم من أن المشرع خطا خطوة يحمد عليها لإصدارها لقانون الاتحادي رقم 02 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات والمؤلف 29 وتزويرها، غير أنه غفل عن تجريم السرقة المعلوماتية، حيث جاء القانون خاليا من أي نص تجريم السرقة المعلوماتية وفي ظل عدم إمكان تطبيق النصوص التقليدية يستوجب الأمر تدخل المشرع لسد هذا النقص التشريعي.

وفي مصر: لا يوجد نظام قانوني خاص يحكم الجرائم المعلوماتية، ولا يوفر القانون الجنائي المصري أي حماية من جريمة السرقة المعلوماتية ومن ثم فالمشرع المصري مدعو كباقي المشرعين إلى سن تشريعات خاصة بهذه الجرائم أو تعديل التشريع العقابي القائم بما يمكن تطبيقه على هذه الأنماط المستحدثة من السلوك الإجرامي[2].

[1]- عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص 329.

[2]- دلخار صلاح بوتاني، مرجع سابق، ص 92.

بينما في التشريع الجزائري : فقد سار المشرع على نهج المشرع الفرنسي في مواجهة الجرائم المعلوماتي من خلال إدخال تعديل على قانون العقوبات الجزائري بموجب القانون رقم 09-01 والمؤرخ في 2009/02/29 حيث فرض حماية جنائية خاصة على أنظمة المعالجة الآلية للمعلومات أو البيانات في المواد 394-394 مكرر08 من قانون العقوبات الجزائري المتضمن الأمر 66-156، لكنه مع ذلك لم يبسط هذه الحماية الجنائية على المعلومات من السرقة المعلوماتية، وإن كان البعض يرى أنه بالإمكان استخلاص قيام جريمة السرقة المعلوماتية من نص المادة394-02 من قانون العقوبات الجزائري، شريطة حيازة المعلومات والانتفاع بها واستعمالها سواء لأغراض شخصية أو الاتجار فيها وإلا كانت الحيازة معنوية.

فموقف القوانين العقابية العربية: من جريمة السرقة المعلوماتية يؤيد من يرى أن نصوص السرقة في أغلب قوانين العقوبات العربية القائمة لا يمكن تطبيقها على جريمة السرقة المعلوماتية، إذ وفقا للفهم القانوني في إطار نظرية الحماية الجنائية للحيازة التي تأسست عليها نصوص السرقة التقليدية والمستقر في فقه القانون الجنائي:

- إن محل جريمة السرقة هو المال المنقول ذو طبيعة مادية مملوك للغير.
- والدليل على ذلك عدم إمكان بسط هذه النصوص التقليدية للسرقة على المال المنقول ذي الطبيعة المعنوية كالكهرباء.

فضلا عن أهم المبادئ المستقرة في القانون الجنائي هو:

- مبدأ الشرعية الجنائية الذي يحظر التجريم والعقاب على أي سلوك دون وجود نص قانوني صريح بذلك.
- كذلك مبدأ حظر القياس في النصوص الجنائية الموضوعية والتوسع فيه فلا يقبل قياس سرقة المعلومات على سرقة الماديات، وجعل ما تقدم نجد بعض الدول كسلطنة عمان مثلا قامت بتعديل قانون العقوبات فيها لمواجهة الجرائم المعلوماتية ومنها جريمة السرقة المعلوماتية[1].

أما في التشريعات الأجنبية فنجد:

الولايات المتحدة الأمريكية مثلا وعلى الصعيد الفيدرالي يجري العمل على مواجهة سرقة المعلوماتية بوصفها سرقة للأسرار التجارية، ووفق التعديل الصادر سنة 1996 على قانون العقوبات الأمريكي في

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 100.

الجزء الأول من الفصل الثالث والبند رقم 18-461 تحت قسم المال العام والذي ينص على أنه "أي شخص يسرق أو يختلس أو يقوم عن عمد أو بدون وجه حق باستغلال الآخرين أو التصريح له بالبيع أو التصرف في أي تسجيل أو مستند... وهو يعلم ذلك سوف يتم تغريمه بما لا يزيد عن 10 آلاف دولار أمريكي أو يسجن لمدة لا تزيد عن عشرة سنوات أو كلاهما"، حيث طبقتها المحاكم على سرقة المعلومات والتي سمتها وزارة العدل الأمريكية جرائم المعلومات.

أما في المملكة المتحدة: فقد استحدثت سنة 1990 قانون يعالج فيه إساءة استخدام الحاسبات الآلية والذي تم بموجبه تجريم عملية دخول أي فرد على المعلومات المختزنة بالنظام المعلوماتي أو على برامجه وكذلك تعديلها أو محاولة فعل ذلك بصورة غير مشروعة كما عالج بعض صور سرقة وقت النظام المعلوماتي، غير أن هذا التشريع لم يتضمن نصا صريحا بتجريم سرقة المعلومات[1].

وفي فرنسا: التي كانت سباقة دائما في مواجهة التحديات التي أفرزتها المعلوماتية أصدر قانون رقم 17-78 في يناير سنة 1978 لحماية البيانات الاسمية لمواطنين في مواجهة نظم المعالجة الآلية للمعطيات، مؤكدة بذلك أن المعلوماتية يجب أن تكون في خدمة المواطن وليست وسيلة للاعتداء عليه وعلى حقوقه وحياته الخاصة وحيرته، غير أن استفحال ظاهرة الإجرام المعلوماتي اقتضت من المشرع الفرنسي أن يتدخل مرة ثانية بتضمين قانون العقوبات نصوصا جديدة من شأنها مواجهة هذه الظاهرة، وتم بالفعل إصدار قانون جديد برقم 19 الصادر في 05 يناير 1988 بشأن الغش المعلوماتي وخصص له الفضل الثالث باسم "الاعتداءات على نظم المعالجة الآلية للمعلومات" والجدير بالإشارة أن قانون رقم 19 يناير 1988 لم ينص على تجريم السرقة المعلوماتية وكان المشرع الفرنسي قد حاول تجريم السرقة المعلوماتية من خلال اقتراح استخدام كلمة متطورة لتناسب الموضوع ولتعبر عن الاختلاس وهي كلمة الالتقاط وإضافتها لنص المادة 307 فقرة 1 "كل من التقط بطريق الاختلاس والتحايل برنامجا أو معلومة أو أي عنصر من عناصر المعالجة الآلية للبيانات يعاقب بالحبس[2].

[1]- ربيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011، ص 86.

[2]- عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص 331.

الفرع الثاني: جريمة الحصول على التوقيع الالكتروني بالوسائل الاحتيالية الاحتيال المعلوماتي.

يعد الاحتيال في مجال نظم معلومات التوقيع الالكتروني من أهم الجرائم التي يمكن أن تقع على التوقيع الالكتروني ويسبب خسائر اقتصادية فادحة، وذلك نظرا للتطور المذهل في مجال التعامل واختزان التوقيعات الالكترونية في حاسبات آلية موصولة بشبكة الانترنت، بالإضافة إلى التطور المذهل في اختراق الإجراءات الأمنية لنظم وشبكات المعلومات، وهو ما يهدد معلومات التوقيع الالكتروني بالاحتراف لذا فقد جرمت التشريعات العديدة للاحتيال سواء في صورته التقليدية وهو ما جرمته المادة 336 من قانون العقوبات المصري المعدلة بقانون 29 لسنة 1982 وكذا في القانون الفرنسي بالمادة 405 من قانون العقوبات الفرنسي القديم والتي حلت محلها المادة 313 من قانون العقوبات الفرنسي الجديد[1].

وكذا في دولة الجزائر فقد جرم النصب والاحتيال بنص المادة 372 من قانون العقوبات الجزائري أما الاحتيال الذي يستهدف الوصول إلى نظم المعلومات وشبكات الحاسب الآلي التي تحوي التوقيعات الالكترونية والحصول عليها بالطرق الاحتيالية فقد نصت عليها الاتفاقية الأوروبية لمكافحة جرائم المعلوماتية في المادة 08 منها وكذا التوجيهات الأوروبية في التوصية رقم 09/89 أما القانون النموذجي فقد نص على هذه الجريمة في المادة 04 والمادة 06 من القانون[2] وغيرها من القوانين، ولدراسة جريمة النصب والاحتيال المعلوماتي لابد من التطرق إلى النقاط التالية.

أولا: تعريف جريمة الاحتيال المعلوماتي:

الاحتيال المعلوماتي وصف يشير إلى صورة مستحدثة للاحتيال تقوم على إساءة استخدام الحاسبات الآلية والتلاعب في نظم المعالجة الآلية للمعلومات بغية الحصول بغير وجه حق على أموال أو أصول أو خدمات، وهي بهذه الصورة تتميز عن الاحتيال التقليدي بعدة سمات أهمها التعقيد الناجم عن استخدام المفاتيح والشفرات والوسائل الالكترونية في ارتكابه ومحلها ذو الطبيعة المعنوية المتمثل في المعلومات وكذا إمكانية ارتكابه عن بعد.

فيعرف الاحتيال المعلوماتي بأنه: "التلاعب بالبرامج أو البيانات بالتغيير فيها بما يترتب عليه إيهام المجني عليه بصحتها والتسليم بها"

[1]- حسام محمد نبيل الشنراقي، مرجع سابق ص 179.

[2]- تنص المادة 04 من القانون العربي النموذجي على: " كل من استحوذ بالالتقاط بطريق التحايل على البرامج والبيانات المخزنة بالحاسب والمسجلة على جميع وسائط التخزين المتعددة أو التي تظهر على الشاشة يعاقب بالحبس الذي لا تقل مدته عن... تترك لتقدير كل دولة وبالغرامة... تترك لتقدير كل دولة".

-وتنص المادة 06 من ذات القانون "كل من استخدم بطاقة ائتمان للسحب الالكتروني بطرق احتيالية أو استخدم اسم كاذب...".

كما عرفة البعض الآخر الاحتيال المعلوماتي: "التلاعب العمدي بالمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، أو أية وسيلة أخرى من شأنها التأثير في الحاسب الآلي حتى يقوم بعمليات على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع وإلحاق ضرر بالغير[1].

مما تقدم يتبين لنا أن الاحتيال المعلوماتي يتماثل مع الاحتيال التقليدي فيما يتعلق باستخدام وسائل خداع من أجل الاستيلاء على أموال المجني عليه، ويختلف معه كونه ينطوي على استخدام الجاني للحاسب الآلي والوسائل التقنية في خداع وإيهام المجني عليه ودفعه إل تسليم أمواله المتمثلة في القيم المعلوماتية.

ثانيا: أركان جريمة الاحتيال المعلوماتي:

جريمة الاحتيال شأنها شأن باقي الجرائم ينبغي لقيامها أن تتحقق أركانها، لذا فدراسة جريمة الاحتيال المعلوماتي تقتضي دراسة أركانها التالية:

أ- الركن المادي لجريمة الاحتيال المعلوماتي:

الركن المادي لجريمة الاحتيال يتألف من ثلاثة عناصر هي السلوك الإجرامي والنتيجة الجرمية والعلاقة السببية وتثير هذه العناصر في مجال الاحتيال المعلوماتي الكثير من خلاف والجدل كونها جريمة على درجة من التعقيد سواء كان ذلك من حيث طبيعة المحل الذي ترد عليه ومن حيث الوسائل التي ترتكب من خلالها، الأمر الذي يقتضي البحث في مجموعة الإشكالات القانونية التي قد تواجهنا ونحن بصدد تطبيق القواعد العامة في جريمة الاحتيال التقليدية على جريمة الاحتيال المعلوماتي، والتي منها مدى انطباق وصف المال على المعلومات التي هي محل جريمة الاحتيال المعلوماتي ومدى إمكانية ممارسة الوسائل الاحتيالية على الحاسب الآلي والنظام المعلوماتي المرتبطة به، ومدى اعتبار تسليم الأموال الكتابية بمثابة تسليم للمال؟ وهو ما سنحاول دراسته والتطرق إليه في الفقرات التالية[2]:

1- **السلوك الإجرامي**: استعمال الجاني وسيلة من وسائل الخداع المنصوص عليها في القانون.

وهي الأعمال والمظاهر الخارجية التي يلجأ إليها الجاني لدعم ما يصدر عنه من كذب أو تغيير في الحقيقة لتحقيق أغراض معينة تمكنه من الاستيلاء على مال الغير وإيقاعه في الغلط[3] والجدير بالذكر

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 127.

[2]- دلخار صلاح بوتاني، مرجع سابق ، ص 134.

[3]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 189.

أنه من الصعب حصر المظاهر الخارجية الداعمة للاحتيال كونها متطورة ومتجددة تبعا إلى التطورات التي تشهدها مختلف مجالات الحياة وبخاصة في ميدان الاختراعات التي يكشف عنها العلم[1].

وتتنوع وسائل الاحتيال المعلوماتي لكنها تتفق في انطوائها على التلاعب بالبيانات والمعلومات التي يحتوي عليها النظام المعلوماتي من أجل تحقيق ربح مادي غير مشروع وحاول جانب من الفقه تحديدها وسوف نوضح أهمها باختصار فيما يأتيك

- **التلاعب في مرحلة إدخال المعلومات:**

من الملاحظ أن معظم حالات الاحتيال في مجال المعلوماتية تكون بالتلاعب في المعلومات والبيانات التي يتم ادخلها لنظم المعلومات وشبكات الحاسب الآلي وذلك لسهولته في هذه المرحلة حيث لا يتطلب مهارة خاصة وتتمثل عملية إدخال البيانات في تغذية نظم المعلومات التوقيع الالكتروني بالبيانات والمعلومات الخاصة بالتوقيعات الالكترونية وبرامجها وقواعد بياناتها ونظم معالجتها وعملية إدخال البيانات تتم عن طريق القائم بالتلاعب فيها أو آخر، وهي متعددة[2] كإدخال بيانات لا وجود لها أصلا أو بيانات محرفة في بعض الأحيان أو بيانات تشتمل على الأمرين معا[3].

- **التلاعب في البرامج:**

هي وسيلة تتميز بقدر كبير من التعقيد ومن ثم فهي تتطلب أن يكون مستخدمي هذه الوسيلة من الجناة من الخبراء في استخدام نظم المعلومات والحاسبات، كما أنه من أصعب الوسائل من حيث إمكانية اكتشافه وأكثرها خطورة ويتم التلاعب في البرامج بإحدى الوسيلتين:

قد تتم عن طريق استخدام البرامج الخبيثة الفيروسات أو عن طريق برامج إضافية يتم إعدادها لغرض الاحتيال من قبل الجناة أنفسهم أو معدة سلفا تهدف بشكل أساسي إلى تعديل المعلومات في الحاسبات الآلية عن طريق إجراء تعديلات مباشرة في ذاكرة الحاسب[4].

---

[1]- صباح رمضان، ياسين صالح، السياسة الجنائية في مواجهة الجرائم المعلوماتية، دراسة تحليلية، رسالة دكتوراه، العراق، 2013، ص 192.

[2]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 192.

[3]-يوسف بن سعد الكلباني، مرجع سابق، ص 126.

[4]- نايل نبيل عمر، الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2012، ص 78.

- **التلاعب في المكونات المادية للحاسب الآلي:**

- قد تمتد أساليب الاحتيال إلى العناصر الميكانيكية للحاسب، أو الدوائر المختلفة التي يتكون منها النظام[1] أو بالدوائر المختلفة التي يتألف منها النظام المعلوماتي، وهذا التلاعب يتطلب درجة كبيرة من العلم بتقنية الحاسب الآلي، الأمر الذي يؤدي ندرة اللجوء إلى هذه الوسيلة وصعبة اكتشافها[2].

- **التلاعب في البيانات التي يتم تحويلها عن بعد:**

التلاعب في البيانات عن بعد جعل الاحتيال أكثر سهولة من ناحية وأكثر صعوبة في الاكتشاف من ناحية أخرى ففي الوسيلة يمكن أن يكون الحاسب الآلي متصلا بوجود وحدة التشغيل المركزية عن طريق شبكة الخطوط الهاتفية العادية أو غيرها من وسائل الاتصال ليتمكن الجاني من إتمام عملية الاحتيال باستخدام النهاية الطرفية الخاصة به دون الحاجة للتواجد داخل المؤسسة المخترقة كما أن هذه الوسائل الاحتيالية تساعد تخطي الجريمة للحدود وهذه الوسيلة هي الأكثر انتشارا في مجال الاحتيال المعلوماتي، ومن صورها التحويل الالكتروني غير المشروع للأموال.

- **استخدام توقيع الكتروني غير صحيح للدخول لنظام مدفوع الأجر:**

إن استخدام توقيع الكتروني غير صحيح للدخول إلى نظام مدفوع تعد من صور "الاحتيال" ويستمد التوقيع الالكتروني صفة عدم الصحة إذا كان مملوكا لآخر أو إذا حصل عليه الجاني قبل تخصيصه لآخر وتمكنه من استخدامه بغير حق وقد كانت هذه الوسيلة محل جدل في إطار التشفير المجرد في قضية "R.V.GOLD"في المملكة المتحدة والتي كانت من أسباب إصدار قانون استخدام الحاسبات عام 1990م[3].

ب-النتيجة الجرمية: (تسليم المال)

التسليم هو النتيجة التي يتوخاها الجاني من استخدامه الوسائل الاحتيالية فالتسليم هو سلوك صادر عمن خدع بالاحتيال الواقع من الجاني، بمقتضاه ينقل إلى الجاني أو إلى غيره المال موضوع الجريمة أي بمعنى ممارسة الجاني لوسائل الاحتيال أوقع المجني عليه في الغلط ودفعه إلى تسليم ماله للجاني، أما في مجال الاحتيال المعلوماتي فإن التسليم يثير العديد من التساؤلات والتي من بينها:

---

[1]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 169.

[2]- نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقه، دار النهضة العربية، القاهرة، 2003-2004، ص 136.

[3]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 197.

ما مدى انطباق وصف المال على معلومات التوقيع الالكتروني ففي ظل هذا التساؤل تعددت الآراء الفقهية في هذا الشأن ومن ذلك "catala" حيث اعتبر أن المعلومة مستقلة عن دعامتها المادية وأن المعلومة قابلة للحيازة ما دامت ذات قيمة مادية، وأنها ترتبط بصاحبها بعلاقة قانونية وهي علاقة المالك بما يملكه وأنها تنتهي لمؤلفها بسبب بعلاقة التبني[1].

- فكرة المال أو الشيء الذي يغلب عليه الطابع المعنوي تعد محل الحق وتمكن أن تعتبر مال معنوي ومن ثم يجدر بالقانون حمايتها.

- كل الأشياء المملوكة معنويا يعترف بها القانون وهذا ما يؤكد أن المعلومة قيمة عندما تكون بصدد اختراع أو علامة تجارية أو رسوم أو غيرها وعليه نستخلص أن المعلومة هي بمثابة مال مبتكر بسبب الخصائص الذاتية لحق الملكية الوارد عليه.

ولما كان نشاط الجاني في جريمة الاحتيال يكون من فعل الاحتيال كما أسلفنا وتسليم المال وهو لاحق عن الفعل الأول وهو النتيجة المتوخاة من ارتكاب الجريمة فقد يكون التسليم نقودا أي منقول آخر ذي قيمة مادية كأن يتلاعب الجاني في البيانات المدخلة للحاسب أو المخزنة به أو ببرامجه لكي يتحصل على أموال كتابية[2] وفي هذا الفرض يثور التساؤل حول ما إذا كان قد حصل استيلاء مادي على المال أم لا؟.

فقد ذهب اتجاه إلى اعتبار النقود الكتابية رغم طابعها غير المادي من قبيل الأموال التي تصلح لجريمة الاحتيال وذلك مثل التشريع الانجليزي والكندي المادة 2/282 عقوبات والهولندي في المواد 310.311.322.

وذهبت تشريعات ألمانيا في المواد 242-246 إل عدم اعتبار الأموال الكتابية مالا ماديا ولكنها تعد ديونا ومن ثم يستحيل وقوع الاحتيال أو التسليم عليها.

أما التشريع الفرنسي فقد ذهب القضاء الفرنسي إلى اعتبار نظرية التسليم المعادل حيث طبقها الفقه على كافة أشكال الاحتيال باستخدام الحاسب الآلي، والملاحظ في التشريع في قانون التوقيع الالكتروني 15 سنة 2004 لم يحدد جريمة الاحتيال وإنما ورد النص عاما ليشمل العديد من الأفعال

[1]- عبد الله حسين على محمود، إجراءات جمع الأدلة في محل سرقة المعلومات، بحث مقدم للمؤتمر العلمي الأول، حول الجوانب القانونية والأمنية للعمليات الالكترونية، محور القانون الجنائي، دبي، الإمارات العربية المتحدة، 23 أفريل 2003، ص 163-171.

[2]- النقود الكتابية: "هي مجموعة الودائع لدى البنوك والمؤسسات المالية، يتم تداولها عن طريق الشبكات والتحولات وهذا المنقول يعتبر غير مادي".

حيث حدد المصلحة محل الحماية ولم يحدد الأفعال التي يتحقق بها الاعتداء وأحال ذلك إلى القانون العام وهو في هذا لإطار الاحتيال على نظم معلومات التوقيع الالكتروني.

ووفقا لما سبق النصوص القانونية في مصر وبالتحديد في نص المادة 336 من قانون العقوبات لا يتسع مفهومها للانطباق على جريمة الاحتيال للحصول على التوقيع الالكتروني، حيث أن النص يحدد مفهوم المال في إطار مادي بحت[1].

ج- العلاقة السببية بين وسيلة الخداع وتسليم المال.

لقيام جريمة الاحتيال المعلوماتي لابد أن تتوافر رابطة سببية بين الخداع وتسليم المال إذ لا يكفي لقيام جريمة الاحتيال المعلوماتي أن يصدر من الجاني سلوك إجرامي منصب على وسيلة من وسائل الخداع المنصوص عليها قانونا وحدوث واقعة تسليم المال من المجني عليه إلى الجاني، بل يلزم أن يكون التسليم سواء كان تسليما ماديا أو حكميا من قبل الحاسب الآلي قد وقع كأثر من آثار استعمال لجريمة الاحتيال وبنتيجة لانخداع المجني عليه بها[2].

د- الركن المعنوي في جريمة الاحتيال المعلوماتي:

جريمة الاحتيال المعلوماتي جريمة عمدية يتطلب قيامها توافر القصد الجنائي الذي يتمثل في القصد الجنائي العام: أي انصراف علم الجاني إلى أن ما يقوم به من تلاعب في المعلومات الموجودة في نظام المعلومات الآلي أوإدخال معلومات إلى هذا النظام هو فعل غير مشروع من شأنه أو يوقع الحاسب الآلي في الغلط ويستجيب وفق هذه المعلومات المتلاعب بها، كما يجب أن ينصرف علم الجاني إلى ما يتسلمه من مال مملوك للغير، ويستوي أن يكون عالما أنه مملوك للمجني عليه أو شخص آخر غيره، وأن تتجه إرادته إلى إيقاع الحاسب الآلي في غلط بهدف سلب المال المملوك للغير[3].

أما القصد الجنائي الخاص فهو يتمثل في توافر النية لدى مرتكب الفعل الإجرامي انصراف إرادته إلى حيازة المال المملوك للغير حيازة كاملة[4]، غير أن استيلاء الجاني على المعلومات محل الاحتيال لا يترتب عليه حرمان المجني عليه منها بل تظل في حيازته وتحت سيطرته الخاصة بمعنى أنه لا إمكانية لاستيعاب

[1]- حسام نبيل الشنراقي، مرجع سابق، ص 210.

[2]- عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص 381.

[3]- دلخار صلاح بوتاني، مرجع سابق، ص 142.

[4]- يوسف بن سعيد الكلباني، مرجع سابق، ص 144.

القصد الخاص لجريمة الاحتيال المعلوماتي في ظل مفهوم القصد الخاص المعروف في جريمة الاحتيال التقليدي[1].

ثالثا: موقف القوانين العقابية من جريمة الاحتيال المعلوماتي.

تباينت تشريعات الدول المختلفة في موقفها حول مدى تحيزها لجريمة الاحتيال المعلوماتي والتي يمكن تصنيفها إلى تشريعات أقرت حماية جنائية موضوعية خاصة إزاء الاعتداءات التي تنطوي على الاحتيال المعلوماتي وتشريعات أخرى عدلت قوانينها العقابية القائمة لما من شأنها أن تشتمل بالتجريم لهذه الاعتداءات المكونة لجريمة الاحتيال المعلوماتي.

فنجد أن التشريع السعودي واجه جريمة الاحتيال المعلوماتي بنص خاص في نظام مكافحة جرائم المعلوماتية رقم 17 لسنة 2007 في المادة الرابعة والتي تنص على أنه "يعاقب بالسجن لمدة لا تزيد عن ثلاث سنوات وبغرامة مليوني ريال أو إحدى هاتين العقوبتين".

"كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية: الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع لهذا السند، وذلك عن طريق الاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة.

أما في دولة الإمارات المتحدة العربية: نجد أن القانون الاتحادي يعاقب على ارتكاب جريمة النصب الاحتيال عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات حيث نصت المادة 15 منه على أن "كل من توصل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك باستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن ثلاثين ألفا أو إحدى هاتين العقوبتين"[2].

أما في التشريع الجزائري فلم يتطرق المشرع في التعديل الذي أجراه على قانون العقوبات الجزائري إلى جريمة الاحتيال إذ تنص المادة 372: "كل من توصل إلى استلام أو تلقي أموالا أو منقولات أو سندات أو تصرفات أو أوراقا مالية أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع في إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو عتاد مالي أو بإحداث الأمل في الفوز أو بأي شيء أو في وقوع حادث أو أية واقعة

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 143.

[2]- محمد عبيد الكعبي، مرجع سابق، ص 475.

أخرى وهمية أو الخشية من وقوع أي شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20000 دج[1].

ويستخلص من هذا النص أن ليس كل شيء مادي ومنقول يصلح أن يكون محلا لجريمة الاحتيال بل يجب أن يكون ضمن التعداد الذي ذكره المشرع في هذه المادة، غير أن لفظ المنقول ورد في النص دون تحديد طبيعته أو تقييده من قبل المشرع مما يعطي المجال لتفسير النص على نحو يشمل المعلومات التي هي ذات طبيعة معنوية "غير أن تطبيق هذا النص قد يواجه العديد من الصعوبات منها التسليم وعلى فرض إمكانية وقوعه فإنه لن ينتج عنه حرمان المجني عليه من المعلومات، وهو إذ كان يتفق مع طبيعة المعلومات، فإنه لا يتفق مع طبيعة النشاط الإجرامي لجريمة الاحتيال[2].

أما في فرنسا وعلى الرغم من إصدار وعلى الرغم من إصدار المشرع قانون الغش المعلوماتي رقم 19 لسنة 1988 لمواجهة الجرائم المعلوماتية، ومن ثم إصداره قانون العقوبات الفرنسي سنة 1992، إلا أنه لم يأت نص خاص لجريمة النصب الاحتيال المعلوماتية، وإنما اكتفى بما جاء في المادة 1/313 التي حلت محل المادة 305 من قانون العقوبات القديم، وقد ذهب غالبية الفقه الفرنسي[3] إلى أن غش وخداع أنظمة المعلومات بهدف سلب المال يتحقق بالوسائل الاحتيالية بمفهومها المستقر في قانون العقوبات الفرنسي الجديد مستندا في ذلك على ما انتهت إليه أحكام القضاء الفرنسي من وقوع جريمة الاحتيال على أجهزة الحاسب الآلي، ومن ذلك ما قضت به محكمة استئناف باريس في 11 أغسطس سنة 1989 على مبرمج نظام الحاسب الآلي يعمل في أحد البنوك عنجريمة الاحتيال عندما قام بالتلاعب بالمعلومات داخل نظام الحاسب الآلي لكي يزيد من حسابه في الصرف بتحويلها المال عن أرصدة العملاء إلى رصيده الخاص، حيث اعتبر ذلك من قبيل استعمال وسيلة احتيالية على الآلة الحاسب الآلي وتتحقق بها جريمة الاحتيال.

هذا وتجدر الإشارة إلى أن المشرع الفرنسي وفي نص المادة 1/313 من قانون العقوبات الجديد قد ساوى بين الأموال والخدمات وأجاز أن يكون محل التسليم في جريمة النصب خدمات وليس أموالا فقط،

[1]- راجع المادة 372 من قانون العقوبات الجزائري من الأمر 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، المعدل والمتمم بالقانون رقم 16 -02 المؤرخ في 19 يونيو سنة2016..

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، سنة 2007، ص 103.

[3] -CAPRIOLI (ERIC), « Vote électronique, sécurité, technique et conformité juridique, Communication commerce électronique, revue mensuelle Lexis NexisJuris Classeur, Octobre 2012 , p311.

إذ تتحقق جريمة الاحتيال وتطبق بشأنها نص المادة 1/313 في حالة إذا طلب أحد الأشخاص استشارة من طبيب أو محامي عبر شبكة المعلومات، وأوهمه بسداد أتعابه من خلال بطاقة الائتمان ولم يسددها[1].

المطلب الثاني: جرائم المساس بحجية التوقيع الالكتروني

تبدو ظاهرة جرائم الاعتداء على التوقيع الالكتروني من جوانب عديدة فمن ناحية، أصبح الجاني في تلك الجرائم يتسم بسمات شخصية تجعله دوما سابقا لملاحقته جهات التحقيق لخطوات واسعة، وتأكيد حرص مشرعي الدول المختلفة على وضع الضمانات الكفيلة بحرية التجارة الالكترونية وإسباغ الحماية الجنائية على المستند الالكتروني، ومن ثم تجريم أفعال الاعتداء على التوقيع الالكتروني[2].

وقد يرتبط السلوك المادي لجرائم الاعتداء على التوقيع الالكتروني يتداول البيانات المحرر إلكتروني كجريمة التعامل غير المشروع في نشاط التصديق وانتهاك سرية وخصوصية البيانات كما أنه من المتصور أن يكون محل الجريمة هو المساس بحجية التوقيع الالكتروني في الإثبات كما هو الحال في جريمة تزوير التوقيع الالكتروني أو إتلافه، وعلى ضوء ذلك سوف نقسم هذا المطلب إلى فرعين:

الفرع الأول: جريمة إتلاف التوقيع الالكتروني.

تتضمن أنظمة المعالجة الآلية للمعلومات عناصر مادية بشكل أموال منقولة يمكن أن تكون ملكا للغير مثل الاسطوانات والأقراص الممغنطة والكابلات ومعدات الإدخال والإخراج[3]، ولا نرى صعوبة في تطبيق الأحكام الخاصة بجريمة الإتلاف في حالة إتلاف العناصر المادية لنظام المعالجة الآلية للمعلومات باعتبارها أموالا منقولة، ذلك أن جميع النصوص التي تناولت تلك الجريمة في التشريعات المختلفة تجرم تلك الجريمة تحت مسمى إتلاف المنقولات المادية، وقد انعقد إجماع الفقه عن ذلك[4]، فعلى سبيل المثال تجرم المادة 361 من قانون العقوبات المصري التخريب والإتلاف على المال الثابت والمنقول، والمادة 322 من قانون العقوبات الفرنسي والتي تجرم أفعال التخريب والإتلاف التي تقع على المنقول والعقار.

لكن ما يهمنا في هذا المقام، هو إتلاف المحررات الالكترونية كمال معنوي غير مادي يشكل الفعل المؤثر فيه اعتداء على المحرر الالكتروني ذاته، وهذا ما سنتطرق إليه في هذا الفرع من خلال دراسته

---

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 103.

[2]- أشرف توفيق شمس الدين، الحماية الجنائية لمستند إلكتروني، دراسة مقارنة، دار النهضة العربية، الطبعة الأولى، القاهرة، مصر، ص 04.

[3]- محمد عبيد الكعبي، مرجع سابق، ص 493.

[4]- جميل عبد الباقي الصغير، مرجع سابق، ص 127.

مفهوم جريمة إتلاف التوقيع الالكتروني ودراسته أركانها وكذا موقف التشريعات العربية والأجنبية من هذه الجريمة.

أولا: مفهوم إتلاف التوقيع الالكتروني.

الإتلاف لغة: هو مصدر التلف، بمعنى الهلاك، ويقال: رجل متلاف أي كثير الإتلاف لماله[1].

أما الإتلاف اصطلاحا: فهو التأثير في مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته لاستعمال المعد له، أو بأية طريقة أخرى[2]، فجوهر الإتلاف هو إفقاد المال المتلف منفعته أو صلاحيته للاستعمال في الغرض الذي أعد من أجله، فمحل الحماية الحقيقي ينصرف إلى قيمة الشيء دون مادته، وحماية المادة لا تعد إلا وسيلة لحماية القيمة.

ويعرف الإتلاف المعلوماتي أنه: "محو المعلومات أو البرامج كليا أو تدميرها إلكترونيا أو أن يتم تشويه المعلومة أو البرامج على نحو فيه إتلاف بما يجعلها غير صالحة للاستعمال"[3].

فالإتلاف المعلوماتي هو الذي يقع على المكونات المعنوية للنظام المعلوماتي أي المعلومات والبرامج دون أن يؤدي ذلك إلى إتلاف أي عنصر مادي، أما الإتلاف المنصب على المكونات المادية للنظام المعلوماتي كشاشات العرض والأشرطة والأسطوانات والأقراص الممغنطة والكابلات ومعدات الإدخال والإخراج وغيرها فإنه يخرج عن إطار جريمة الإتلاف المعلوماتي، ولا حاجة إلى إفراد نصوص خاصة بإتلاف المكونات المادية للنظام المعلوماتي كونها تخضع للنصوص العقابية التقليدية التي تجرم إتلاف الأموال المادية[4].

ومن الملاحظ أن النشاط الإجرامي المكون لجريمة الإتلاف المعلوماتي لا يؤدي إلى تعطيل أو إعاقة النظام المعلوماتي أو الإخلال بسير العمل فيه دائما[5]، الأمر الذي يجعل التمييز بين الإتلاف المعلوماتي وبين تعطيل أو إفساد النظام المعلوماتي ومعاملتهما كسلوكين منفصلين من موجبات الاعتبارات العملية، ولذلك نلاحظ أن أغلب التشريعات قد ميزت بين جريمتي الإتلاف المعلوماتي وتعطيل أو إفساد النظام

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 204.

[2]- جميل عبد الباقي الصغير، مرجع سابق، ص 158.

[3]- أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، القاهرة، 2005، ص 112.

[4]- محمد عبيد الكعبي، مرجع سابق، ص 494.

[5]- دلخار صلح بوتاني، مرجع سابق، ص 255.

المعلوماتي، فجريمة تعطيل أو إفساد النظام المعلوماتي تتعلق بتجريم الاعتداء على النظام ذاته، بينما جريمة الإتلاف المعلوماتي موضوع هذا البحث بجرم الاعتداء على المعلومات الموجودة داخل النظام[1].

ثانيا: الركن المادي لجريمة إتلاف التوقيع الالكتروني.

يتمثل السلوك الإجرامي المكون للركن المادي لجريمة الإتلاف المعلوماتي في أفعال الإدخال غير المشروع للمعلومات والبيانات داخل أنظمة الحسابات الآلية أو تدميرها أو التعديل غير المشروع لها، الأمر الذي يستدعي بيان كل صورة من هذه الصور في النقاط التالية:

أ- **فعل إدخال المعلومات:** يقصد بفعل إدخال المعلومات "إضافة معلومات جديدة على دعامة الشيء المادي، الخاص بها، سواء كانت خالية أم توجد عليها معلومات من قبل وذلك قد يتم بهدف التشويش على صحة البيانات والمعلومات القائمة[2].

وبالرجوع إلى التشريعات المختلفة التي جرمت الإتلاف المعلوماتي نجد أ الكثير منها اعتبرت فعل الإدخال صورة من صور الركن المادي لهذه الجريمة كما هو الحال في المادة 3/323 من قانون العقوبات الفرنسي الجديد والمادة 02 من قانون مكافحة الجرائم التقنية للمعلومات في دولة الإمارات المتحدة والمادة 394 مكرر من قانون العقوبات الجزائري.

وبعد إدخال المعلومات إلى نظام الحاسب الآلي أمر يسهل تحقيقه في أولى مراحل تشغيله، وهي مرحلة إدخال البيانات لمعالجتها، حيث تجهز البيانات وتحول إلى شكل أو لغة مقروءة من قبل الجهاز المستخدم في المعالجة، ويكون من السهل تغذية الحاسب الآلي بمعلومات مغلوطة أو مخزنة.

وإن إدخال المعلومات بصورة غير مشروعة في نظام الحاسب الآلي ينتج عنه إضافة إلى تعديل ذاكرة الحاسب الآلي تعديل في المعلومات ذاتها وتدميرها وذلك بمحوها، كما في حالة إدخال أحد البرامج الخبيثة إلى نظام الحاسب الآلي والذي يؤدي إلى إلحاق تعديل أو محو المعلومات الموجودة داخله[3].

ب-فعل محو المعلومات:

يعرف فعل محو المعلومات على أنه: "إزالة جزء من المعلومات المسجلة على الدعامة الموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل أو تخزين جزء من المعلومات إلى المنطقة الخاصة بالذاكرة"[4]،

[1]- محمد عبيد الكعبي، مرجع سابق، ص 122.

[2]- يوسف بن سعيد الكلياني، مرجع سابق، ص 151.

[3]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 318.

[4]- دلخار صلاح بوتاني، مرجع سابق، ص 259.

بمعنى أن محو المعلومات يعني إزالتها أي تدميرها بصورة كلية أو جزئية وقد أشارت المذكرة التفسيرية لاتفاقية بودابست 2001 إلى أن مصطلح محو البيانات يعادل تدمير الأشياء المادية، فهو يهدمها ويجعلها في حالة لا يمكن التعرف عليها[1].

وقد أوصى المجلس الأوروبي في تقريره المرفق 89 9 بخصوص جرائم المعلوماتية، دول الأعضاء بتجريم الأفعال التي تؤدي إلى تدمير المعلومات إتلافها، وقد ميز بين نوعين من أنواع التدمير الذي يلحق بالمعلومات هما محو المعلومات أي إزالتها تماما وإخفاء المعلومات، حيث يمكن الوصول إليها دون أن يؤدي ذلك إلى إزالتها تماما، وهو ذات ما نصت عليه أغلب التشريعات التي جرمت الإتلاف المعلوماتي.

ج- فعل التعديل غير مشروعك

يعد التعديل بشكل غير مشروع لملومات وبيانات التوقيع والمحررات الوسائط الالكترونية صورة من صور الركن المادي لجريمة الإتلاف في مجال التوقيع الالكتروني وقد يعرف بأنه "كل تغيير غير مشروع للمعلومات والبرامج باستخدام إحدى وظائف الحاسب الآلي"[2].

فالتعديل يتمثل في تغيير حالة المعلومات الموجودة داخل النظام المعلوماتي بشكل يؤدي إلى تبديلها، بغض النظر عن الطريقة التي يقع بها، الأمر الذي يقتضي حظر قيام الغير بتعديل المعلومات بأي شكل كان، لذا نرى أن غالبية الدول التي جرمت تشريعاتها الإتلاف المعلوماتي جرمت أشكال التعديل وإن اختلفت فيما بينها في تحديد هذا التعديل[3].

د- فعل تدمير نظم معلومات التوقيع الالكتروني والمحررات الالكترونية.

هذه الصورة أشد من إجراء التعديل على المعلومات إذ أنها تقم المعلومات الخاصة بالتوقيع والمحررات الالكترونية تمام وتتم عن طريق ما يسمى بالفيروسات حيث يعرف الفيروس على أنه "مرض يصيب الجهاز وهو عبارة عن برنامج صغير يمكن تسجيله أو زراعته على الاسطوانات المرنة أو الأقراص الصلبة الخاصة بالحاسب ويظل هذا الفيروس خاملا خلال فترة محدودة ثم ينشط فجأة في توقيت معين

[1]- هلالي عبد الله أحمد، جرائم المعلوماتية التقليدية والمستحدثة وتطبيقها في النظام البحريني، دار النهضة العربية، القاهرة، 2013، ص 257.

[2]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 316-317.

[3]- دلخار صلاح بوتاني، مرجع سابق، ص 261.

ليدمر البرامج والمعلومات المسجلة في الحاسب، الأمر الذي يؤدي إلى إتلاف المعلومات أو حذفها أو تدميرها[1].

والحقيقة أن أغلب النصوص التشريعية لم ترق بعد إلى الحد الذي يجرم هذه الأعمال وحيازة وإعداد البرامج والأنظمة الخاصة بإعداد الفيروسات والبرامج الخبيثة والمدمرة والتي تؤدي إلى إتلاف الأجهزة والبرامج.

ومما سبق يتضح لنا أن إنشاء الفيروسات يؤثر على أنظمة المعلومات، فالمعلومة هي المادة الخام للبرامج وقواعد البيانات، ومتى ما صيغت بأسلوب إبداعي فيه ابتكار في الأنشطة الصناعية أو التجارية فإنه يدخل في نطاق الحماية القانونية، والفيروسات تشكل في حد ذاتها اعتداءا على البرامج والقواعد والبيانات وأنظمة المعلومات، لكونها تعمل على تخريب وتعطيل هذه البرامج والاعتداء عليها[2].

ثالثا: الركن المعنوي لجريمة إتلاف التوقيع الالكتروني.

جريمة إتلاف التوقيعات والمعلومات والمحررات والوسائط الالكترونية هي جريمة عمدية تتطلب القصد العام[3] والذي يقوم على توافر عنصري العلم والإرادة وانصراف كليهما إلى العناصر كافة التي يتكون منها الركن المادي للجريمة، وفي جريمة الإتلاف المعلوماتي ينبغي أن ينصرف علم الجاني إلى أنه يقوم بإدخال أو تعديل أو محو المعلومات أو من له السيطرة عليها، وأن من شأن نشاطه هذا يؤدي إلى نتيجة هي تغيير حالة المعلومات، ومن ثم تته إرادته إلى هذا النشاط وتلك النتيجة[4].

غير أن بعض التشريعات تتطلب أن تتجه إرادة الجاني لتحقيق قصد خاص ومثال ذلك قانون لوكسمبورغ الذي تبنى النص الفرنسي القديم الذي كان يتطلب قصدا خاصا يتمثل في ارتكاب الفعل دون مراعاة لحقوق الآخرين أي أن تتجه إرادة المتهم إلى تحقيق قصد خاص كقصد الإضرار بالغير أو قصد تحقيق ربح مادي غير مشروع للجاني، أو للغير كما في القانون البرتغالي والفنلندي.

كما يضاف إلى ما تقدم أن جريمة الإتلاف المعلوماتي قد تقع بطريق الخطأ غير العمدي أي بدون أن يتوافر قصد الإتلاف، فقانون العقوبات الفرنسي الجديد يعاقب على تعديل المعلومات أو محوها إذ تم بطريق الخطأ وهو ما أشار إليه في المادة 1/223 ضمن جريمة الدخول أو البقاء بدون تصريح في النظام

[1]- محسن محمد العبودي، كارثة فيروسات الكمبيوتر والجرائم المتعلقة بالانترنت، بحث منشور على شبكة الانترنت www.arabla.winfo.com يوم 16أفريل على الساعة 13:00

[2]- محمد عبيد الكعبي، مرجع سابق، ص 529.

[3]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 325.

[4]- دلخار صلاح بوتاني، مرجع سابق، ص 264.

المعلوماتي حيث تستند العقوبة إذا ما ترتب على هذا الدخول أو البقاء تعديل أو محو للمعلومات الموجودة داخل النظام، ذلك أن الركن المعنوي في الجرائم التي تتجاوز قصد الجاني يكون مزدوج التكوين، فهو يقوم على القصد الجنائي متجها إلى النتيجة الأقل جسامة وعلى الخطأ توافر النتيجة الأشد جسامة، وتبعا لذلك يمكن القول أن الركن المعنوي في جريمة الدخول أو البقاء بدون تصريح يكون مزدوج التكوين فعمل الدخول أو البقاء بدون تصريح يكون عمديا، في حين أن إتلاف المعلومات المترتب على هذا الدخول يكون مبنيا على الخطأ[1].

رابعا: موقف القوانين العقابية من جريمة الإتلاف المعلوماتي:

لقد ولت التشريعات العربية أو الأجنبية عناية كبيرة بالمكونات المنطقية للأنظمة الالكترونية وما تشمله من برامج ومعلومات وبيانات نظرا لما لها من قيمة اقتصادية كبيرة خاصة في عصر عرف بكونه عصر المعلوماتية وتمثل هذا الاهتمام بصفة خاصة في تجريم جريمة الإتلاف المعلوماتي التي تعد إحدى الجرائم المعلوماتية المستحدثة، وتبعا لذلك سوف نقسم هذه النقطة إلى قسمين.

أ- موقف بعض القوانين العقابية العربية:

اهتمام المشرع العربي بجريمة الإتلاف الالكتروني لم يكن بذاته المستوى الموجود لدى المشرع الغربي، فأغلب الدول العربية لم تحرك ساكنا لمواجهة هذا النوع المستحدث من الجرائم وإنما اعتمدت على النصوص القائمة المنصوص عليها في مدونتها العقابية، ومع ذلك قامت بعض الدول العربية باستحداث نصوص خاصة بهذه الجرائم والأمثلة التالية توضح ذلك:

ففي مصر نجد أنالمشرع المصري جرّم الإتلاف ولكن وفقا للمفهوم التقليدي له، فالمادة 361 من قانون العقوبات تنص "كل من خرّب أو أتلف عمدا أموالا ثابتة أو منقول لا يمتلكها أو جعلها غير صالحة للاستعمال أو عطلها بأية طريقة يعاقب بالحبس مدة لا تزيد عن ستة أشهر وبغرامة لا تتجاوز ثلاثمائة جنيه أو بإحدى هاتين العقوبتين".

أما بالنسبة للإتلاف الالكتروني الواقع على المكونات المنطقية للأجهزة والأنظمة الالكترونية فلا يوجد نص خاص كذلك الموجود في التشريع الأمريكي والفرنسي أو في التشريع العماني باستثناء بعض النصوص الواردة في القانون رقم 143 لسنة 1994 بشأن الأحوال المدنية والتي يقتصر تطبيقها بصريح النص الفقهي حول استحداث نصوص جديدة تتلائم مع التطور التقني في تكنولوجيا المعلومات وشبكة

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 266.

الاتصال، كما تجدر الإشارة أن هناك مشروع قائم في مصر يتناول دراسة الجرائم المتصلة بعالم التقنية الحديثة[1].

ففي السعودية نجد أن المشرع السعودي ساير الاتجاه الحديث الذي ينقضي بضرورة اتجاه نص خاص للعقاب على إتلاف المعلومات والبرامج وعدم ترك المسألة للقواعد العامة التي يختلف فيها الرأي حول ما إذا كانت نصوص تجريم الإتلاف التقليدية تسري على الإتلاف المعلوماتي أم لا، حيث تنص الفقرة الثانية من المادة الخامسة من النظام السعودي رقم 17 لسنة 2007 "يعاقب... على إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدميرها أو مسح البرامج أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها أو إتلافها أو تعديلها" حيث تقع هذه الجريمة بتوافر ركنيها المادي والمعنوي، فهي من جرائم النتيجة وليس جرائم السلوك، فلا تقوم إلا بتحقق النتيجة وهي تدمير أو مسح أو حذف أو تسريب أو إتلاف أو تعديل البرامج والبيانات الموجودة أو المستخدمة في الشبكة المعلوماتية ويمكن أن يتحقق النشاط الإجرامي المكون لهذه الجريمة باستعمال الجاني برامج خبيثة.

ففي دولة الامارات وباستقراء ما نصت عليه الفقرة 02 من المادة 02 من قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 02 لسنة 2006 "من أنه "إذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس لمدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين" نجد أن المشرع الإماراتي قد جعل محل اعتداء المعلومات أيا كان أسلوب احتوائها محتوى حاسب آلي أو دعامة أو وسيط أو غيرها كما أضافت فعل إلغاء أو حذف المعلومات وهو ما يرادف فعل المحو أو الإتلاف لتطابقها في النتيجة إعدام المعلومات[2].

كما شدد المشرع العقوبة في البند 03 من هذه المادة متى كانت البيانات أو المعلومات محل الاعتداء شخصية وشدد العقوبة أيضا متى ارتكبت الجريمة أثناء أو بسبب أداء العمل أو تسهيل ذلك للغير في المادة 03 من ذات القانون والتي تنص على أنه "كل من ارتكب أيا من الجرائم المنصوص عليها في البند 02 من المادة 02 من هذا القانون، أثناء أو بسبب تأدية عمله أو سهل للغير ذلك يعاقب بالحبس لمدة لا تقل عن سنة والغرامة التي لا تقل عن عشرين ألف درهم أو بإحدى هاتين العقوبتين".

[1]- يوسف بن سعيد الكلباني، مرجع سابق، ص 183.

[2]- محمود عمر محمود، المسؤولية الجنائية الناشئة عن جرائم المحمول، دراسة مقارنة بين القانون الوضعي والشريعة الإسلامية، رسالة دكتوراه، جامعة عين شمس، القاهرة، مصر، 2003، ص 122.

كما جرم هذا القانون إدخال ما من شأنه أن يؤدي إلى تدمير أو مسح أو حذف أو إتلاف أو تعديل الملومات أو البرامج أو البيانات بواسطة الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات وذلك في المادة 02 والتي تنص "كل من ادخل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات فيها يعاقب بالسجن المؤقت وبالغرامة التي لا تقل عن خمسين ألف درهم أو بإحدى هاتين العقوبتين" فالواضح أن هذه المادة تعاقب على الإتلاف المعلوماتي الذي ينشأ عن إدخال البرامج الخبيثة كالفيروسات والقنابل والدود وغيرها.

أما في التشريع الجزائري ووفق التعديل الذي أجراه المشرع على قانون العقوبات، أصبحت المادة 394 مكرر 01 تنص على "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500000دج إلى 2000000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

ومن الواضح تأثر المشرع الجزائري بالمشرع الفرنسي، فهذه المادة تعد ترديدا لما أورده المشرع الفرنسي في المادة 3/323 عقوبات فرنسي جديد مع اختلاف بسيط في العقوبة المقررة.

فالنشاط الإجرامي المكون للركن المادي لهذه الجريمة يتحقق وفق القانونين بإتيان أفعال الإدخال والمحو والتعديل، ولا يشترط اجتماعها معا إذ يكفي وقوع واحدة منها[1].

فالبرنامج الجديد الذي يتم إدخاله قد يكون برنامجا وهميا يهدف إلى التسوية والتظليل في ارتكاب الجريمة، أو قد يتم إدخال بيانات أو معلومات جديدة وهو ما عده المشرع الجزائري أهم المراحل في الجريمة المعلوماتية، كونها تمهد لمرحلة أخطر وهي مرحلة استغلال المعلومات، كما اعتبر المشرع الجزائري إزالة أو تعديل المعلومات التي يتضمنها النظام المعلوماتي بطريق الغش عملا مجرما أيضا، فلا يقتصر الأمر على إدخال معلومات أو برامج جديدة، بل يشمل تعمد إزالة أو تعديل البيانات أو المعلومات المخزنة إتلافها أو محوها سواء كان كليا أو جزئيا ولا يشترط المشرع أن يكون مرتكب فعل الإدخال أو المحو أو التعديل قد دخل إلى النظام بدون تصريح، ذلك أن فعل الدخول بدون تصريح يعد مجرما وحده[2].

ولا يشترط المشرع أن تكون المعطيات محل الاعتداء داخل نظام المعالجة الآلية أو أن تكون قد تمت معالجتها، فحسب المادة 394 مكرر02 يستوي أن يكون محل الجريمة معلومات مخزنة في أشرطة أو

[1]- خيثر مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى، عين مليلة، الجزائر، 2012، ص 123.

[2]- دلخار صلاح بوتاني، مرجع سابق، ص 274.

أقراص أو معالجة آليا أو مرسلة عن طريق منظومة أو شبكة معلوماتية، طالما يمكن أن تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من هذا القانون[1].

وينبغي القول هنا: أن المشرع الجزائري قد شدد العقوبة بحيث تصبح مضاعفة في حالة ما إذا استهدفت هذه الجريمة الدفاع الوطني أو والهيئات والمؤسسات الخاضعة للقانون العام وذلك وفق المادة 394 مكرر 03 التي تنص "تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد".

ب-موقف بعض القوانين العقابية الغربية:

لقد أولى المشرع الأجنبي اهتمام كبيرا لتجريم الأفعال التي م شانها أن تسبب إتلافا معلوماتيا، وذلك إما باستحداث نصوص ضمن التشريعات الخاصة بجرائم المعلوماتية أو بتعديل نصوص قانون العقوبات فيها بما يلاءم تطبيقها على إتلاف أشياء ذات طبيعة غير مادية أي معلومات.

ففي الولايات المتحدة الأمريكيةلم يحتو التشريع الفدرالي لجرائم الحاسب الآلي الصادر عام 1984م على ما شانه تجريم إتلاف المعلومات والبرامج بصورة عامة، وإنما اقتصر التجريم فقط على إتلاف المعلومات والبرامج بصورة عامة وإنما اقتصر التجريم فقط على الإتلاف الذي يترتب عليه إعاقة أنظمة الحاسبات الآلية عن العمل حيث جرمت الفقرة الثانية من المادة a/1030 من التشريع الفدرالي الأمريكي إتلاف المعلومات الذي يترتب عليه إعاقة الحكومة عن استعمال أنظمة الحاسبات الآلية، إلا انه ونتيجة لكثرة الانتقادات التي وجهت إلى هذا التشريع تم تعديله بحيث أصبحت الفقرة الثالثة من المادة a/1030 تتناول فقط الدخول غير المصرح به إلى حاسب آلي تستعمله الحكومة متى أعاق الدخول هذا الاستعمال، وأضيفت فقرة خامسة إلى ذات المادة جرّمت الإتلاف العمدي غير المصرح به لمعلومات يحتويها حاسب آلي تابع لحكومة الولايات المتحدة وإدارتها أو حاسب آلي غير تابع للحكومة، إلا انه يتم استخدامه من قبلها أو لصالحها، والهدف من هذه الفقرة السابقة هو حماية البيانات والمعلومات وأنظمة الحسابات الآلية من أعمال الإتلاف التي ترتكب بواسطة أشخاص غير مصرح لهم الدخول إلى النظام[2].

وفي عام 1996 صدر قانون حماية بنية المعلومات القومية وبصورة عدلت المادة a/1030 حيث تم التوسيع من نطاق حماية أنظمة الحسابات الآلية، حيث لم تعد الحماية قاصرة على الحسابات الآلية

[1]- سويسر سفيان، جرائم المعلوماتية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2010، ص 95.

[2]- يوسف بن سعيد الكلباني، مرجع سابق، ص 174.

التابعة للحكومة وإدارتها أو التي تستخدم من قبلها أو لصالحها وإنما اتسعت الحماية لتشمل جميع الحسابات التي يتم استخدامها من قبل المؤسسات الاقتصادية التابعة لكومة الولايات الأمريكية فيما بينها أو بين الولايات الأمريكية والدول الأخرى، وهو ما أطلق عليه الحاسبات الآلية التي تتمتع بالحماية، كما امتد النص ليشمل أعمال الإتلاف التي تقع من أشخاص مصرح لهم بالدخول إلى النظام متى ما تم ذلك عمدا.

ومن أهم ما أتت به المادة a/1030 يعد تعديلها تجريم الإتلاف المعلوماتي فالبند الأول من الفقرة الخامسة ينص على "تعديل المعلومات والبرامج والشفرات والأوامر داخل أنظمة الحاسبات الآلية مما يترتب عليه أضرار وتلحق بحاسب آلي يتمتع بالحماية متى ما كان إحداث الضرر قد تم عمدا والفعل الإجرامي هنا يعد جناية[1].

أما فرنسا تعتبر من أوائل الدول الغربية التي سارعت إلى إصدار تشريعات خاصة بحماية النظم المعلوماتية والتصدي لبعض صور الجرائم المستحدثة والتي تقع بسبب التقدم في استخدام الحاسب الآلي وكذلك الشبكة العالمية للمعلومات أو بعض الشبكات المحلية كما هو الحال في شبكة المانتيل الفرنسية.

ويعد القانون رقم 17-78 الصادر في السادس من يناير 1978 بشأن الحريات والمعلومات هو اللبنة الأساسية لتنظيم وحماية النظم المعلوماتية في فرنسا، حيث عالج المشرع من خلاله مسألة تخزين البيانات من الحاسب الآلي وبيان لأنواعها المختلفة ومد التخزين كذلك الجهة المختصة بالرقابة والإشراف على أعمال ذلك القانون.

ومن أهم ما جاء به هذا القانون فيما يتعلق بالإتلاف المعلوماتي نص المادة 1/323 والخاصة بجريمة الدخول غير المشروع على أنظمة الحاسب الآلي، حيث اعتبر الإتلاف الواقع على المعطيات الموجودة داخل النظام ظرفا مشددا لجريمة الدخول غير المشروع متى كان الإتلاف بسبب هذه الجريمة الأخيرة وهناك أيضا المادة 3/323 التي جرّمت إدخال البيانات بطريقة غير مشروعة في نظام معالجة البيانات أو إلغاء أو تعديل البيانات التي يحتوي عليها النظام بطريقة غير مشروعة[2].

[1]- أيمن عبد الحفيظ عبد الحميد سليمان، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة القاهرة، 2010، ص 15-16.

[2]- تنص المادة 323-1 "على الدخول أو البقاء –بطريق الغش- داخل كل أو جزء من نظام المعالجة الآلية يعاقب عليه بالحبس لمدة سنة وغرامة مقدارها 10000 يورو، وإذا نجم عن هذا الدخول محو أو تعديل في المعطيات المخزنة في النظام أو إتلاف تشغيل هذا النظام تكون العقوبة الحبس لمدة سنتين وغرامة مقدارها 30000 يورو".

الفرع الثاني: جريمة تزوير التوقيع الالكتروني.

تشهد جريمة تزوير التوقيع الالكتروني، بوصفها إحدى صور الغش المعلوماتي تزايدا ملحوظا، وذلك تماشيا مع حلول الدعامات المعلوماتية محل المحررات التقليدية كأوراق، مستندات ودفاتر في جميع المجالات، نظرا إلى ما تمتاز به من سعة تخزينية وحسن تبويب المعلومات المخزنة وسرعة استرجاعها، الأمر الذي دفع البعض إلى القول أن جريمة تزوير التوقيع الالكتروني هي من أخطر جرائم الغش المعلوماتي[1] وقد عالجت التشريعات والقوانين في دول العالم المختلفة حتى الشريعة الإسلامية، كافة أشكال جريمة التزوير في المحررات التقليدية، لكنها انقسمت اتجاه التزوير الذي يقع في مجال المعلوماتية، حيث يرى فريق من الفقه عدم إمكانية تطبيق النصوص التقليدية على جرائم التزوير المعلوماتي، ولابد من تشريع نصوص خاصة بجرائم التزوير التي تقع في مجال المعلوماتية، ومن خلال ما تقدم سنحاول أن تلتقي البحث على مفهوم التزوير بصفة عامة والتطرق إلى جريمة تزوير التوقيع الالكتروني بصفة خاصة.

أولا: تعريف جريمة التزوير:

يعرف التزوير الالكتروني بأنه: "أي تغيير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة أو كانت مرسومة عن طريق الراسم ويستوي في المحرر الالكتروني أن يكون مدونا باللغة العربي أو لغة أخرى لها دلالتها، كذلك قد يتم في مخرجات لا ورقية شرط أن تكون محفوظة على دعامة كبرنامج منسوخ على اسطوانة وشرط أن يكون المحرر الالكتروني ذا أثر في إثبات حق أو اثر قانوني معين"[2].

"والتزوير في المحررات هو: "تغيير في الحقيقة في محرر بإحدى الطرق التي نص عليها القانون تغيير من شانه إحداث ضرر مقترن بنية استعمال المزور فيما أعد له.

كما يعرف التزوير بأنه: "إدخال تغيير بالإضافة أو الحذف أو التعديل على شيء صحيح في القانون".

كما قيل أنه: " تغيير الحقيقة بقصد الغش بإحدى الطرق المقررة بالقانون في محرر يحميه القانون"[3].

وعلى الرغم من أن أغالب التشريعات الجنائية تنتهج سياسة الابتعاد عن إيراد التعريفات

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 155.

[2]-عبد الحليم فؤاد الفقهي، جريمة تزوير التوقيع الالكتروني، دار النهضة العربية، القاهرة، 2016، ص 79.

[3]- رؤوف عبيد، جرائم التزييف والتزوير في القانون المصري، مطابع دار الكتاب العربي، القاهرة، مصر، 2007، ص 32.

وخلافا للتعريفات الفقهية السابقة نجد أن التشريع المصري لم يعرف التزوير في المحررات ولم يوضح أركان الجريمة، وغنما وضع الطرق التي يقع بها التزوير والعقاب عليها، بينما اتجه المشرع الفرنسي في القانون الجديد اتجاها مختلفا حيث عرفه في المادة 1/441 بأنه: "تغيير في الحقيقة المنطوي على غش ومن شأنه إحداث ضرر إذا ارتكب بأية وسيلة في محرر أو في أي دعامة تعبر عن فكرة موضوعها أو يمكن أن يكون موضوعها إقامة الدليل على حق أو واقعة ذات آثار قانونية"[1].

أماالتشريع العراقي عرف التزوير في المادة 268 من قانون العقوبات العراقي والتي تنص على "التزوير هو تغيير الحقيقة بقصد الغش في سند أو وثيقة أو أي محرر آخر بإحدى الطرق المادية والمعنوية التي بينها القانون، تغييرا من شأنه إحداث ضرر بالمصلحة العامة بشخص من الأشخاص".

وعرفها المشرع اللبناني في المادة 453 من قانون العقوبات اللبناني لسنة 1943 وتعديلاته التي نصت على أن "التزوير هو تحريف متعهد للحقيقة في الواقع أو البيانات التي يثبتها صك أو مخطوط بشكل مستندا بدافع إحداث ضرر مادي أو معنوي أو اجتماعي"[2].

وتجدر الإشارة إلى أنه على الرغم من اختلاف العبارات في التعاريف السابقة إلا أنها تلتقي في المضمون والمتمثل في تعيير للحقيقة ينص على المحرر، وأن تتم بإحدى الطرق المحددة قانونا، وأن يكون من شأنه التسبب بضرر.

ثانيا: أركان جريمة تزوير التوقيع الالكتروني.

تعتبر جريمة تزوير توقيع أو وسيط الكتروني من جرائم الضرر، ويتكون ركنها المادي من الفعل الإجرامي، النتيجة الإجرامية علاقة سببية.

وسنتناول قواعد الركن المادي للجريمة، وذلك على النحو التالي:

أ- الركن المادي في جريمة تزوير التوقيع الالكتروني:

لقيام الركن المادي في جريمة التزوير لابد من توافر العناصر التالية:

1- تغيير الحقيقة:

يقوم الركن المادي في جريمة تزوير التوقيع الالكتروني على تغيير الحقيقة، ومدلول تغيير الحقيقة يعني إبدالها بما يغايرها، وبالتالي فتغير الحقيقة هو الأساس الذي تقوم عليه جريمة التزوير وبالتالي إذا

[1]-حسام محمد نبيل الشنراقي، مرجع سابق، ص 233.

[2]- دلخار صلاح بوتاني، مرجع سابق، ص 157.

انتفى هذا العنصر فلا تقوم جريمة التزوير، وحيث أن التوقيع الالكتروني جزءا لا يتجزأ من المحرر الالكتروني فإن وقوع التزوير فيه أمرا مقصورا وذلك بتغيير الحقيقة على الشرائط أو المستندات التي تمثل مخرجات الحاسب الآلي، طالما هذا التغيير قد طال البيانات الموجودة في جهاز الحاسب الآلي شرط حصول الضرر الذي يتمثل في اهتزاز الثقة في المحررات[1].

ب-استعمال إحدى الطرق المحددة قانونا:

يقصد بطرق التزوير تلك الوسائل التي يتم بها تغيير الحقيقة، حيث لا يكفي لقيام جريمة التزوير أن يتم تغيير الحقيقة في محور بل ينبغي أن يكون هذا التغيير قد تم بطريقة من الطرق التي حددها القانون وهي تندرج تحت نوعين من التزوير وهما: التزوير المادي وهو تغيير للحقيقة في محرر بطريقة مادية، والتزوير المعنوي فهو تغيير الحقيقة بطريقة غير مادية ويتمثل في تغيير معنى المحرر ومضمونه أو أن تمس مادته أو شكله وهذا ما سيتم بيانه كالنحو التالي:

1- التزوير المادي:

لقد حددت الشريعة المقارنة كأمل عام عدة طرق لتزوير المادي وسنتناول البعض منها.

– وضع إمضاءات وأختام وبصمات مزورة:

في ظل الأحكام القضائية في هذا الشأن نرى من بين إمكان تحقق هذه الطريقة في المحررات الالكترونية وذلك بقيام شحن بتزوير توقيع الكتروني موضوع على محرر الكتروني ويكون ذلك بوضع اسم المزور على المحرك الالكتروني حتى ولو لم ينطوي على توقيع الكتروني في الأصل، ذلك وضع التوقيع الالكتروني المزور على محرر الكتروني هو الطريقة المتوقعة للتزوير المادي في محرر الكتروني لعدم إمكان تحقق ذلك بوضع أختام مزورة، وإن كان الغالب أن يكون التوقيع الالكتروني مؤمنا بمفتاحين مشفرين عام وخاص[2]، أما ختم المزور فيكفي وضع ختم شخص على المحرر، وهدفه نسبة المحرر لصاحب الختم.

أما البصمة المزورة فهي تأخذ حكم الإمضاء، إذ نصت المادة 225 من قانون العقوبات المصري، على أن: "تعتبر بصمة الإصبع كإمضاء في تطبيق أحكام هذا الباب" ويقصد بذلك الباب السادس المتعلق

[1]- راشد بن محمد البلوشي، مرجع سابق، ص 95.

[2]- أحمد عصام عجيلة، مرجع سابق، ص 193.

بالتزوير، ومضمون ذلك أن البصمة هي بديل الإمضاء لشخص لا يستطيع التوقيع وهي دليل على شخصية صاحبها[1].

- **وضع أسماء أو صور أشخاص آخرين مزورة.**

أما هذه الطريقة فهي تتحقق باستخدام الوسائل العديدة في معالجة البيانات الخاصة بالمحررات والتوقيعات الالكترونية عندما يقوم المزور بالدخول إلى موقع المحرر أو التوقيع والوسيط الالكتروني، وإلى نظام المعلومات، ثم يضع أسماء أشخاص لا صلة لهم ويترتب على ذلك خلق وضع قانوني ضار بهم ثم يتم إخراج هذه البيانات على دعامة مادية ورق، وذلك سواء من موظف بالمؤسسة التي تتعامل مع نظام المعلومات الخاص بالتوقيع الالكتروني، أو شخص من الغير متسلل للنظام حيث يقوم بتغيير الحقيقة في تلك المحررات أو الوسائط ويترتب عليها تغير في بيانات ومعلومات التوقيع الالكتروني، كما يتحقق ذلك أيضا بوضع صورة شخص مكان صورة شخص آخر في محرر الكتروني[2].

- **التقليد:**

ويقصد به إنشاء محرر الكتروني بكامل أجزائه على غرار محرر الكتروني آخر موجود صحيح، أي إنشاء محرر الكتروني ابتداء أو جزء منه شبيه المحرر الالكتروني الصحيح في الأصل، وهو يتحقق بتقليد محرر الكتروني بالمحاكاة لمحرر الكتروني صحيح أو بتقليد ختم أو علامة وقد ينص على محرر الكتروني بأكمله، أو على عبارة أو كلمة فيه[3].

- **الاصطناع:**

تتمثل هذه الطريقة من طرق التزوير المادي في خلق محرر بأكمله ونسبته إلى غير محرره، أو كما قالت محكمة النقض المصرية في هذا الشأن: أن الاصطناع هو إنشاء محرر بكامل أجزائه على غرار أصل موجود، أو خلق المحرر على غير مثال سابق[4].

---

[1]- محمد عبيد الكعبي، مرجع سابق، ص 536.

[2]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 261.

[3]- أحمد عصام عجيلة، مرجع سابق، ص 195.

[4]- محمد عبيد الكعبي، مرجع سابق، ص 556.

2- التزوير المعنوي:

وهذا النوع من التزوير المعلوماتي يؤدي إلى تغيير مضمون المحرر وظروفه وملابساته وليس في شكله لذا فهو يحدث عند إنشاء المحرر ولا يترك أثر ظاهر، وقد يقع التزوير المعنوي في المحررات الالكترونية بذات الطرق التي يقع بها التزوير المعنوي في المحررات العادية وهي:

- تغيير إقرار أولي الشأن:

وفي هذه الحالة يقوم الجاني بتسجيل بيانات لم تصدر من أولي الشأن إثباتها في المحرر الالكتروني فيعمد إلى تغيير الحقيقة في البيانات التي يطلب أولي الشأن إثباتها في محرر الكتروني وقد تكون في محرر الكتروني رسمي وفيها يكون الفاعل موظف عام، كما لو قام الموظف المعهود إليه بكتابة البيانات في محرر الكتروني داخل منظومة حكومة الكترونية في أي موقع من المواقع بتدوين بيانات مغايرة للحقيقة غير التي أدلى بها أولي الشأن[1].

- جعل واقعة غير معترف بها في صورة واقعة معترف بها[2]

3- ركن الضرر:

لا يعد تغيير الحقيقة تزوير إلا إذا نشأ عنه ضرر أو كان من شأنه إحداث ضرر، فلا يكفي تغيير الحقيقة في محرر بإحدى الطرق المحددة قانونا وإنما لابد من أن يكون من شأنه إحداث ضرر بالغير فانعدام الضرر يعني انعدام جريمة التزوير، والضرر بشكل عام هو: "الأذى الذي يصيب المتضرر في حق من حقوقه أو في مصلحة من مصالحه" والضرر قد يكون ماديا يصيب المجني عليه في ذمته المالية أو معنويا وهو الذي ينال من شرف وكرامة واعتبار إنسان أو جماعة، ولا يشترط أن يكون الضرر حالا أي يتحقق فعلا فيكفي أن يكون الضرر محتملا وقوعه فالعبرة في تقدير احتمال حدوث الضرر من التزوير نكون بالوقت الذي وقع فيه تغيير الحقيقة في المحرر باعتباره وقت تمام الجريمة، ولم يضع القانون ضابطا للضرر، لذا فإن التحقق من وجوده أو احتمال وجوده أو انتفائه مسألة موضوعية متروكة لتقدير محكمة الموضوع التي هي ملزمة بتوضيح توافر الضرر في حكمها[3].

---

[1]- أحمد عصام عجيلة، مرجع سابق، ص 196.

[2]- ويقصد بها: "كل إثبات لواقعة غير الحقيقية" ولذا يعد أي تشويه أو تحريف يدخله كاتب المحرر على ما يثبته به عند تدوينه هو جعل واقعة مزورة في صورة واقعة صحيحة، وتعد هذه الطريقة الأكثر انتشارا أو الأوسع نطاقا حيث تشمل الطريقة الأولى والثالثة طالما أن هذه الطريقة تعني كل إثبات لواقعة في محرر يغاير حقيقتها، وتتم هذه الطريقة في المحررات الرسمية والعرفية.

[3]- دلخار صلاح بوتاني، مرجع سابق، ص 165.

ب-الركن المعنوي في جريمة تزوير توقيع الكتروني:

يتمثل الركن المعنوي في جريمة التزوير في القصد الجنائي وهو تعمد تغيير الحقيقة في محرر تغير من شانه أن يسبب ضررا ونية استعمال المحرر فيما غيرت الحقيقة من أجله.

والتزوير جريمة عمدية تتطلب قصد جنائي عام أي أن يعلم الجاني أنه يقوم بتغيير حقيقة المحرر الالكتروني من خلال وضع توقيع الكتروني مزور وأن تزوير هذا التوقيع من شانه أن يرتب ضررا، وان الفعل الذي ارتكبه هو فعل غير مشروع، أي أن الجاني عالما بأن الفعل الذي ارتكبه يشكل جريمة يعاقب عليها القانون.

وتأتي الإرادة في مرحلة لاحقة لمرحلة العلم وهي عبارة عن إرادة العقل أو السلوك المكون للجريمة وإرادة النتيجة التي تتمثل في الاعتداء على الحق أو المصلحة التي يحميها قانون العقوبات.

ولا يكفي لقيام الركن المعنوي في التزوير توافر القصد الجنائي العام وإنما يتعين فقط عن ذلك أن يتوافر لدى الجاني القصد الخاص وهو نية استعمال المحرر فيما زور من اجله، فإذا انتفت نية استعمال التوقيع الالكتروني المزور فيما زور من أجله فحينئذ ينتفي القصد الخاص كما ينتفي استعماله[1].

ثالثا: موقف التشريعات العقابية من جريمة تزوير المحررات المعلوماتية.

من أجل مواجهة الجرائم المستحدثة ومعالجة القصور في النصوص العقابية التقليدية، وبهدف مد حماية جنائية للمعلوماتية من هذه الجرائم وخاصة جريمة تزوير المحررات المعلوماتية وخاصة جريمة تزوير التوقيع الالكتروني، عمد المشرع في العديد من الدول إلى استحداث صور تجريمية أو إدخال تعديلات على النصوص القائمة في حين سكت البعض الآخر عن مواجهتها وعليه سيبحث في موقف التشريعات المقارنة من هذه الجريمة.

أ- موقف بعض التشريعات العقابية العربية:

لقد اصدر المشرع المصري قانون رقم15 سنة2014 الخاص بتنظيم التوقيع الإلكتروني وفيه اعتقد المشرع المصري بحجية المحرر الإلكتروني في مادة 15 من قانون السالف الذكر كما نص في المادة 23 من ذات القانون على جريمة التزوير في محرر الإلكتروني السالف يعاقب بالحسب وبغرامة لا تقل عن عشرة ألاف جنيه ولا تتجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من:

[1]- عبد الحليم فؤاد الفقي، مرجع سابق، ص 98.

-تلف أو عيب توقيعا أو وسيطا أو محرر إلكتروني أو زور شيئا من ذلك بطريق الاصطناع أو التعديل أو التحويل أو بأي طريق آخر.

-استعمل توقيعا أو وسيطا أو محررا إلكترونيا معيبا أو مزورا مع علمه بذلك ومن خلال ما سبق نستشف أن المشرع المصري قبل مرور قانون التوقيع الإلكتروني قد اعتقد بفكرة المحرر الإلكتروني، وإذ كانت غير راسخة في الأذهان بتعريفه ومدلوله الحالي، وأن فكرة السجل الإلكتروني أو البيانات الإلكترونية هي التي كانت أكثر وضوحا، لذلك تدخل المشرع وعاقب على التزوير الحامل فيها وإن كانت في الأصل محررات إلكترونية بطريقة غير مباشرة، حتى ظهرت فكرة المحرر الإلكتروني فنص المشرع على العقاب على تزوير المحرر الإلكتروني بصورة مباشرة في قانون التوقيع الإلكتروني بمفهومه الحالي[1].

فالمشرع الجزائري قد عالج جريمة التزوير في الفصل السابع من قانون العقوبات الجزائري وتناول تزوير المحررات الرسمية في القسم الثالث منه وتزوير المحررات العرفية في القسم الرابع ولم يعرف المشرع الجزائري جريمة التزوير شأنه شأن المشرع المصري بل اكتفى ببيان طرق التزوير المادية والمعنوية للمحررات الرسمية في المواد 214 و215 و216 من قانون العقوبات الجزائري ومن خلال استقرائنا لهذه النصوص نصل إلىعدم إمكان تطبيقها على تغيير حقيقة النص في المحررات المعلوماتية، كما أن المشرع الجزائري وإن سار على نهج المشرع الفرنسي بأن قام بإجراء تعديل على قانون العقوبات بهدف حماية النظام المعلوماتي ككل متكامل الكيان المادي والكيان المعنوي إلا أنه لم يتعرض إلى جميع الجرائم التي نطرق لها المشرع الفرنسي ومنها جريمة تزوير المستندات المعلوماتية والتي هي على قدر كبير من الأهمية، ومن ثم فإن المشرع الجزائري لم يكن موفقا في الإحاطة الشاملة بكل الجرائم المعلوماتية وعلى رأسها جريمة تزوير المحررات المعلوماتية سواء من خلال تعديل النصوص القائمة أسوة بنظيره الفرنسي أو استحداث أخرى جديدة[2].

ب-موقف بعض التشريعات العقابية الغربية:

أما في التشريع الفرنسي فقد أدخل المستندات المعلوماتية في نطاق الحماية الجنائية بصورة فعلية بصدور قانون الغش المعلوماتي رقم 19 سنة 1988 والذي اعتبر جريمة تزوير المحررات المعلوماتية جريمة مستقلة عن جريمة تزوير المحررات التقليدية حيث نصت الفقرة 5 من المادة 462 من هذا القانون على أنه " كل من يقوم بتزوير مستندات معالجة آليا أيا كان شكلها بما يؤدي إلى حدوث ضرر للغير

[1]- أحمد عصام عجيلة، مرجع سابق، ص 208.

[2]- دلخار صلاح بوتاني، مرجع سابق، ص 189.

يعاقب..." ويلاحظ من هذا النص انه استخدم تعبير المستندات المعالجة آليا ولم يستخدم مصطلح المحررات المعلوماتية، وبصدور قانون العقوبات الفرنسي الجديد في 1992/12/16 ودخوله حيز التنفيذ سنة 1994 ألغى المشرع نص المادة 5/462 سالفة الذكر وقام بإعادة صياغة نص جريمة التزوير الأصلية لتستوعب المحررات المعلوماتية، حيث نص المشرع الفرنسي المادة 1/441 من قانون العقوبات الجديد لتجريم التزوير في المحررات العرفية أيا كانت تقليدية أو معلوماتية، وبذلك لم يحدد المشرع الفرنسي طريقة معينة لقيام التزوير بذكره لفظ بأية وسيلة "par quelque moyen" كما أعطى النص الجديد تعريفا واسعا لمحل جريمة التزوير حيث لم يعد يقتصر فقط على المحرر بمعناه الضيق بل أصبحت الحماية تمتد إلى كل دعامة للتعبير عن التفكير والتي قد تكون على شكل معلوماتي طالما كان من شأنها أن تستخدم في إثبات الواقع أو الحق فتعبير "tout autre support" تعبير مطلق من أي قيد، وتدخل فيه بلا جدال كل الدعامات المستخدمة في المجال المعلوماتي[1].

وفي تشريع لوكسنبورغ صدر قانون التجارة الالكترونية في يونيو سنة 2000 والذي عدل نص المادة 196 من قانون العقوبات التي تجرم التزوير، فأضافت الكتابة والتوقيع الالكتروني إلى محل جريمة التزوير بصورتها التقليدية[2].

وفي التشريع الانجليزي صدر في المملكة المتحدة قانون التزوير والتزييف لسنة 1981 متضمنا وسائط التخزين في المادة 8-1 بأنه يشمل كل قرص أو شريط ممغنط أو شريط صوتي أو كل وسيلة توجد بها أو عليها بيانات مسجلة أو محفوظة بطريقة ميكانيكية أو الكتروني أو أي وسيلة أخرى، وبالتالي فإنه منذ سنة 1981 يعترف القانون الانجليزي بمحرر الكتروني وقد حكم القضاء الانجليزي بوقوع التزوير في المحررات التي تعدها أجهزة الكمبيوتر مثل التي تعمل في البنوك والشركات[3].

المبحث الثاني:الجرائم المستحدثة الماسة بالنظام المعلوماتي للتوقيع الالكتروني وبياناته

لقد تناولنا في المبحث الأول من هذا الفصل جرائم التوقيع الالكتروني التقليدية وهي جرائم الإتلاف والسرقة والاحتيال والتزوير، أما في هذا المبحث سنتناول سلوكيات إجرامية مستحدثة تتخذ من سلامة النظام المعلوماتي وسرية وسلامة المعلومات والبيانات التي تحويه موضوعا محلا ينص عليه الاعتداء وتبعا لذلك سوف نتطرق في هذا المبحث إلى عدد من الجرائم التي تنتمي إلى هذه الطائفة من الجرائم المعلوماتية

[1]- عبد القادر القهوجي، الحماية الجنائية لحاسب آلي، دار الجامع للطباعة والنشر، الإسكندرية، 2004، ص 144.

[2]- مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، مصر، 2001، ص 86.

[3]- شيماء عبد الغني عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2008، ص 75.

والتي تتخذ من النظام المعلوماتي لتوقيع الالكتروني وبياناته موضوعا لها واهما، جريمة إفساد وتعطيل النظام المعلوماتي إما في المطلب الثاني سنتعرض لجرائم الاعتداء على التوقيع الالكتروني وبياناته وشخص فرع الأول: لدراسة جرائم الاعتداء على التوقيع الالكتروني وبياناته في التشريعات المقارنة وفي الفرع الثاني، سنعرض صور الاعتداءات الواقعة على التوقيع الالكتروني وبياناته في التشريع الجزائري وبخصوص في قانون رقم 15-04 المتعلق بالتوقيع والتصديق الالكتروني

المطلب الأول: جرائم الاعتداء على النظام المعلوماتي لتوقيع الالكتروني:

إن ربط أجهزة الحاسبات الآلية مع بعضها البعض عن طريق الشبكات المعلوماتية أدى إلى سرعة انتقال المعلومات فيما بينها من جهة، وإلى سهولة التطفل عليها عن طريق الدخول إلى الحاسبات من جهة أخرى[1]. فالنظام المعلوماتي قد يتعرض إلى اختراق من قبل إفراد غير مصرح لهم بالدخول إليه أو البقاء فيه[2] وقد يتعرض إلى تعطيل وإعاقته بشكل تام أو تباطأ واضطراب في عمله مما يؤدي إلى نتائج غير صحيحة ومخالفة للحالة المعهودة لعمل النظام وهذا ما يعرف بجريمة تعطيل أو إفساد النظام المعلوماتي، وللوقوف على هذه الجرائم سنقسم هذا المطلب إلى فرعين، الفرع الأول جريمة الدخول أو البقاء بدون تصريح في النظام المعلوماتي، الفرع الثاني: جريمة إفساد وتعطيل النظام المعلوماتي.

الفرع الأول: جريمة الدخول غير المصرح به على قاعدة بيانات خاصة بالتوقيع الالكتروني

قد تتعرض الكثير من الأنظمة المعلوماتية لتوقيع الالكتروني إلى الاختراق بواسطة الكمبيوتر بدون تصريح بالقراصنة "hakers"، وتختلف الأهداف المباشرة للاختراقات، فقد تكون المعلومات هي الهدف المباشر حيث يسمى المخترق لتغيير أو سرقة أو إزالة معلومات معينة، وقد يكون الجهاز هو الهدف المباشر بغض النظر عن المعلومات المخزنة على الشبكة وسرعة انتشار الخبر حول اختراق ذلك الجهاز خاصة إذا كان يضم مواقع معروفة، فجريمة الدخول غير مصرح به على قاعدة بيانات خاصة بالتوقيع الالكتروني تعد من أهم الجرائم المعلوماتية وأكثرها انتشارا وللوقوف على ثنايا هذه الجريمة لابد من التعرض إلى مفهومها وأركانها وكذا موقف التشريعات المقارنة من تجريم هذا نوع من الجرائم الماسة بنظام المعلوماتي.

[1]- دلخار صلاح بونابي، مرجع سابق، ص 188

[2]- نهلا عبد القادر الموسني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، طبعة1، عمان، 2008، ص 158

أولا: ماهية الدخول غير المصرح به إلى النظام المعلوماتي لتوقيع الالكتروني

يقتضي تناول ماهية الدخول غير المصرح به إلى النظام المعلوماتي لتوقيع الالكتروني أن نعرض أولا لمفهوم الدخول ووسائل الاختراق والدخول غير المصرح به النظام المعلوماتي لتوقيع الالكتروني وكذا أسباب الاختراق والدخول غير المصرح به للنظام المعلوماتي لتوقيع الالكتروني.

أ- مفهوم الدخول غير المصرح به النظام المعلوماتي

ينصرف معنى مصطلح "الدخول" access في إطار المعلوماتية بصفة عامة ليشمل كافة الأفعال التي تسمح بالولوج إلى النظام المعلوماتي والإحاطة أو السيطرة على المعلومات التي يتكون منها أو الخدمات التي يقدمها[1] أو إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه، للوصول إلى المعلومات والمعطيات المخزنة بداخلها، للاطلاع عليها أو لمجرد التسلية، أو لإشباع الشعور بالنجاح في اختراق الحاسب الآلي[2].

وقد عرف المشرع السعودي الدخول في المادة الأولى من نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية بأنه "دخول شخص بطريقة معتمدة إلى حاسب آلي أو موقع الكتروني أو نظام معلوماتي أو شبكة حاسبات إلية غير معرج لذلك الشخص الدخول إليها"

إن فعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يعني الدخول بمعناه المادي، كالدخول إلى مكان أو منزل وحديقة، وفي نفس الاتجاه الدخول إلى الحاسب الآلي أو مكان وجوده، إنما يقصد بالدخول هنا كظاهرة معنوية تشبه تلك التي بغير عنها بقولها "الدخول إلى فكر أو مملكة التفكير لدى إنسان أي الدخول إلى العمليات الذهنية التي يقوم بها النظام المعلوماتي" فالدخول إلى النظام المعلوماتي يتشابه مع الدخول إلى ذاكرة إنسان.[3]

ويتحقق الدخول غير المصرح به جهاز الكمبيوتر بالوصول إلى المعلومات أو البيانات المخزنة داخل نظام الكمبيوتر والقوائم والمعدات والمكونات دون رضاء المسئول عن هذا النظام أو المعلومات التي يحتوي عليها أو بمعنى آخر إساءة استخدام الكمبيوتر ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعلومات والبيانات الموجودة بداخله لاستخدامها في غرض ما[4].

---

[1]-نائلة عادل محمد فريد قورة ، مرجع سابق، ص 242.

2-خالد ممدوح إبراهيم ،مرجع سابق ،ص 84.

[3]- دلخار صلاح بوتاني، مرجع سابق، ص 191

[4]- أحمد عصام عجيلة، مرجع سابق، ص 251

وقد جاء في نص المادة 2 من قانون الاتحاد الإماراتي رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات على أنه "كل فعل عمدي يتوصل بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به ويعاقب عليه بالحبس أو بالغرامة أو بإحدى هاتين العقوبتين"

ويلاحظ أن تحديد فكرة الدخول غير لمشروع من حيث دلالة المكان يمكن ان تعرف بأنها "التسلل في داخل النظام المعلوماتي إما الدخول من حيث الزمان فيتمثل في "تجاوز حدود التصريح أو الترخيص داخل النظام والممنوح لفترة زمنية محددة عن طريق تجاوز هذه الفترة الزمنية.

كذلك قد يتحدد مضمون الدخول من زاوية فنية بحيث قد يتم الدخول بصور مختلفة منها الاعتداء على البرامج أو البيانات أو المكونات المادية وقد يتم الدخول بواسطة الغش المعلوماتي.[1]

ب- وسائل الاختراق والدخول غير المصرح به للنظام المعلوماتي لتوقيع الالكتروني:

تختلف الوسائل التي يمكن اللجوء إليها لدخول غير المصرح به إلى النظام كمبيوتر ففي بعض الأحيان لا يتطلب الدخول أكثر من تشغيل جهاز الكمبيوتر أو فتح البرنامج الذي يقوم بتشغيله وقد يتطلب الحصول على الشفرات الخاصة بالدخول باستخدام جهاز لفك الشفرة، كما يمكن الدخول عن طريق وسائل أخرى لدخول لأنظمة الحسابات الآلية، ويستوي في ذلك أن يتم بطريقة الكترونية من خلال كلمة السر passoword أو طريقة مادية فيزيائية مثل اقتحام الملفات وسرقة الهوية الشخصية والطريقة الأولى هي الأكثر شيوعا وتستعمل من قبل الذين يسرقون كلمات السر أو يستخدمون الحاسب الآلي في إدخال كلمات سر عشوائية لحين التوصل إلى كلمة السر الصحيحة[2]

ويلاحظ أن الاختراق لا يطال أجهزة الكمبيوتر إلا إذا كانت موصولة بشبكة الانترنت التي توصل الجهاز بقراصنة الانترنت، ويعتبر من ضعف جرائم الاختراق أنشطة اقتحام أو الدخول أو التوصل غير المصرح به مع نظام الكمبيوتر أو الشبكة أما مجردا ولجهة ارتكاب فعل آخر هذا البرامج والبيانات وتخريب المعطيات والنقم والممتلكات فمن مفهوم تخريب الكمبيوتر وإيذاء الكمبيوتر وخلق البرمجيات الخبيثة[3]

[1]- خالد ممدوح إبراهيم، الحماية الجنائية لتوقيع الالكتروني، مجلة الفكر الشرطي، عدد 88 يناير 2019، ص 166

[2]- عبد الفتاح بيومي حجازي، مرجع سابق، ص 81-82

[3]- خالد ممدوح إبراهيم، مرجع سابق، ص 168

ج- أسباب الاختراق والدخول غير المصرح به لنظام المعلوماتي لتوقيع الالكتروني:

تختلف أسباب الاختراق والدخول لنظام المعلوماتي باختلاف أهداف المخترق، فقد يكون الهدف من عملية اختراق أجهزة كمبيوتر البعض أو مواقعهم على الشبكة لمجرد الفضول وقد يخترق بعض السرقة لمعلومات والبيانات، وهذا هو السبب الأبرز الذي يدفع قراصنة الانترنت إلى الدخول إلى مواقع وأجهزة كمبيوتر الغير لسرقة معلوماتهم التي قد يكونون قد عرضوها مقابل بدل مالي للاضطلاع عليها وقد يكون الاختراق في بنية المخترق فيتغير أو تحريف أو تعطيل المعلومات في أجهزة الغير وقد يكون الاختراق تزوير البيانات ومعلومات التوقيع الالكتروني وفي هذا الصدد نصت المادة 4 من قانون اتخاذ رقم 2 لسنة 2006 "بشأن مكافحة جرائم تقنية المعلومات" يعاقب بالسجن المؤقت كل من زور مستندا من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية معترف بها قانونا في نظام معلوماتي".

وقد يكون الاختراق بهدف تعطيل الأجهزة والشبكات الخاصة بتشكيل التوقيع الالكتروني حيث يتم تعطيل أجهزة الكمبيوتر عبر تعطيل برامجها، كما قد يؤدي تعطيل البرامج والشبكات عن تأدية عملها دون أن تتم عملية اختراق فعلية لتلك الأجهزة، تتم عملية تعطيل الأجهزة عن طريق إرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها، الأمر الذي يعيقها عن تأدية عملها[1].

ثانيا: أركان جريمة الدخول غير المصرح به إلى نظام التوقيع الالكتروني:

تتطلب جريمة الولوج غير القانوني للنظام المعلوماتي إلى توافر ركن مادي وركن معنوي بشقيه القصد العام والقصد الخاص، وتتناولها على نحو ما يلي:

أ- الركن المادي لجريمة الدخول غير القانوني لنظام المعلوماتي للتوقيع الالكتروني:

يعد فعل الدخول بدون تصريح إلى النظام المعلوماتي سلوكا إجراميا يتحقق به الركن المادي لهذه الجريمة[2] والذي يطلق عليه الدخول المنطقي، وذلك بغرض فح باب يؤدي إلى نظام الكمبيوتر بمكوناته المنطقية، حيث يختلف المحل الذي يتخذه الركن المادي في جريمة الدخول غير المصرح به إلى نظام مواقع ويب "web site" ويتم عادة التفرقة في هذا الخصوص بين العمليات التي تنطوي على اعتراض عمليات الاتصال من اجل الدخول إلى أحد نظم الكمبيوتر وبين الدخول إلى أحد نظم الكمبيوتر وبين الدخول

[1]- المرجع نفسه، ص 170

[2]- عبد القادر القهوجي، مرجع سابق، ص 125

المباشر إلى هذه النظم ويمكن بالنظر إلى التشريعات المختلفة التي جرمت الدخول غير المصرح به أن نميز بين ثلاث صور للمحل في جريمة الدخول غير مصرح به وهذا ما سيتم بيانه كالآتي:

ب- محل الدخول بدون تصريح إلى النظام المعلوماتي لتوقيع الالكتروني:

باستعراض التشريعات المختلفة في مجال مكافحة الجرائم المعلوماتية، والتي تناولت جريمة الدخول بدون تصريح إلى النظام المعلوماتي، نجد أنها تميز بين ثلاث صور للمحل الذي ينص عليه فعل الدخول بدون تصريح تتمثل الصور الأولى في المعلومات ذاتها والثانية في أنظمة الحسابات الآلية أما الثالثة في شبكة

1- الاتجاه الأول:

أن محل الدخول وفق هذا الاتجاه التشريعي يجمع بين الصور الثلاث التي أشرنا إليها، أي المعلومات وأنظمة الحسابات الآلية وشبكة المعلومات، فهذا الاتجاه يوسع من محل الدخول بدون تصريح، لذا أطلق عليه اسم الاتجاه الموسع ومن التشريعات التي أخذت باتجاه الموسع لمحل الدخول تصريح، التشريع الجنائي الفرنسي إذ تجرم المادة 1/323 من قانون العقوبات الفرنسي لسنة 1992" فعل الدخول أو البقاء بدون تصريح داخل نظام المعالجة الآلية بالمعنى الواسع للكلمة، وقد اجتمع الفقه في فرنسا على نظام الآلية للمعلومات وفق منظور المادة 1/323 من قانون العقوبات الفرنسي الجديد ينصرف إلى المعلومات والنظام الذي يحتوي عليها بإضافة إلى الشبكات[1].

2- الاتجاه الثاني:

وفق هذا الاتجاه فإن محل الدخول بدون تصريح بنصب على المعلومات وأنظمة الحاسبات الآلية دون شبكات المعلومات، حيث يستبعد هذا الاتجاه شبكة المعلومات عن نطاق تجريم الدخول بدون تصريح ومن أبرز التشريعات التي أخذت بهذا الاتجاه هو التشريع الانجليزي بشأن إساءة استخدام الكمبيوتر لسنة 1995 إذ تعاقب المادة الأولى منه على الدخول غير المصرح به إلى البرامج والمعلومات التي يحتوي عليها الحاسب الآلي فقد دون الإشارة إلى شبكة المعلومات[2] الأمر الذي يعني عدم شمول النص لحالات الدخول بدون تصريح التي تتم بصورة غير مباشرة عن طريق اعتراض الاتصالات المتضمنة نقل المعلومات[3].

[1]- نائلة عادل محمد فريد قورة، مرجع سابق، ص 332

[2]- خالد ممدوح إبراهيم، مرجع سابق، ص 88

[3]- دلخار صلاح بوتاني، مرجع سابق، ص 194

3- الاتجاه الثالث:

يتمثل هذا الاتجاه في تجريم الدخول بدون تصريح إلى أنظمة الحاسبات الآلية غير شبكات المعلومات ومن التشريعات التي تبنت هذا الاتجاه قانون عقوبات السويسري حيث تعاقب المادة 143 مكرر منه على الدخول بدون تصريح إلى أنظمة الحاسبات الآلية بواسطة جهاز لنقل المعلومات، وتوضح المناقشات التي دارت من خلال الأعمال التحضيرية لهذا القانون أن هذا النص لا يقصد من ورائه تجريم اعتراض وسائل الاتصال فهذا النص لا يعالج سوى حالات الدخول بدون تصريح التي تتم عن طريق أشخاص خارج المؤسسات التي تحتوي على أنظمة بواسطة شبكات الاتصال، أما الحالات التي تنطوي على دخول مباشر إلى النظام والتي تتم عادة من العاملين بالمؤسسات التي تحتوي هذه الأنظمة فلا ينطبق عليها النص ما لم يكن الدخول قد تم من خلال شبكة داخلية تابعة إلى المؤسسة.[1]

ومن خلال استعراضنا لهذه الاتجاهات الثلاثة والتي تبنتها التشريعات المختلفة من خلال نصوص تجريم الدخول بدون تصريح، فإننا نسير مع الرأي الذي يرى أن الاتجاه الأول هو الأصوب إذ ينبغي عدم التمييز بين الحالات الثلاثة للدخول بدون تصريح، وأن عملية التجريم يجب أن تطال جميعها طالما تم الدخول بدون تصريح وهو ما أكدته منظمة التعاون والتنمية الاقتصادية من خلال التوصية التي قدمتها للأعضاء في تقريرها الصادر سنة 1986 في شأن جرائم المعلوماتية، بأن تجرم قوانين العقوبات في دول الأعضاء الدخول بدون تصريح إلى الأنظمة المعلوماتية وأنظمة الاتصالات، وكذلك اعتراض نظام الاتصالات دون تصريح من المسؤول عن النظام.[2]

ج- الركن المعنوي في جريمة الدخول للنظام المعلوماتي لتوقيع الالكتروني:

يشكل الركن المعنوي أهمية في قيام جريمة الدخول غير المصرح به إلى نظام الكمبيوتر فالأفعال التي تقوم بها هذه الجريمة يقوم بها كل يوم مستخدمو الكمبيوتر، ومن بين هذه الأفعال لا يمكن تجريم سوى تلك التي يتحقق بشأنها القصد الجنائي فالركن المعنوي لجريمة الدخول غير المصرح به لنظام معلوماتي في كل التشريعات التي تناولناها يتخذ صورة القصد الجنائي، باعتبارها من الجرائم العمدية، فلكي يتوافرلهذه الجريمة ركنها المعنوي يجب أن تتحقق عناصر القصد الجنائي من علم وإرادة، وسوف نتناول فيما يأتي القصد العام المطلوب تحققه في جريمة الدخول غير المصرح به إلى نظام الكمبيوتر ثم تتعرض للقصد الخاص في هذه الجريمة.

---

[1]- نائلة عادل محمد فريد قورة، مرجع سابق، ص 337

[2]- دلخار صلاح بوتاتي، مرجع سابق، ص 195

1- القصد العام في جريمة الدخول غير المشروع لنظام المعلوماتي للموقع الالكتروني:

عبرت جميع النصوص القانونية التي تناولت جريمة الدخول غير المصرح به إلى نظام الكمبيوتر عن القصد العام المتطلب في هذه الجريمة، وذلك على الرغم من الاختلاف في العبارات المستخدمة لهذا الغرض، فقد عبر النص الفرنسي عن القصد العام يتطلبه أن يكون الدخول إلى النظام قد تم عن طريق الغش والخداع، فاستخدام هذه العبارة يعني أن الفاعل على علم بأن دخوله إلى نظام الكمبيوتر غير مصرح به[1]

وفي الدنمرك أشار النص إلى أن الفاعل يقوم بالدخول غير المصرح به إلى النظام على نحو مخالف للقانون، وفي فنلندا وسويسرا والبرتغال والو.م.أ اشترط أن يتم الدخول إلى النظام بدون تصريح وفي السويد واليونان أن يتم الدخول إلى النظام بدون وجه حق وقد تطلب القانون الانجليزي أن يتم الدخول إلى النظام على نحو غير مصرح به مع العلم بذلك، ويتطلب القصد العام يحيط علم الجانب بكل واقفة ذات أهمية قانونية في تكوين الجريمة، وكل ما يتطلبه القانون لاستكمال عناصرها، وعلم الجاني لا يقتصر نطاقه على الوقائع التي تدخل في تكوين الجريمة وإنما يتعين أن يحيط أيضا بالتكييف الذي تتصف به بعض هذه الوقائع وتكسب به أهميتها في نظر القانون[2] حيث أن عددا من الوقائع التي تقوم بها الجريمة لا تمثل أهمية في نظر القانون، إلا إذا اكتسبت وصفا معينا، فان تجردت من هذا الوصف فقد تجرت من الأهمية القانونية ولم تعد صالحة لتقوم بها الجريمة.

ويتطلب القصد الجنائي أيضا أن يتوقع الجاني حيث يأتي فعله النتيجة الإجرامية التي يوف تترتب على الفعل، فتوقع النتيجة هو الأساس النفسي الذي تقوم عليه إرادته والنتيجة التي يجب أن تتجه إليها الفاعل هي النتيجة التي يحددها القانون.

وإذا ما توفر العلم على النحو السابق، تعين بعد ذلك القول يتوافر القصد الجنائي، بحيث تتجه إرادة الجاني نحو الدخول إلى النظام غير المصرح به بالدخول إليه أي أن نتيجة إرادته إلى تحقيق هذه النتيجة.

[1]- محمد عبيد الكعبي، مرجع سابق، ص 481

[2]- محمود نجيب حسني، النظرية العامة لقصد الجنائي، دراسة تأصيلية مقارنة لركن المعنوي في الجرائم العمدية، دار النهضة العربية ، القاهرة، مصر، 1989، ص 51

2- القصد الخاص في جريمة الدخول غير مشروع لنظام المعلوماتي لتوقيع الالكتروني:

تتطلب بعض النصوص التي جرمت الدخول غير المصرح به إلى نظام الحاسب الآلي في التشريعات المختلفة قصدا خاصا إلى جانب القصد العام وقد يترتب على توافر هذا القصد تشديد العقوبة ففي الدنمرك تشدد العقوبة متى ارتكب فعل الدخول بنية الإحاطة بمعلومات تتعلق بالإسرار المتعلقة بعمل إحدى الشركات، وفي استراليا يوجد نص خاص يشدد العقوبة من ارتكب الفعل بنية الأضرار بالغير وفي النرويج تشدد العقوبة على نحو ملحوظ متى ارتكبت بنية حصول الفاعل له أو الغير على ربح غير مشروع أو إلحاق ضرر بالغير نتيجة الاطلاع على المعلومات التي يحتوي عليها النظام.[1]

أما في التشريع الجزائري فلا يبدو من نص المادة 394 مكرر أن المشرع يتطلب وجود نية خاصة لدى الجاني حتى تقوم جريمة الدخول أو البقاء غير المصرح بهما وأنه يكفي لقيامها توافر القصد العام القائم على العلم والإرادة وكذلك الشأن مع نص المادة 1/232 من قانون العقوبات الفرنسي المطابقة للمادة السابقة فهي لا تشترط قصد خاصا.[2]

ثالثا: موقف التشريعات العقابية من جريمة الدخول غير مصرح به لنظام معلوماتي:

تختلف خطة التشريعات المقارنة كما قدمنا في معالجة جريمة الدخول غير المشروع لنظام المعلوماتي، فتتفاوت من ناحية النص على الركن المادي للجريمة وفي محل الدخول غير المشروع الذي عليه نص التجريم وفي تطلب قصد خاص من عدمه، لذا فإننا سوف نعرض إلى موقف التشريعات التالية.

1- موقف التشريعات الأجنبية:

نص المشرع الفرنسي في المادة 1/232 من قانون العقوبات الجديد الصادر في 1994 على أنه "يعاقب على الدخول أو البقاء بطريق الغش داخل كل أو جزء من نظام المعالجة الآلية بالحبس لمدة سنتين وبغرامة 30000 يورو" فإذا نجم عن الدخول محو أو تعديل في البيانات أو إتلاف نظم تشغيل هذا النظام تكون العقوبة الحبس لمدة ثلاث سنوات وغرامة قدرها 45000 يورو" وتقرر المادة 3/232 من ذات القانون عقوبة بذات العقوبة المقررة للجريمة أو المقررة للجريمة الأشد في حالة المساهمة في جماعة أو الاتفاق بين مجموعة من الأشخاص للتحضير بعمل أو أعمال مادية لارتكاب جريمة أو أكثر من الجرائم السابقة وينبني على المواد السابق ذكرها، أن المادة 1/323 من قانون العقوبات الفرنسي التي تجرم الدخول غير

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص 178

[2]- محمد خليفة، مرجع سابق ،ص 167.

المصرح به إلى جميع أنظمة الحاسبات الآلية تمثل الاتجاه الموسع الذي يشمل الدخول غير المصرح به للمعلومات وعلى رأسها شبكة الانترنت، وكذلك البيانات المخزنة بطريقة الكترونية داخل النظام.[1]

ولم يحدد المشرع الفرنسي وسيلة الدخول إلى النظام، وبالتالي يجوز الدخول إلى النظام بأية وسيلة، مثل الدخول عن طريق كلمة السر الحقيقية عندما يكون الجاني غير مخول له استخدامها، واستخدام برامج شفرة خاصة، أو عن طريق استخدام الرقم الكودي لشخص آخر، سواء ثم ذلك عن طريق شبكات الاتصال التليفونية أو محطات طرفيه سواء محلية وعالمية.[2]

أما في القانون الأمريكي فقد أصدرت الولايات المتحدة الأمريكية القانون الفيدرالي في شأن الاعتداء على الكمبيوتر واستغلاله في عام 1984 وتجرم المادة 1535 أ2 من قانون الفدرالي الأمريكي الخاصة بإساءة استخدام الحاسب الآلية الحصول على المعلومات عن طريق الدخول غير المصرح به، كما نجرم المادة 1535 أ 3 الدخول إلى الحاسبات الآلية التابعة للحكومة الفيدرالية أو تلك التي يؤدي الدخول غير المصرح به إليها المساس بأعمال تتعلق بحكومة. وبالتالي تم اعتبار كل دخول غير مشروع إلى معلومات مصنفة في حاسوب جنحة، أما إذا كان الدخول غير المشروع قاصدا سجلات مالية أو سجلات ائتمان في المؤسسات المالية أو انتهاك حرمة كمبيوتر الحكومة الفيدرالية فإن الجريمة تأخذ شكل جناية.[3]

2- موقف التشريعات العربية:

أما بالنسبة للمشرع السعودي ومن خلال نظام مكافحة جرائم المعلوماتية رقم 17 سنة 2007 نجده قد واجه جريمة الدخول غير المشروع بعدة نصوص، منها نص المادة الثالثة فقرة 2 تنص على أنه "يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

- التصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو احد أجهزة الحاسب الآلي

- الدخول غير المشروع إلى موقع الكتروني أو الدخول إلى موقع الكتروني لتغير تصاميم هذا الموقع أو إتلافه أو تعديله أو شغل عنوانه.

كما جاء في نص المادة 5على أنه "يعاقب بالسجن مدة لا تزيد على أربعة سنوات وبغرامة لا تزيد على 3 ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

[1]- أحمد عصام عجيلة، مرجع سابق، ص 315

[2]- أمين عزان، الحماية الجنائية لتجارة الالكترونية، دراسة مقارنة، رسالة دكتوراه، حقوق عين شمس، القاهرة، مصر، 2005، ص 91.

[3]- خالد ممدوح إبراهيم، مرجع سابق، ص 179

- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها أو تدميرها أو تسريبها، أو إتلافها أو تغييرها أو إعادة نشرها.

- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير أو مسح البرامج أو البيانات الموجودة أو المستخدمة فيها أو حذفها أو لتسريبها أو إتلافها، أو تعديلها.

- إعاقة الوصول إلى الخدمة أو تشويشها أو تعطيلها، بأي وسيلة كانت.[1]

أما في دولة الجزائر، وضمن سياق التعديل الذي أجراه المشرع على قانون العقوبات الجزائري فقد تناول جريمة الدخول أو البقاء بدون تصريح في النظام المعلوماتي وذلك في المادة 394 مكرر والتي تنص على "يعاقب بالحبس من ثلاثة أشهر، إلى سنة وبغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغير معطيات المنظومة، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين وبغرامة من 50000 إلى 150000 دج ويلاحظ أن المشرع الجزائري جرم فعل الدخول المجرد بدون تصريح إلى النظام المعلوماتي واعتبر السلوك بحد ذاته جريمة، فمجرد الدخول سواء كان بقصد الوصول إلى بالبيانات أو لمجرد التسلية يعد انتهاكا لنظام المعلوماتي وأن لم يترتب على ذلك إضرار بالمعلومات أو النظام الذي تحويه.[2]

كما جرم المشرع البقاء بدون تصريح في ذات النص، وذلك لمواجهة حالات الدخول عن طريق الخطأ أو السهو أو تجاوز التصريح واعتبر البقاء عن قصد مشكلا جريمة تتم عن إرادة الجاني في الإضرار بالغير[3] وكذلك من خلال استقراء نص المادة 394 مكرر من قانون العقوبات الجزائري نجد أنها قد نصت على ظرفين مشددين لعقوبة جريمة الدخول أو البقاء بدون تصريح داخل النظام، حيث تضاعفت العقوبة في الحالة التي ينتج عنها محو أو تعديل للبيانات التي يحتويها النظام بينما تشدد العقوبة وتصبح الحبس من 6 أشهر إلى سنتين وبغرامة 50000 إلى 150000 دج، إذا ترتب على الدخول أو البقاء عدم قدرة النظام على تأدية وظائفه وتجدر الإشارة أن المشرع الجزائري لم يكتفي بتجريم الدخول أو البقاء بدون تصريح في

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 218.

[2]- ربيحة زيدان، مرجع سابق، ص 51.

[3]- محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت، ، دار الفكر، طبعة الأولى، المنصورة، القاهرة، 2013، ص 30.

النظام المعلوماتي بل تجاوز ذلك إلى تجريم المحاولة وذلك بحسب العبارة أو يحاول ذلك بما معناه تجريم المشروع في جريمة الدخول أو البقاء بدون تصريح في النظام المعلوماتي.[1]

الفرع الثاني: جريمة تعطيل أو إفساد النظام المعلوماتي

تتحقق هذه الجريمة بتعطيل وإعاقة النظام المعلوماتي عن القيام بوظائفه المعتادة حيث يترتب على ذلك توقف النظام عن العمل بشكل تام أو تباطأ واضطراب في عمله مما يؤدي إلى إصدار نتائج غير صحيحة ومخالف للحالة المعهودة لعمل النظام والوقوف على هذه الجريمة لابد أن نستعرض مفهومها ولا ثم أركانها ثم موقف القوانين العقابية منها.

أولا:تعريف جريمة تعطيل وإفساد النظام المعلوماتي

تعرف جريمة تعطيل وإفساد النظام المعلوماتي بأنها "الاعتداء على نظم المعالجة الآلية للمعلومات بمنعها من أداء وظائفها بصورة تامة أو إجراء تعديل في تلك الوظائف.[2]

أو تعرف بأنها "كل فعل يتسبب في توقف أو تباطأ أو ارتباك عمل نظام المعالجة ومن ثم ينتج عن ذلك تغير في حالة النظام.[3]

ولخطورة السلوكيات التي تنطوي عليها هذه الجريمة اتجه اغلب المشرعين إلى مواجهتها سواء من خلال التشريعات الصادرة لمواجهة الجرائم المعلوماتية أو من خلال إجراء تعديلات على التشريعات العقابية القائمة، ففي فرنسا مثلا جرم المشرع فعلي إعاقة النظام وإفساده في المادة 323 ف1-2[4] وكذا في كندا أضيفت فقرة إلى المادة 430 من قانون العقوبات لسنة 1985 والخاصة بالإتلاف جرمت بموجبها الأفعال التي من شأنها منع أو إيقاف أو عرقلة نظام الحاسب الآلي عن أداء عمله، كما جرم المشرع في دولة الإمارات العربية المتحدة إعاقة وتعطيل النظام المعلوماتي من خلال المواد 5-6 من قانون مكافحة جرائم تقنية المعلومات، وكذا قانون جرائم المعلوماتية في السودان 2007 حيث نصت المادة 8 من هذا القانون "كل من يدخل بأية وسيلة نظاما أو وسائط أو شبكات المعلومات وما في حكمها ويقوم عمدا بإيقافها وتعطيلها يعاقب بالسجن مدة لا تتجاوز ستة سنوات أو بالغرامة أو بالعقوبتين معا.[5]

---

[1]- ربيحة زيدان، مرجع سابق، ص 52.

[2]- دلخار صلاح بوتاني، مرجع سابق، ص 227

[3]- نائلة عادل محمد فريد، مرجع سابق، ص 225

4- محمد خليفة، مرجع سابق، ص 167.

[5]- دلخارصلاح بوتاني ، مرجع سابق، ص 229

ثانيا: الركن المادي لجريمة تعطيل وإفساد النظام المعلوماتي

يتمثل النشاط الإجرامي المكون لركن المادي لهذه الجريمة أما في فعل تعطيل النظام المعلوماتي وأما في إفساد نشاط أو وظائف هذا النظام[1] وفعل التعطيل أو الإفساد قد يقع بوسيلة مادية كما في حالة وقوع النشاط الإجرامي على أجهزة الحاسب الآلي بكسرها أو سكب سائل عليها أو إحراقها مثلا أو قد يقع بوسائل معنوية عندما يقع النشاط الإجرامي على الكيانات المنطقية المعنوية الحاسب الآلي، كإدخال الفيروسات مثلا.[2]

وعليه سوف نتناول فعل تعطيل وإفساد النظام المعلوماتي- نتناول الوسائل المعنوية المستخدمة في هذه الجريمة كونها الوسائل الأكثر فعالية وقوعا في الواقع العملي.

1- فعل التعطيل أو إفساد النظام المعلوماتي:

يتمثل مضمون الركن المادي لجريمة تعطيل أو إفساد النظام المعلوماتي في فعلي التعطيل والإفساد، اللذين ينصرفان إلى أي عمل يأتيه الجاني ويكون من شأنه إعاقة النظام المعلوماتي أو إدخال سير عمله وهو ما سنبحثه فيما يأتي:

أ- فعل التعطيل:

العطل لغة: يعني الخلو من الشيء ويقال تعطيل الرجل أي بقي بلا عمل

أما اصطلاحا: هو منع النظام المعلوماتي بصفة كلية أو جزئية من العمل وهو ما يرد على النظام بأكمله أو على أحد البرامج الموجودة بداخله.[3]

- إن التعطيل الذي من شأنه منع سير وظائف النظام المعلوماتي عن العمل يقتضي أن يكون موجها إلى برامج تشغيل النظام التي تقوم بأداء وظائف عمل النظام وليس المعلومات بالمعنى الضيق كالبرامج التشغيلية أو التطبيقية التي إليها النظام في القيام بعمله.

وقد يتم بوسيلة مادية أو معنوية فتكون وسيلة التعطيل مادية سواء اقترنت بهدف أم لا إذا ما انصب نشاط إجرامي بطريقة مادية وعلى الأجهزة المادية عن طريق تخريبها أما بكسرها أو سكب سائل عليها وتحطيم الاسطوانة وأي عمل من شأنه منع العاملين في النظام من العمل، بينما تكون وسيلة

[1]- عبد القادر القهوجي، مرجع سابق، ص 128

[2]- دلخار صلاح بوتاني، مرجع سابق، ص 229

[3]-أيمن رمضان محمد أحمد، الحماية الجنائية لتوقيع الالكتروني، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، القاهرة، 2010، ص 160.

التعطيل معنوية مثل إدخال فيروسي تدميري، يؤدي إلى توقف دائم لنظام أو طريق إدخال قنبلة معلوماتية زمنية مبرمجة ينتج عنها شكل في التشغيل ويستوي أن يكون التعطيل بالنسبة إلى مستخدمي نظام أو بالنسبة إلى جميع المستخدمين.[1]

ب- فعل الفساد:

الإفساد أصله فسد، معناه لغة الخلل والاضطراب أو التلف أو العطب أما اصطلاحا وفي الجريمة فإنه يقصد به "ممارسته أي فعل على النظام المعلوماتي من شأنه أن يعدل في وظيفته دون أن يعوقه عن أداء هذه الوظيفة" أي بمعنى جعل النظام غير قابل للاستعمال،وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها، هذا السياق قضي في فرنسا بوقوع جريمة تعطيل وإفساد النظام المعلوماتي بحق المتهمين الذين ارسلو رسائل كثيرة بدون وجه حق عبر نظام الحاسب الآلي، مما أدى إلى إرباك النظام المتلقي لهذه الرسائل والإفساد قد يرد على برنامج من البرامج الموجودة في النظام وليس شرطا أن يرد على كل النظام.[2]

وتتعدد وسائل إفساد النظام المعلوماتي،فقد يقع الإفساد بوسائل معنوية أو مادية منها استخدام القنبلة المعلوماتية والتي تتكاثر داخل النظام وتجعله غير صالح للاستعمال أو استخدام برنامج يحمل فيروسا يقوم بتغيير غير محسوس في البرامج والمعلومات الموجودة داخل النظام،أو قد يتحقق الإفساد عن طريق تخريب العناصر المادية في النظام.[3]

2- الرسائل المعنوية المستخدمة في تعطيل وإفساد النظام المعلوماتي:

سبق واشرنا إلى أن تعطيل وإفساد النظام المعلوماتي قد يتم باستخدام وسائل معنوية تنصب على الكيانات المنطقية للنظام، كالقيام بإدخال برنامج فيروسي أو تغيير كلمة السر الخاصة بالدخول إلى النظام، ومن الصعب عمليا حصر هذه الوسائل المعنوية في الوقت ومن اخطر وأكثر الوسائل المعنوية التي تصيب النظام المعلوماتي ما يلي

[1]- عبد القادر القهوجي، مرجع سابق، ص 129.

[2]- أشرف توفيق شمس الدين، مرجع سابق، ص 118.

3- دلخار صلاح بوتاني، مرجع سابق، ص 232.

- الفيروسات:

الفيروس هو عبارة عن كود مبرمج بطريقة معينة، أحيانا يتذكر في شيء آخر والذي يتسبب في إظهار بعض الأحداث غير المتوقعة وغالبا ما تكون غير مرغوبة، وبإمكانه أن ينتشر بصورة أوتوماتيكية إلى حواسب آلية أخرى أو هو "برنامج يعمل على تعطيل النظام المعلوماتي أو شبكة الحاسبات الآلية.[1]

إذن الفيروسات عبارة عن برامج وضعت من قبل أشخاص على علم ودراية وخبرة بالبرمجة المعلوماتية، استخدموا تقنيات متقدمة في وضعها لها القدرة على التكاثر بنسخ نفسها والانتقال والانتشار في الأنظمة المعلوماتية وقد تؤدي في النهاية إلى تعطل النظام بالكامل.[2]

- برنامج الدورة المعلوماتية:

برنامج الدورة "عبارة عن برمجة تقوم بالانتقال من حاسب آلي إلى آخر دون حاجة إلى تدخل إنساني لتنشيطها، فتغطي شبكة بأكملها، ولديها إمكانية تعطيل نظام الحاسب إلا بصورة كاملة عن طريق استغلال أي خلل أو فجوة في نظام تشغيل الحاسب وتهدف برامج.

وتهدف برامج الدورة أساسا إلى استغلال أكبر مساحة ممكنة من سعة النظام مما يؤدي إلى التقليل أو الخفض من قدراته وقد يتجاوز ذلك في بعض الأحيان فتقوم بأعمال تخريب للملفات والبرامج وأنظمة تشغيل الحاسب.[3]

- القنبلة الزمنية:

تعرف بأنها "ذلك البرنامج الذي يثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة ويتم إدخالها في برنامج، وتنفذ من خلال جزء من الثانية، وعدة ثوان أو دقائق بحسب التحديد اللازم وسميت بالقنبلة الزمنية كونها تنشط وتعمل على تعطيل النظام في وقت محدد بالساعة واليوم والسنة.[4]

ثالثا: الركن المعنوي لجريمة تعطيل أو إفساد النظام المعلوماتي:

جريمة تعطيل أو إفساد النظام المعلوماتي هي جريمة عمدية لا يكفي لقيامها تحقيق الركن المادي فقط، وإنما لا بد من توافر الركن المعنوي أيضا والذي يتخذ في هذه الجريمة صورة القصد الجنائي العام

---

[1]- هدى حامد قشقوش، مرجع سابق، ص 99

[2]- دلخار صلاح بوتاني، مرجع سابق، ص 236

[3]- سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة عربية، القاهرة، مصر، 2008، ص 106

[4]- حسام محمد نبيل الشزاقي مرجع سابق، ص 197

بتوافر عنصريه العلم والإرادة وأن يتجه كلاهما إلى العناصر المشكلة للركن المادي للجريمة كافة، إذ يجب أن يعلم الجاني أن النشاط الإجرامي الذي يأتيه من شأنه تعطيل وإفساد النظام المعلوماتي وان ذلك يتم دون رضا صاحب الحق في السيطرة على ذلك النظام أو ضد إرادته ومع ذلك تتجه إرادته إلى فعل التعطيل أو الإفساد، فإذا تحقق الركن المادي والركن المعنوي بعنصريه قامت الجريمة.[1]

هذا وتستوجب بعض التشريعات التي جرمت تعطل أو إفساد النظام المعلوماتي إلى جانب القصد الجنائي العام، أن تتجه إرادة الجاني إلى تحقيق قصد خاص، فنجد القانون الفرنسي رقم 19 لسنة 1988 قبل تعديله كان يتطلب قصدا خاصا عبر عنه المشرع بعبارة دون مراعاة لحقوق الغير حيث نصت المادة 3/462 من القانون المذكور على أنه "يعاقب بالحبس لمدة تتراوح ما بين ثلاثة أشهر وثلاث سنوات وبغرامة تتراوح ما بين عشرة ألاف ومائة ألف فرنك أو بإحدى هاتين العقوبتين كل من عطل أو أفسد متعمدا ودون مراعاة لحقوق الغير، تشغيل نظام المعالجة الآلية للمعلومات.

كما نجد أن القانون البرتغالي لسنة 1991 يتطلب في المادتين 5-6 لقيام جريمة التعطيل أو الإفساد أن تتجه نية المتهم إلى الإضرار بالغير أو إلى تحقيق ربح غير مشروع له أو للغير.

وعلى خلاف ذلك تعاقب بعض التشريعات على تعطيل أو إفساد النظام المعلوماتي الذي يقع بدون قصد جنائي كقانون الدنمركي وذلك من خلال تجريم حالات الدخول أو البقاء بدون تصريح داخل النظام التي ينتج عنها تعطيل أو إفساد للنظام دون أن تتجه نية المتهم إلى تحقيق ذلك.[2]

رابعا: موقف التشريعات العقابية من جريمة تعطيل أو إفساد النظام المعلوماتي

لا شك أن جريمة تعطيل أو إفساد النظام المعلوماتي من الجرائم المعلوماتية المستحدثة والتي لا نجد مثيلا لها في التشريعات الجنائية للدول التي لم تسن بعد قوانين عقابية جديدة خاصة بمواجهة الجرائم المعلوماتية أو تعدل نصوص قوانين العقوبات النافذة فيها بما يمكنها من مواجهة هذه الأفعال الإجرامية المستحدثة لذا نجد تفاوت في موقف القوانين العقابية شأنها على النحو التالي:

[1]- عبد القادر القهوجي، مرجع سابق، ص 131

[2]- نائلة عادل محمد فريد قورة، مرجع سابق، ص 228.

- موقف التشريعات الغربية:

ففي فرنسا نص قانون العقوبات الجديد على تجريم أو إفساد النظام المعلوماتي وذلك بنص المادة 2/232 والتي تنص بأنه "تعطيل أو إفساد سير نظام المعالجة الآلية للبيانات يعاقب عليه بالسجن لمدة خمس سنوات وغرامة قدرها 75000 يورو.[1]

ويلاحظ أن المشرع الفرنسي لم يتطلب في هذه المادة أن يسبق فعل التعطيل أو الإفساد دخول غير مشروع إلى النظام، وأن النص يتسع ليشمل كل سلوك من شأنه تعطيل النظام سواء كان هذا التعطيل كليا أو جزئيا أو اقتصر على مجرد إفساد النظام وليس بضرورة أن يكون تعطيل النظام ناتجا عن سلوك مادي ينطوي على استخدام العنف من قبل الجاني فقد يكون التعطيل ناجما عن وسيلة معنوية، وهو الأمر الغالب.[2]

ففي قانون الولايات المتحدة الأمريكية جرمت المادة 1/1030 من القانون الفيدرالي إتلاف المعلومات الذي يترتب عليه تعطيل أنظمة الحاسبات الآلية التابعة إلى الحكومة، وقد وجهت انتقادات عديدة إلى هذه المادة كون الحماية تقتصر على الحاسبات الآلية التابعة إلى الإدارات الحكومة، ونتيجة لذلك عدل القانون سنة 1986 وأصبحت فقرة 3 من المادة 1030 أ نتناول فقط الدخول غير المصرح به إلى حاسب آلي تستعمله الحكومة حتى عطل الدخول هذا الاستعمال، ثم عدلت مرة أخرى سنة 1996 بقانون حماية بنية المعلومات القومية وأصبحت الحماية تشمل إلى جانب أنظمة الحاسبات الآلية للمؤسسات الاقتصادية التابعة إلى حكومة الولايات المتحدة وأنظمة الحاسبات الآلية التي تستخدم في التجارة والاتصالات بين الولايات وبين الولايات والدول الأخرى شريطة حدوث أضرار تلحق بالحاسب الآلي، حيث تنص على تجريم "تعديل المعلومات والبرامج والشفرات والأوامر داخل أنظمة الحسابات الآلية مما يترتب عليه إضرار تلحق بحاسب آلي يتمتع بالحماية متى كان إحداث الضرر قد تم عمد...".

وقد حددت الفقرة الثامنة من المادة 1030/د المقصود بالإضرار التي تلحق بالحاسب الآلي إنها "كل إتلاف أو إفساد لسلامة المعلومات، والبرامج وأنظمة الحاسبات الآلية".

---

[1]- عدلت هذه المادة بالأمر رقم 575 لسنة 2004 وتنص باللغة الفرنسية

Article 323-2 le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatise de donnes et puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

[2]- نائلة عادل محمد فريد قورة، مرجع سابق، ص 211

موقف التشريعات العربية:

أما بالنسبة إلى موفق المشرع في المملكة العربية السعودية من جريمة تعطيل أو إفساد النظام المعلوماتي، نجده قد نص على هذه الجريمة في المادة الخامسة فقرة 2-3 من نظام مكافحة جرائم المعلوماتية رقم 18 سنة 2008 والتي تنص على انه "يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أي من الجرائم المعلوماتية الآتية إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدمير أو مسح البرامج أو البيانات الموجودة أو المستخدمة فيها أو حذفها أو تسريبها أو إتلافها أو تعديلها- إعاقة الوصول إلى الخدمة أو تشويشها أو تعطيلها بأي وسيلة كانت، ويشترط وقف المشرع السعودي أن تتحقق نتيجة معينة على السلوك الايجابي الذي يصدر من الجاني وهي إما تعطيل الشبكة أو تدمير ومسح البيانات الموجودة فيه أو تسريبها أو تشويه الخدمة وتعطيلها[1].

أما في التشريع الجزائري فلم يتعرض المشرع الجزائري إلى جريمة تعطيل أو إفساد النظام المعلوماتي حتى بعد إضافة القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات، وذلك بالتعديل الذي أجراه المشرع على قانون العقوبات واكتفى بالنص على جريمة الاعتداء على المعطيات المعلومات [2] والمادة 394 مكرر1 وبرر البعض موقف المشرع الجزائري بعدم النص على جريمة تعطيل أو إفساد النظام المعلوماتي للتشابه الكبير بينهما وبين جريمة الاعتداء على المعطيات والتي يصعب بحسب هذا الرأي التمييز بينهما، ذلك لأن الأفعال التي تتضمنها جريمة الاعتداء على المعطيات تؤدي هي الأخرى إلى تعطيل النظام وإفساده، كما اعتبر المشرع الجزائري إفساد النظام نتيجة ظرف مشددا لجريمة الدخول بطريق الغش إلى النظام المعلوماتي وذلك في الفقرة الأخيرة من نص المادة 394 مكرر من قانون العقوبات إضافة إلى أن المشرع الجزائري اعتبر برامج سير نظام المعالجة الآلية للمعطيات تدخل ضمن المعطيات المعلوماتية والتي عرفها في الفقرة ج من المادة الثانية من قانون رقم 04-09 المؤرخ في 2009/8/5[3] أنها المعطيات المعلوماتية أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها" وفي هذا الصدد وضع الفقه معيارا للتفرقة بين الاعتداء على المعطيات وبين الاعتداء على النظام على

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 248-251

[2]- خثير مسعود، مرجع سابق، ص 120

[3]- القانون رقم09-04 المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم :47 المؤرخة في 16-08-2009.

أساس ما إذا كان الاعتداء وسيلة أم غاية، فإذا كان الاعتداء مجرد وسيلة فإن الفعل يشكل جريمة الاعتداء العمدي على النظام تعطيل أما إذا كان الاعتداء غاية فإنه يشكل جريمة الاعتداء العمدي على المعطيات المعلومات[1].

المطلب الثاني: جرائم الاعتداء على التوقيع الالكتروني وبياناته.

إن التحول الحضاري والتقدم الذي اجتاح العالم في العصر الحديث أحدث تغيرا ملموسا في نوعية الجرائم للمجرمين، فبعد أن كانت الغلبة للجرائم القائمة على العنف أو القسوة، أصبحت الغلبة للجرائم القائمة على المقدرة الذهنية والذكاء وتعتبر تقنية المعلومات إحدى نتائج هذا التحول الحضاري والتقدم الذي اجتاح العالم في العصر الحديث، ففي عالم فخم ومتنوع دخلت تقنية المعلومات جميع أروقته، عالم ساهم في إنتاج وتطوير العديد من السلوكيات الإجرامية ذات الأثر البالغ على حياة الأفراد والمجتمع كالجرائم المتعلقة باعتداء على التوقيع الالكتروني وبياناته وهذا ما سنعرضه في هذا المطلب ضمن فرعين

الفرع الأول: جرائم الاعتداء على التوقيع الالكتروني وبياناته فيالتشريعات المقارنة.

الفرع الثاني: جرائم الاعتداء على التوقيع الالكتروني وبياناته في قانون 09/15 قانون متعلق بالتوقيع والتصديق الالكتروني الجزائري.

الفرع الأول: جرائم الاعتداء على التوقيع الالكتروني وبياناته في التشريعات المقارنة.

نظرا لخطورة جرائم الاعتداء على التوقيع الالكتروني وبياناته في العصر الحديث استجابت التشريعات الأجنبية منها والعربية لمتطلبات عصرنة هذه التقنية واتخذت التدابير التشريعية اللازمة التي تمكنها صد الآثار السلبية الإجرامية الناجمة عن إساءة استعمال هذه التقنية ومن خلال هذا الجزء من البحث سنتناول الجرائم المهمة الواقعة على التوقيع الالكتروني وبياناته في التشريعات المقارنة.

أولا: جرائم الاعتداء على بيانات التوقيع الالكتروني.

كفلت التشريعات المقارنة نوعا من الحماية الجنائية لسرية البيانات ومعلومات التوقيع الالكتروني، وهذا ما سنعرضه في هذا الجزء من البحث.

أ- جنحة إفشاء بيانات التوقيع الالكتروني أو الوسائط الالكترونية أو المعلومات.

[1]- دلخار صلاح بوتاني، مرجع سابق، ص 250.

تقوم هذه الجريمة باستنزاف فعل إفشاء البيانات، مع الأخذ بعين الاعتبار توافر صفة خاصة في المتهم إلى جانب القصد الجنائي، وسنتناول أركان هذه الجريمة وذلك على النحو التالي:

1- الركن الشرعي:

نصت المادة 21 من قانون رقم 15 لسنة 2004 على أن "بيانات التوقيع الالكتروني والوسائط الالكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الالكتروني سرية، ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها أو استخدامها في غير الغرض الذي قدمتن من أجله.

ونصت المادة 23 من هذا القانون على أنه "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في القانون العقوبات أو في قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تتجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من خالف أيا من أحكام المادتين 19 و21 من هذا القانون[1].

2- علة التجريم:

تتجسد علة التجريم في المساعدة على تحقيق الأمن المعلوماتي، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية، أو حماية المصلحة العامة والأخلاق والآداب العامة.

وفضلا عن ذلك حماية الحياة الخاصة بصفة عامة وعدم اطلاع الغير عليها وعلى ما يدور بين الأفراد من أسرار[2].

كما أكدت التوجيهات الأوروبية مبدأ حماية المعطيات الشخصية عبر الانترنت وحماية الحياة الخاصة، وأهمها التوجيه الحالي رقم 80 لسنة 2002 الصادر في 12 يوليو 2002 بمعالجة المعطيات ذات الطابع الشخصي، وحماية الحياة الخاصة في إطار الاتصالات الالكترونية.

وقد حدد القانون الفرنسي رقم 801 لسنة 2004 الصادر في 06 أغسطس 2004 المقصود بالمعطيات ذات الطابع الشخصي وهي "كل معلومة متعلقة بشخص طبيعي معين أو قليل لتعي، سواء بطريقة مباشرة أو غير مباشرة، وذلك بالرجوع إلى رقم تحديد هوية أو إلى عناصر أخرى خاصة به[3].

---

[1]- محمد علي سويلم، مرجع سابق، ص 988.

[2]- طارق سرور، جرائم النشر والإعلام، دار النهضة العربية ،الطبعة الأولى، القاهرة، مصر2001، ص 191.

[3]- سعيد السيد قنديل، مرجع سابق، ص 32.

3- الركن المفترض المرخص له:

الشرط المفترض هو مركز قانوني تحميه القاعدة الجنائية، يستقل ويتميز عن أركان الجريمة التي تعد في نهاية الأمر انتهاكا لهذا الشرط وعدوانا عليه ويتعلق الشرط المفترض بصفة الجاني وهو ان يكون قدمت إليه بيانات التوقيع الالكتروني أو الوسائط الالكترونية أو المعلومات من الجهة المرخص لها بإصدار شهادات التصديق الالكتروني أو من اتصل بها بحكم عمله ويعني أي شخص طبيعي أو اعتباري، مرخص له من هيئة تنمية صناعة تكنولوجيا المعلومات بتقديم خدمة إصدار شهادة التصديق الالكتروني وتقديم خدمات تتعلق بالتوقيع الالكتروني[1].

4- الركن المادي:

تقوم الجريمة على سلوك إيجابي يتمثل في إفشاء من قدمت إليه بيانات التوقيع الالكتروني او الوسائط الالكترونية أو المعلومات من الجهة المرخص لها بإصدار شهادات التصديق الالكتروني أو من اتصل بها بحكم عمله لتلك البيانات للغير، ويقصد بالإفشاء البوح أو إحاطة علم الغير ببيانات التوقيع الالكتروني او الوسائط الالكترونية أو المعلومات من المرخص لها بإصدار شهادات التصديق الالكتروني وينصرف مدلول الغير إلى كل شخص غير صاحب التوقيع الالكتروني، ويستوي بعد ذلك طريقة النشر أو الإذاعة للمعلومات أو البيانات.

وتطبيقا لذلك يعد الشخص الذي يعمل لدى إحدى جهات التصديق الالكتروني مرتكبا لهذه الجريمة إذا أفشى بيانات التوقيع الالكتروني أو الوسائط الالكترونية أو المعلومات من الجهة المرخص لها بإصدار شهادات التصديق الالكتروني التي اتصل بها بحكم عمله أو قدمها للغير دون أن يكون له سند قانوني والسند القانوني هو تنفيذ أمر أو حكم أو تنفيذ الموظف لمقتضيات وظيفة التي تستلزم تسجيل مكالمات معينة أو تسجيل كل ما يصل من رسائل[2].

وتعتبر هذه الجريمة من الجرائم الشكلية، إذ لا يوقف القانون توافر نموذجها القانوني على تحقيق نتيجة معينة أو صور معينة كما تعتبر هذه الجريمة من الجرائم الوقتية أو الجرائم ذات السلوك المنتهي، لأنها تتم في الوقت الذي يقع فيه السلوك الإجرامي المتمثل في الإفشاء أو الاستخدام[3].

---

[1]- محمد علي سويلم، مرجع سابق، ص 990.

[2]- محمد علي سويلم، مرجع سابق، ص 991.

[3]- محمود نجيب حسني، مرجع سابق، ص 101.

5- الركن المعنوي:

تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي ويتألف القصد الجنائي من عنصرين هما العلم والإرادة، فالعلم يقتضي أن يعلم الجاني بأنه يخرق الحظر الوارد بنص المادة 21 من قانون التوقيع الالكتروني فيما يتعلق بإفشاء بيانات التوقيع أو المعلومات أو الوسائط الالكتروني وأنه اتصل علمه بسرية تلك البيانات بمناسبة وظيفته، وأن يعلم كذلك عدم إباحة صاحب التوقيع إفشاء السر كما يلزم أن تتجه إرادة الفاعل إلى إفشاء هذه البيانات للغير ومجرد الإفشاء كاف لتوافر القصد دون الحاجة لنية خاصة أو قصد الإضرار بالغير، ولا عبرة للبواعث بإفشاء السر حتى لو كان القصد درء المسؤولية[1].

6- العقوبة:

يعاقب على هذه الجريمة بغرامة الحبس وغرامة لا تقل عن عشرة آلاف جنيه ولا تتجاوز مائة ألف جنيه أو إحداهما والحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار وعلى شبكة المعلومات الالكترونية المفتوحة على نفقة المحكوم عليه م 23/1-3.

وفي حالة العود تزداد بمقدار المثل للعقوبة المقررة لهذه الجرائم في حديها الأدنى والأقصى م3/23[2].

ب-جنحة استخدام بيانات التوقيع الالكتروني أو الوسائط الالكترونية أو المعلومات في غير الغرض الذي قدمت من أجله.

لقيام هذه الجريمة لابد من توافر أركانها على النحو الآتي:

1- **الركن الشرعي:** نصت المادة 2 من القانون رقم 15 لسنة 2004 على أن بيانات التوقيع الالكتروني والوسائط الالكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الالكتروني سرية ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها أو استخدامها في غيرالغرض الذي قدمت من أجله[3].

2- **الركن المادي للجريمة:** يتحقق الركن المادي في الجريمة بإساءة استخدام بيانات التوقيع الالكتروني وذلك باستخدامها في غرض آخر غير ما قدمت من أجله[4].

---

[1]- أحمد محمود موافى، شرح وتعليق على أحكام قانون التوقيع الالكتروني، دار الفكر القانوني، طبعة أولى، مصر، 2008، ص 189.

[2]- محمد علي سويلم، مرجع سابق، ص 993.

[3]- محمد علي سويلم، مرجع سابق ، ص 987.

[4]- سليمان أحمد فاضل، مرجع سابق، ص 61.

كما تعد هذه الجريمة من جرائم السلوك الإيجابي يتحقق ركنها المادي بحدوث النشاط الإجرامي، ولا حاجة لتحقق النتيجة معينة، ويتحقق الركن المادي باستخدام الجاني للبيانات الخاصة بالتوقيع الالكتروني أو الوسائط الالكترونية أو المعلومات وذلك في غير الغرض الذي قدمت من أجله[1].

3- الركن المعنوي:

هذه الجريمة عمدية يلزم لقيامها توافر القصد الجنائي باتجاه إرادة الجاني إلى إساءة استخدام بيانات التوقيع الالكتروني، باستعمالها في غير الغرض المخصص لها، مع علمه بذلك وقبول النتائج المترتبة على هذا السلوك الإجرامي الذي لا يتصور وقوعه بالطريق الخطأ[2].

ومتى تحقق الركن المادي والركن المعنوي وجب إنزال العقوبة على الجاني السابق بينها بنص المادة 3/23 السابق بيانها دون النظر إلى الباعث الذي دفعه إلى إساءة استخدام بيانات التوقيع الالكتروني[3].

ثانيا: جرائم الاعتداء على شهادات التصديق الالكتروني.

لقد اهتمت التشريعات المقارنة بالتصديق الالكتروني وحددت له نطاقا من الحماية الجنائية لمنع أي مساس أو اعتداء عليه وهذا ما سنعرضه في هذا الجزء من البحث لأهم الجرائم الماسة بشهادات التصديق الالكترونية.

أ- جريمة إصدار شهادة التصديق الالكتروني قبل الحصول على ترخيص.

يتطلب لقيام هذه الجريمة توافر البنيان القانوني لها والمتمثل في أركانها على النحو التالي:

1- الركن الشرعي:

لقد نص المشرع المصري على هذه الجريمة في المادة 23/أ من قانون التوقيع الالكتروني –ويتطلب لقيامها- والتي نصت على أنه "يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تتجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من: أصدر شهادة تصديق الكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة.

2- الركن المادي:

تقوم هذه الجريمة على سلوك إيجابي يتمثل السلوك الإجرامي في إصدار شهادة تصديق الكتروني قبل الحصول على ترخيص بمزاولة النشاط من الهيئة المختصة، ومؤدي ذلك أن النموذج القانوني للركن المادي لهذه الجريمة يتمثل في نشاط إيجابي، ومن ثم لا يكفي مجرد الامتناع أو إصرار الجاني داخل

[1]- راجع المادة 21 من قانون التوقيع الالكتروني المصري.

[2]- سليمان أحمد فاضل، مرجع سابق، ص 161.

[3]- راجع المادة 3/23 من قانون التوقيع الالكتروني المصري.

نفسيته على ارتكاب الجريمة، بل لابد أن يظهر فعل الجاني في مزاولة هذا النشاط دون الحصول على ترخيص ومخالفة المادة 19 من قانون التوقيع الالكتروني[1].

والسبب في تجريم هذا الفعل هو الآثار الخطيرة المترتبة على شهادة التصديق الالكترونية في حق الغير[2].

ويمكن القول أن هذه الجريمة من جرائم الخطر، أو جرائم السلوك المجرد حيث بتكامل قيام الركن المادي فيها بمجرد إتيان الجاني لسلوك إصدار شهادات التصديق الالكتروني بدون ترخيص، دون تطلب حصول ضرر بجهة ما أو شخص ما[3].

3- الركن المعنوي:

تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي ويتألف القصد الجنائي من عنصرين هما العلم والإرادة فالعلم يقتضي إدراك الجاني لحقيقة النشاط الإجرامي، وهو يتمثل في إصدار شهادة تصديق الكتروني قبل الحصول على ترخيص بمزاولة النشاط من الهيئة المختصة.

كما يتطلب القصد اتجاه إرادة الجاني إلى إصدار شهادة تصديق الكتروني قبل الحصول على ترخيص.

4- العقوبة:

يعاقب على هذه الجريمة بالحبس وغرامة لا تقل عن عشرة آلاف جنيه ولا تتجاوز مائة أف جنيه أو إحداهما والحكم بالنشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار وعلى شبكات المعلومات الالكترونية[4].

ب-جنحة توقف الجهة المختصة بإصدار شهادات التصديق الالكتروني عن عملها أو اندماجها أو تنازلها عن الترخيص للغير قبل الحصول على موافقة كتابية مسبقة من الهيئة.

تقوم هذه الجريمة بتوفر أركانها وهذا ما سنعرضه على النحو التالي:

---

[1]- تنص المادة 19 من قانون التوقيع الالكتروني على مجموعة من الالتزامات تقع على عاتق من يرغب في مزاولة نشاط إصدار شهادات التصديق الالكتروني وهي - ضرورة الحصول على ترخيص من هيئة تنمية صناعة تكنولوجيا المعلومات قبل ممارسة النشاط المذكور - سداد رسم الهيئة المذكورة مقابل هذا النشاط عدم جواز التوقف عن النشاط المرخص به أو الاندماج في جهة أخرى أو التنازل عن الترخيص للغير، سوى بعد الحصول على موافقة كتابية من الهيئة المذكورة.

[2]- عرف القانون 15 لسنة 2004 في مادته الأولى شهادة التصديق الالكتروني بأنها الشهادة التي تصدرها الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع.

[3]- عبد الفتاح بيومي حجازي، مرجع سابق، ص 541.

[4]- محمد علي سويلم، مرجع سابق، ص 940.

1- الركن الشرعي:

صنت المادة 19 من القانون رقم 15 لسنة 2004 على أن "لا تجوز مزاول نشاط إصدار شهادات التصديق الالكتروني إلا بترخيص من الهيئة، وذلك نظير مقابل يحدده مجلس إدارتها وفقا للإجراءات والقواعد والضمانات التي تقررها اللائحة التنفيذية لهذا القانون. "ولا يجوز التوقف عن مزاولة النشاط المرخص به أو الاندماج في جهة أخرى أو التنازل عن الترخيص للغير إلا بعد الحصول على موافقة مسبقة من الهيئة[1].

ونصت المادة 23 من هذا القانون على انه " مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تتجاوز مائة آلف جنيه أو إحدى العقوبتين كل من خالف أحكام المادتين 19 21 من هذا القانون[2].

وقد أوردت السلوكات الإجرامية لهذه الجريمة بالأوصاف التالية:

– جنحة التوقف عن مزاولة نشاط إصدار شهادات التصديق الالكتروني المرخص به قبل الحصول على موافقة كتابية مسبقة من الجهة المختصة.

والتي يقوم ركنها المادي في هذه الجريمة باتخاذ الجهة المختصة والمرخص لها بإصدار شهادات التصديق على التوقيع الالكتروني لسلوك سلبي يتمثل في امتناعها عن إصدار تلك الشهادات، أي أن هذه الجريمة تدخل ضمن جرائم الخطر فيكفي لقيامها تحقق الركن المادي دون حاجة إلى تحقق نتيجة إجرامية، إلا انه استلزم المشرع أن يكون الامتناع هو الناتج عن إحجام الجاني عن إصدار شهادة التصديق دون موافقة كتابية مسبقة من الهيئة.

أما فيما يتعلق بالركن المعنوي لهذه الجريمة فهي من الجرائم العمدية يتخذ ركنها المعنوي صورة القصد الجنائي العام وقوامه العلم والإرادة، فيجب أن يعلم مرتكب الجريمة بتوقفه أو امتناعه عن إصدار شهادات التصديق الالكتروني، وأن يعلم باستلزام حصوله على موافقة كتابية من جهة الترخيص وأن تتجه إرادته إلى ارتكاب الفعل المجرم[3].

– جنحة اندماج الجهة المرخص لهابإصدار شهادات التصديق الالكتروني في جهة أخرى قبل الحصول على موافقة كتابية مسبقة من الهيئة المختصة.

[1]- راجع المادة 19 من قانون التوقيع الالكتروني المصري.

[2]- محمد علي سويلم، مرجع سابق، ص 980.

[3]- أحمد محمود موافى، مرجع سابق، ص 189.

قد تقرر الجهة المرخص لها بإصدار شهادات الاندماج أو الانضمام إلى جهة أخرى دون الحصول على موافقة كتابية مسبقة من الهيئة وبذلك ادخلها المشرع داخل نطاق التجريم.

فالركن المادي لهذه الجريمة تتكون من فعل إيجابي، قوامه قيام الجهة المرخص لها بالاندماج في جهة أخرى دون الحصول على موافقة كتابية مسبقة من هيئة تنمية صناعة تكنولوجيا المعلومات.

أما عن ركنها المعنوي فهي من الجرائم العمدية التي تتطلب توافر القصد الجنائي العام بعنصريه العلم والإرادة فيتعين على صاحب الجهة المرخص لها أن يعلم بأن الاندماج يتم مع جهة أخرى بدون استصدار موافقة كتابية من الهيئة المختصة وأن تتجه إرادته غلى ارتكاب الفعل المؤثم رغم اتصال علمه بالقيد الوارد في المادة.

– جنحة تنازل الجهة المرخص لها بمزاولة نشاط إصدار شهادات التصديق الالكتروني عن الترخيص للغير قبل الحصول على موافقة كتابية مسبقة من الهيئة المختصة.

قيد المشرع المصري الجهة المصرح لها بمزاولة نشاط إصدار شهادات التصديق فألزمها بمقتضى المادة 19 من قانون التوقيع الالكتروني والمادة 23 من اللائحة التنفيذية بضرورة الحصول على موافقة كتابية مسبقة من هيئة تنمية صناعة تكنولوجيا المعلومات متى رغبت في التنازل عن الترخيص الممنوح لها للغير[1].

وتعتبر الجريمة محل البحث من جرائم السلوك التي تقوم على ركنين احدهما مادي يتمثل في نشاط يصدر عن الجهة المرخص لها بإصدار شهادات التصديق، حيث تتنازل عن الترخيص الممنوح لها للغير دون الحصول على موافقة مسبقة من الهيئة المختصة تسمح خلالها بهذا التنازل.

أما الركن المعنوي لهذه الجريمة فيتمثل كون الجريمة عمدية لها توافر القصد الجنائي بعنصريه العلم والإرادة، فلابد أن يتصل علم الجاني بأنه قام بتنازل المرخص له بمزاولة نشاط إصدار شهادات التصديق الالكتروني عن الترخيص للغير قبل الحصول على ترخيص، وأن تتجه إرادته إلى إحداث ذلك قبل حصول الموافقة على التنازل[2].

الفرع الثاني: جرائم الاعتداء على التوقيع الالكتروني وبياناته في قانون الجزائري رقم 15-04:

بعدما اقتصر المشرع الجزائري في حماية التوقيع الالكتروني جنائيا على ما هو منصوص عليه في قانون العقوبات، توجه نحو إصدار قانون خاص بالتوقيع والتصديق الالكترونيين وهو القانون رقم 15-

[1]- راجع المادة 23 من اللائحة التنفيذية للقانون المصري.

[2]- محمد علي سويلم، مرجع سابق، ص 986.

04 المؤرخ في 2015/02/01 أين أقر في هذا القانون حماية جنائية للتوقيع والتصديق الالكترونيين من خلال تعداده لمختلف الجرائم الواقعة عليهما.

ومن هذا المنطلق سنتناول في هذا الفرع أهم الجرائم الواقعة على التوقيع والتصديق الالكترونيين التي نص عليها هذا القانون.

وبالرجوع إلى النصوص القانونية التي اقرها القانون رقم 15-04 نجد أنها تتفق في كون أن الجرائم المنصوص عنها هي جرائم عمدية يتطلب قيامها توافر الركن المعنوي الذي يقوم على القصد الجنائي العام بعنصريه العلم والإرادة ولا تحتاج إلى القصد الخاص.

ويتمثل العلم بكل واقعة ذات أهمية قانونية في تكوين الجريمة، أي كل واقعة يتطلبها القانون لبناء أركان الجريمة واستكمال عناصرها إضافةإلى ذلك لابد أن يشمل أيضا على التكييف الذي تتصف به بعض هذه الوقائع من الناحية القانونية أو بعبارة أخرى يتعين على الجاني العلم بموضوع الحق المعتدى عليه.

أما الإرادة التي يتطلبها القصد العام فهي "حالة ذهنية أو نفسية يكون عليها الجاني ساعة إقدامه على ارتكاب الجريمة وإرادة الجاني في القصد الجرمي على هذا النحو يجب أن تتجه إلى ارتكاب الفعل وكذا إلى إحداث النتيجة إلا أن الملاحظ على الجرائم التي قررها المشرع بموجب القانون 15-04 هي جرائم خطر وليست جرائم ضرر وبالتالي يكفي لقيامها توفر السلوك الإجرامي دون الحاجة إلى تحقق أو عدم تحقق نتيجة معينة[1] وترتيبا على ما تقدم فإن دراسة هذه الجرائم سوف يقتصر على الركن المادي مع تبيان النص القانوني المنظم لها على النحو التالي:

أولا: صور الاعتداء على بيانات التوقيع والتصديق الالكتروني.

عمل المشرع الجزائري على تعداد الجرائم المتعلقة ببيانات التوقيع والتصديق الالكتروني من خلال عدة مواد يمكن إنجازها في الجرائم التالية.

أ- جنحة إفشاء بيانات شهادة التصديق الالكتروني:

نصت على هذه الجريمة المادة 70 من القانون 15-04 والتي جاء فيها "يعاقب بالحبس من ثلاثة أشهر 03 إلى سنتين 02 وبغرامة من 200.000 دج إلى مليونين دج أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الالكتروني أخل بأحكام المادة 42 من هذا القانون".

[1]- عزيزة لرقط، الحماية الجنائية للتوقيع والتصديق الالكترونيين في التشريع الجزائري، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي تمنراست، عدد 1 جانفي، 2017، ص 118.

حيث نصت المادة 42 من نفس القانون على أنه "يجب على مؤدي خدمات التصديق الالكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الالكتروني الممنوحة[1].

ويظهر أن المشرع الجزائري اشترط لقيام هذه الجريمة توفر مجموعة من الأركان الآتي بيانها:

1- **صفة الجاني:** حتى تقوم هذه الجريمة يجب أن تتوافر لدى القائم بها صفة العمل لدى الجهة المختصة بإصدار شهادة التصديق الالكتروني وفي المقابل لا تقوم هذه الجريمة ممن لا يعملفي الهيئة أو الجهة المرخص لها بإصدار شهادات التصديق على التوقيعات الالكترونية وعلة التجريم تكمن في أن الجاني في هذه الجريمة قد أو تمت على هذه المعلومات أو البيانات بسبب وظيفته أو عمله.

2- **الركن المادي:** يتمثل المادي في هذه الجريمة بإتيان الجاني بفعل إيجابي بفعل إفشاء أو إعلام الغير بالمعلومات والبيانات المتعلقة بالتوقيع الالكتروني وينصب الفعل الإجرامي على محل الذي يتمثل في المعلومات الالكترونية ويقصد بها المعلومات المعالجة آليا بواسطة نظام معلوماتي أو احد أجزائه كالحاسب الآلي بهدف تصنيفها وإعادة إنتاجها وبثها أو تخزينها وتسجيلها سواء بواسطة أحد الأجزاء الداخلية للنظام المعلوماتي كذاكرة الحاسب الآلي أو على وسائل تخزين خارجية كالأقراص المرنةCD.

وتنقسم المعلومات أو البيانات الالكترونية من حيث إمكانية الوصول إليها غلى معلومات متاحة، ومعلومات سرية أو غير متاحة.

فيقصد بالمعلومات المتاحة تلك المعلومات والبيانات المنشورة على المواقع الالكترونية المفتوحة للجمهور أما المعلومات الالكترونية السرية أو غير المتاحة فهي التي يقتصر العلم بها على أشخاص محددين كمالكها أو من بملك السلطة القانونية عليها ولا تكون متاحة للكافة للوصول إليها والإطلاع عليها[2]وهذا هو ذات الشأن بالنسبة لبيانات السرية لشهادة التصديق الالكتروني باستثناء تلك التي رخص بشأنها كتابيا أو الكترونيا في نشرها أو الإعلام بها من الجهة المختصة.

الركن المعنوي :تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي، ويتألف القصد الجنائي من عنصرين هما : العلم والإرادة،فلعلم يقتضي إدراك الجاني لحقيقة النشاط الإجرامي،وهو أن يعلم بوقائع الجريمة كونها من المحظورات،ومع ذلك تتجه إرادتهإلى الفعل المجرم ويقبل النتيجة المترتبة عليها،وهي إفشاء بيانات شهادة التصديق الإلكترونية،كما يتطلب القصد

[1]- المادة 70 والمادة 42 من قانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 الموافق ل أول فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

[2]- محمد كمال محمود الدوسقي، الحماية الجنائية لسرية المعلومات الالكترونية، دار الفكر والقانون، المنصورة، مصر، 2018، ص 53.

اتجاه إرادة الجاني لارتكاب الفعل المؤثم قانونا والمتمثل فيافشاء البيانات المتعلق بمنظومة شهادة التصديق الإلكترونية .

ب-جنحة حيازة أو إفشاء أو استعمال بيانات توقيع موصوفة خاصة بالغير.

1-نص التجريم :ينص المشرع في المادة 68من نفس القانون على أنه " يعاقب بالحبس من ثلاثة 03 أشهر إلى ثلاث 03 سنوات وبغرامة من مليون دينار 1000.000دج إلى خمسة ملايين دينار أو بإحدى هاتين العقوبتين فقط كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير.

2-**صفة الجاني** :وهو أن يكون ممن قدمت إليه بيانات التوقيع الالكتروني الموصوف من الجهة المرخص لها بإصدار شهادات التصديق الالكتروني أو من اتصل بها بحكم عمله ويعني : أي شخص طبيعي أو معنوي،مرخص له بتقديم خدمة تتعلق بالتوقيع الالكتروني

3- **الركن المادي**:يشتمل نص هذه المادة على عدة أفعال هي الحيازة والإفشاء واستعمال بيانات إنشاء توقيع إلكتروني خاصة بالغير،يقصد بإفشاء البوح أو إحاطة علم الغير بيانات التوقيع الالكتروني أو الوسائط الالكترونية أو معلومات من الجهة المرخص لها بإصدار شهادات التصديق الالكتروني ويقصد بها جهات التصديق الالكتروني، أما استخدام البيانات فيعني، استعمال من قدمت إليه بيانات التوقيع الإلكتروني الخاص وبالغير ونقصد بالغير هنا كل شخص طبيعي أو معنوي صاحب التوقيع الإلكتروني أو الوسائط الإلكترونية أو المعلومات أو البيانات أما الحيازة فتتمثل في قيام الجاني إما بحيازة بيانات توقيع إلكتروني خاصة بالغير وتكفي هذه الحيازة المادية ولايشترط الحيازة القانونية.

وبالتالي يعد أحد هذه الأفعال كاف لقيام هذه الجريمة وتتحقق الجريمة أيضا في الحالة التي يقوم بها الجاني بإفشاء بيانات إنشاء التوقيع الالكتروني والعلة من التجريم انه من وضعت لديه هذه البيانات قد أؤتمن عليها[1].

4-**الركن المعنوي** :تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي، ويتألف القصد الجنائي من عنصرين هما:العلم والإرادة،فلعلم يقتضي إدراك الجاني لحقيقة النشاط الإجرامي وهو إفشاء من قدمت إليه بيانات التوقيع الإلكتروني واستخدامها وحيازتها واتجاهإرادة الجاني إلى ارتكاب الفعل المؤثم والمعاقب عليه قانونا .

[1]- عزيزة لرقط، مرجع سابق، ص 124.

ج- جنحة جمع البيانات الشخصية للموقع واستخدامها في غير غرضها.

1-نص التجريم :

وهي الجريمة المنصوص والمعاقب عليها بنص المادة 71 من نفس القانون والتي نصت على انه "يعاقب بالحبس من ستة 06 أشهر غلى ثلاث 03 سنوات وبغرامة من مائتي ألف دينار 200.000 إلى مليون دينار 1000.0000دج أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الالكتروني أخل بأحكام المادة 43 من هذا القانون.

حيث تنص المادة 43 من نفس القانون على انه لا يمكن لمؤدي خدمات التصديق الالكتروني جمع البيانات الشخصية للمعني إلا بعد موافقته الصريحة.

ولا يمكن لمؤدي خدمات التصديق الالكتروني أو يجمع إلا البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الالكتروني، ولا يمكن استعمال هذه البيانات لأغراض أخرى[1].

ويتبين من خلال المواد السابقة الذكر أم المشرع الجزائري اشترط لقيام هذه الجريمة توافر صفة معينة في الجاني بإضافة إلى الركنين المادي والمعنوي وفقا لما يلي:

-**2 صفة الجاني**: يتطلب لقيام هذه الجنحة أن تقع من مؤدي خدمات التصديق الالكتروني أو أحد العاملين به، ويجب أن يستخدم هذه البيانات التي قام بجمعها دون رضا الموقع في غير الغرض المخصص لها، وبالتالي لقيام هذه الجريمة في الحالة التي يكون جمع هذه البيانات الشخصية بموافقة صريحة من الموقع وكذلك في الغرض الذي خصص لها، ومن خلال ما تقدم يتعين توافر شرطين، الشرط الأول يتمثل في كون الجاني احد العاملين في الجهة المختصة بإصدار شهادات التصديق الالكتروني، أما الشرط الثاني فيتمثل في القيام بفعل جمع البيانات الشخصية دون الموافقة الصريحة من الموقع أو استخدام هذه البيانات في غير الغرض المخصص لها[2].

3-الركن المادي:

يتحقق الركن المادي بإتيان الجاني فعل إيجابي متمثل في استخدام بيانات التوقيع الالكتروني في غير الغرض المخصص لها، أو جمع البيانات دون الحصول على الموافقة الصريحة منه،فاستخدام يعني استعمال ممن قدمت إليه بيانات التوقيع الإلكتروني في الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني في غير الغرض الذي قدمت من اجله إما جمع البيانات دون الحصول على الموافقة الصريحة

[1]- راجع المادة رقم 71. 43 من قانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين السالف الذكر.

[2]- عزيزة لرقط، مرجع سابق، ص 122.

من صاحب التوقيع الإلكتروني ودون علمه ورضاه أيإتيان سلوك ايجابي من طرف الجاني هدفه استعمال في غير الغرض المخصص له،وتعتبر هذه الجريمة من جرائم السلوك إذ يتكون السلوك الإجرامي فيها من أفعال متعددة يكفي توافر إحداها لقيام الجريمة،كما أن توافرها مجتمعة لا يؤدي إلى تعدد الجرائم .

4-**الركن المعنوي** : تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي ، ويتألف القصد الجنائي من عنصرين : هما العلم والإرادة،فعلم يقتضي إدراك الجاني إن نشاطه الإجرامي معاقب عليه قانونا يتمثل جمع البيانات الشخصية للموقع واستخدامها في غير غرضها الأصلي واتجاه إرادة الجاني إلىارتكاب الفعل المجرم والنتيجة معا.

ثانيا: جرائم الاعتداء على شهادة التصديق الالكتروني.

لقد عدد القانون رقم 15-04 صور تجريمية متعددة ماسة بشهادة التصديق الالكترونية ومن بين أهم هذه الجرائم ما يلي:

أ- إصدارشهادة تصديق إلكتروني بدون ترخيص أوسحبه.

1-**نص التجريم** :جاء في نص المادة 72من نفسه على أنه "يعاقب بالحبس من سنة 01 إلى ثلاث سنوات 03 وبغرامة من 200.000 دج إلى مليوني دج أو بإحدى هاتين العقوبتين فقط كل من يؤدي خدمات التصديق الالكتروني للجمهور دون ترخيص أو كل مؤدي خدمات تصديق الكتروني يستأنف ويواصل نشاطه بالرغم من سحب ترخيصه تصادر التجهيزات التي استعملت لارتكاب الجريمة طبقا للتشريع المعمول به"[1].

2 -**الركن المادي للجريمة :**

يتضح من خلال نص المادة أن المشرع جرم قيام أية جهة غير مرخص لها من السلطات المختصة السلطة الاقتصادية حسب أحكام المادة 33[2] من ذات القانون، إصدار شهادات التصديق الالكتروني المعروفة بموجب الفقرة السابعة من المادة 02 من ذات القانون على أنها "وثيقة في شكل الكتروني تثبت الصلة بين بيانات التحقق من التوقيع الالكتروني والموقع.

كما أن ذات المادة جرمت استمرار الجهة المختصة بمنح شهادات التصديق الالكتروني بالرغم من سحب هذا الترخيص وبالتالي لقيام هذه الجريمة لابد من توافر الركن المادي والمعنوي.

وترتيبا على ذلك فإن جريمة إصدار شهادة التصديق الالكتروني من جهة لا تملك رخصة بذلك أو تم سحب الرخصة منها من الجرائم الشكلية التي يتطلب قيامها توافر السلوك الإجرامي فقط والذي يتمثل

[1]- المادة 72 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الالكترونيين، السالف الذكر.

[2]- أنظر المادة 33 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الالكترونيين، السالف الذكر.

في قيام جهة قبل الحصول على الترخيص وفق الإجراءات والشروط التي حددها القانون 15-04 خاصة المواد 33 وما يليها منه في إصدار شهادات التصديق الالكتروني أو الاستمرار في منح شهادات التصديق بالرغم من سحب الرخصة المخولة لمؤدي خدمات التصديق الالكتروني في الحالات التي حددها القانون.

3-الركن المعنوي

تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي،ويتألف القصد الجنائي من عنصرين هما :العلم والإرادة،فلعلم يقتضي إدراك الجاني لحقيقة النشاط الإجرامي وهو يتمثل في إصدار شهادة تصديق إلكتروني قبل الحصول على ترخيص بمزاولة النشاط من الهيئة المختصة،كما يتطلب القصد اتجاه إرادة الجاني إلى إصدار شهادة تصديق إلكتروني قبل الحصول على ترخيص أو سحبه،ولم يشترط القانون لقيام الجريمة قصدا جنائيا خاصا،بل يكفي توفر القصد العام القائم على العلم والإرادة .

ب-جنحة الإدلاء بإقرارات كاذبة للحصول على شهادات التصديق.

1-نص التجريم :

نص عليها المشرع الجزائري في المادة 66 على أنه "يعاقب بالحبس من ثلاث 03 أشهر إلى ثلاث 03 سنوات وبغرامة من عشرين ألف دينار20.000دج إلى مائتي ألف دينار 200.000دج أو بإحدى هاتين العقوبتين فقط، كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق الكتروني موصوفة"[1].

2-الركن المادي :

وعليه لقيام هذه الجريمة أيضا لابد من توافر الركنين المادي والركن المعنوي ويتحقق السلوك الإجرامي في هذه الجريمة في قيام الجاني بتقديم إقرارات كاذبة سواء لمؤدي الخدمات أو للطرف الثالث الموثوق باعتباره المسؤول عن منح شهادة التصديق.

وتعد الجريمة كغيرها من الجرائم الأخرى من جرائم السلوك المجرد وليست من جرائم الضرر، وبالتالي لا يشترط المشرع لقيام الركن المادي حلول ضرر معين أو تحقق نتيجة معينة، وإنما يكفي لقيامها تحقق النشاط أو السلوك الإجرامي وهو تقديم معلومات خاطئة وكاذبة[2].

3-الركن المعنوي:تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي،ويتألف القصد الجنائي من عنصرين هما :العلم والإرادة،فلعلم يقتضي إدراك الجاني

[1]- راجع المادة 66 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين السالف الذكر

[2]- عزيزة لرقط، مرجع سابق، ص 124.

لحقيقة النشاط الإجرامي وهو يتمثل في الإدلال بإقرارات كاذبة لأجل الحصول على شهادة تصديق إلكتروني،واتجاه إرادة الجاني إلى تقديم تصريحات كاذبة لأجل الحصول على شهادة تصديق إلكتروني.

ج- جنحة الإخلال بإخبار السلطة الاقتصادية عن التوقف:

-نص التجريم :

نصت المادة 67 من القانون رقم 15-04 على ما يلي: "يعاقب بالحبس من شهرين 02 إلى سنة 01 واحدة وبغرامة من مائتي ألف دينار 200.000دج إلى مليون دينار 1000.000دج أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الالكتروني اخل بالتزام إعلام السلطة الاقتصادية بالتوقف عن نشاطه في الآجال المحددة في المادتين 58 و59 من هذا القانون[1].

-الركن المادي:

وعليه تعد هذه الجريمة من جرائم السلوك الخطر يقوم ركنها المادي بمجرد اتخاذ مؤدي الخدمات موقف سلبي يتمثل في عدم إعلام السلطة الاقتصادية بالتوقف عن نشاطه المحدد حسب أحكام المادة 41 من ذات القانون وبالتالي فإن السلوك الإجرامي المكون للركن المادي يتحقق بامتناع الجهة المختصة المرخص لها إصدار شهادات التصديق الالكتروني عن الاستمرار في إصدار الشهادات دون إعلام السلطة الوصية بذلك سواء في الحالات العادية أو الحالات الاستثنائية المنصوص عليها في المادتين 58-59 من ذات القانون إلا أن المشرع من خلال المادة 67 المذكورة أعلاه نص على ضرورة القيام بدلك خلال آجال محددة إلا انه لم يحدد ذلك ترك المجال مفتوحا ويسأل عن هذه الجريمة صاحب الترخيص أي من تم منحه الترخيص بإصدار شهادات التصديق دون سائر العاملين لديه في الشركة أو الجهة[2].

-الركن المعنوي :تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي،ويتألف القصد الجنائي من عنصرين هما :العلم والإرادة،فلعلم يقتضي إدراك الجاني لحقيقة النشاط الإجرامي والذي يتمثل في عدم إعلام السلطة الاقتصادية بالتوقف عن النشاط واتجاه إرادة الجاني إلىإتيان كل من السلوك الإجرامي والنتيجة معا .

[1]- راجع المادة 67 من القانون رقم 15-04المتعلق بالتوقيع والتصديق الالكترونيين السالف الذكر.

[2]- عزيزة لرقط، مرجع سابق، ص 120.

الباب الثاني

الأحكام الإجرائية للحماية الجنائية للتوقيع الالكتروني

لقد ترتب على الثورة الحاصلة في مجال تكنولوجيا المعلومات ظهور بعض الصعوبات الخاصة بتطبيق قانون الإجراءات الجنائية على الكثير من جرائم الاعتداء على التوقيع الالكتروني، وإزاء الفراغ التشريعي أصبح سبيل للجناة إخفاء معالم جرائمهم ومحوها عن بعد ومن ثم فإن النجاح في إجراءات التحقيق في تلك النوعية من الجرائم بتوقف على مدى السرعة والسرية التي تتم بها هذه الإجراءات وهو ما يصعب حدوثه في ظل القواعد الإجرائية التقليدية.[1]

لذلك فإن الحماية الجنائية لجرائم التوقيع الالكتروني تمتد لتشمل فضلا عن القواعد الموضوعية للجريمة، الجوانب الإجرائية الملائمة لما تتسم به تلك الجرائم من خصوصية وإزاء قصور بعض القواعد الإجرائية التقليدية عن ملاحقة الظواهر الإجرائية المستحدثة ظهرت أهميته تحديث الدليل الجنائي الالكتروني، فمن ناحية يصعب في الكثير من الأحيان العثور على اثر مادي للجريمة والتي لا تكتشف إلا بمحض الصدفة، فضلا عن سهولة محو الدليل الالكتروني أو تدميره إضافة إلى ضخامة كم المعلومات في تلك الجرائم على نحو يزيد من صعوبة تتبع الجرائم الناشئة عنها.

غير أن الأمر لا يتوقف عن هذا الحد، إذ أنه من الضروري تتبع الدعوى الجنائية ابتداء من سلطات الضبط الجنائي وهو لا زال العقاب على الجاني وهو ما يتسنى تحديد القانون واجب التطبيق على تلك الجرائم وسلطة المحكمة في قبول الدليل الالكتروني في تلك الجرائم، ولذلك ظهرت أهمية التعاون الدولي لمكافحة تلك الجرائم والذي يتخذ صورا عديدة منها تسليم المجرمين ووضع الضوابط، والإجراءات الدولية التي تمثل قانونا عاما في هذا الصدد، فيستحيل على الدولة بمفردها القضاء على جرائم الاعتداء على التوقيع الالكتروني والتي ترتكب عبر الانترنت وذلك لأنها جرائم عابرة للحدود.وفي ضوء ما تقدم سوف نقسم دراسة هذا الباب إلى فصلين على النحو التالي:

الفصل الأول: الإجراءات التقنية للإثبات الجنائي في جرائم الاعتداء على التوقيع الالكتروني.

الفصل الثاني: التعاون الدولي لمواجهة جرائم الاعتداء على التوقيع الالكتروني

[1]- Matthew R. *Zakaras*, Revue *internationale* de droit pénal, 2001, p 821

الفصل الأول

إجراءات الإثبات الجنائي في جرائم الاعتداء على التوقيع الالكتروني

يعد إثبات الجريمةإلى فاعلها، هو الهدف الجوهري الذي تسعى إلى تحقيقه إجراءات الخصومة الجنائية منذ نشأتها بتحريك الدعوى الجنائية وحتى انقضائها بإصدار حكم نهائي في مواجهة شخص ما، ونضرا لتعدد الصعوبات التي تواجه جهات التحقيق في إثبات جرائم الاعتداء على التوقيع الالكتروني، يرى البعض أن اللجوء إلى وسائل الإثبات التقليدية لإثبات الجرائم التوقيع الإلكتروني يبدو أمرا صعبا فقد دفع ذلك بالكثير من الدول أن تصدر تشريعا إجرائيا ينظم الأدلة الالكترونية التي يمكن الركون إليها لإثبات تلك الجرائم مثل: التشريع الأمريكي فأدلة الإثبات الجنائي في جرائم الاعتداء على التوقيع الالكتروني متعددة فهناك تلقي البلاغات، المعاينة التقنية لمصلح الجريمة إضافة إلى ما يتبعه من تفتيش في نظم الحاسب الآلي كدليل الكتروني إلى الخبرة التقنية إضافة إلى إجراءات جمع الدليل المستحدثة من تسجيل أصوات التقاط الصور والتسرب، كما وقد ساهم التطور المذهل في علوم الحاسب الآلي في تجاوز الجريمة الحدود الجغرافية للدولة، فقد ترتب على الطبيعة التقنية الممتدة لشبكة الانترنت أن الاختصاص بالنظر في تلك الجرائم سوف ينعقد لأكثر من دولة هذا ما نتج عنه تنازع في اختصاص التشريعي والقضائي للنظر في جرائم الاعتداء على التوقيع الالكتروني.

وفي ضوء ما تقدم سوف نقسم هذا الفصل إلى مبحثين على النحو التالي:

المبحث الأول:الإثباتالجنائي في جرائم التوقيع الالكتروني

أدى سوء استخدام الفضاء الافتراضيإلى بروز جرائم مستحدثة تطلبت نوعا جديدا من الأدلة يسمى بالأدلة الرقمية أو الأدلة الالكترونية، تتفق وطبيعة الوسط الافتراضي الذي ارتكبت فيه الجريمة، فكان التحدي أمام المشرع الجزائري والمشرع المقارن ليس فقط تحديد هذه الأفعال بدقة ولكن إيجاد حلول للمشكلات المتعلقة بالدليل الالكتروني من حيث الوسائل المستعملة في ذلك وإجراءات الحصول عليه، سواء أكانت دليل تقليدي أو دليل حديث وهذا ما سنتناوله كالآتي:

المطلب الأول:الإجراءات التقليدية لجمع الدليل في جرائم الاعتداء على التوقيعات الالكترونية .

مما لاشك فيه أنه لا يوجد ما يسمى بالجريمة الكاملة مهما حاول إخفاءها، وذلك استنادا إلى قاعدة "لوكارد لتبادل المواد" التي تنص على انه"عند اتكاءك جسمين بعضهما ببعض فإنه لابد وأن ينتقل جزء من الجسم الأول إلى الثاني وبالعكس[1] وبالتالي ينتج عن هذا الاحتكاك ما يعرف بالدليل الجنائي"، وفي مجال الجريمة الالكترونية لدينا الدليل الالكتروني ولكي يتحقق هذا الدليل لإثبات هذا النوع المستحدث من الإجرام فانه لابد من جمع عناصر التحقيق والشكوى، أو تقديم هذه العناصر إلى سلطة التحقيق الابتدائي فإذا أسفر هذا التحقيق عن دليل توج معها إدانة المتهم وتقديمه إلى المحكمة.

إلاأن خصوصية جرائم الاعتداء على منظومة التوقيع الالكتروني وذاتية الدليل الالكتروني سيقودان دون شك إلى تغيير كبير إن لم يكن كليا في المفاهيم السائدة حول إجراءات الحصول على هذا الدليل،حيث تتعدد أدلة الإثبات الجنائي التقليدية في جرائم الاعتداء على التوقيع الالكتروني، وعليه سنتطرق إلى هذه الإجراءات التقليدية كآتي

الفرع الأول: تلقي التبليغات

يتطلب الكشف عن جرائم الاعتداء على التوقع الالكتروني إتباع استراتيجيات خاصة تتعلق باكتساب القائمين بجمع الدليل مهارات تقنية على نحو يساعدهم على مواجهة تطورات تقنية الحاسب الآلي وشبكاته، بحيث تتعقد وتتنوع التقنيات المرتبطة بارتكاب تلك الجرائم، حيث تتعدد أدلة الإثبات الجنائي التقليدية في جرائم الاعتداء على التوقيع الالكتروني،كتلقي التبليغات والشكاوى وهذا ماستناوله على النحو التالي :

[1]- سعيد سيد قنديل، مرجع سابق ، ص125

أولا: تلقي التبليغات والشكاوى في جرائم الاعتداء على التوقيع الالكتروني

أدى التطور التقني الهائل في مجال تكنولوجيات الإعلام والاتصال إلى إساءة استخدام هذا الفضاء الافتراضي، مما تنتج عنه أنماط جديدة للإجرام سواء من حيث الأساليب المستعملة أو نوعية الحياة أو أضاف المحني عليهم وهو ما دفع بالمجلس الأوروبي اتخاذ جملة من التدابير الإجرائية [1] في مجال مكافحة جرائم الاعتداء على التوقيع الالكتروني مثل استقبال الشكاوى والتبليغات عبر الانترنت وهذا ما سنتناوله في هذه الدراسة

أ- المقصود بآلية تلقي البلاغات والشكاوى:

تقصد بها مجموعة الإجراءات والمراحل التي تتم في دائرة البلاغات والشكاوى وتمر خلالها البلاغات والشكاوى بداية من استقبالها مرورا بدراستها والتحري حولها والتصرف فيها وفقا لتشريعات النافذة للتأكد من صحتها وتباشر الهيئات متلقية البلاغات والشكاوى من تلقاء نفسها التحري والتحقيق في جرائم الاعتداء على المنظومة التوقيع الالكتروني وتحليل مرفقاتها وإعطاء التوظيف القانوني لما تتلقاه من بلاغات وشكاوى وإعداد السجلات والاستمارات المنظمة لعملية تلقي البلاغات والشكاوى منتظمة البيانات الأساسية لكل منها شاملا مرفقاتها .[2]

اضافة إلى ذلك وإعداد نظام توثيق الكتروني لكافة البلاغات والشكاوى الواردة إلى الهيئة، وإعداد تقارير دورية عن البلاغات والشكاوى التي تلقتها الإدارة متبوعة بنتائج دراستها ومقترحات التعامل معها وانتهاء بمسابقة الإجراءات التي تمت شأنها وفي هذا الإطار نص الدستور المصري لعام 1971 في مادة 63، لكل فرد حق مخاطبة السلطات العامة كتابة وبتوقيعه إلا انه لم يرد بالقانون المصري تعريف صريح بمفهوم التبليغ عن الجريمة إلاأن قانون الإجراءات جاء به في المادة 25 " إن التبليغ الصادق عن الجرائم حق مقرر لكل إنسان".[3]

أما المشرع الفرنسي فقد قرر بموجب المادة 30 من قانون الإجراءات الجنائية الفرنسي "للمواطنين حق الإبلاغ عن الجرائم ولم يقرر جزاء على ذلك، أما القانون الإنجليزي فالقاعدة العامة هي أن البلاغ البوليس أمر متروك للفرد وهو واجب أخلاقي وليس قانوني ولعل هذه القواعد العامة تسري بشأن الإبلاغ عن جرائم

[1]- Christiane Féralschuhl, Cyberdroit, le droit à l'épreuve de l'Internet édition dalloz, 2009, p358.

[2] فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية ، دار الجامعة الجديدة ،الإسكندرية ، مصر، 2016 ، ص160.

[3]- حسام محمد نبيل الشراقي، مرجع سابق ، ص337.

التوقيع الالكتروني بإضافة للإبلاغ عن طريق استخدام شبكة الانترنت وفقا لنماذج التي تعدسلطات تلقي البلاغ لهذا الغرض.[1]

ب- الجهة المختصمة بتلقي الشكاوى والتبليغات

يكون من اختصاصات الضبط القضائي طبقا لقانون الإجراءات الجنائية تلقي البلاغات والشكاوى[2]،التي تبلغ إليهم أو التي يعينون بها بأية كيفية فقد يتم كتابيا أو شفويا ويصطلح على البلاغ في هاتين الحالتين "بالبلاغ المادي" وقد يقدم بواسطة البريد أو البرقية أو التليفون أو الصحف وهذا ما يصطلح عليه "بالبلاغ المعنوي" أو قد يقدم عن طريق الانترنت وهذا ما يسمى "بالبلاغ الرقمي" وعلى الضباط الشرطة القضائية أن يتخذوا جميع الوسائل اللازمة للمحافظة على أدلة الجريمة[3]

وطبقا لقانون الإجراءات والمحاكمات الجزائية رقم 18 لسنة 1960 والتي نصت على أن (تختص الشرطة بتلقي البلاغات عن جميع الجرائم وعليها أن تقوم بفحصها، وجمع المعلومات المتعلقة بها، وإثباتها في محضر التحري، ويقيد ملخص البلاغ وتاريخه فورا في دفتر يعد لذلك بمركز الشرطة، فإذا بلغ أحد رجال الشرطة أو علم بارتكاب جريمة فعلية أن يخطر فورا النيابة العامة في الجنايات، ومحققي الشرطة في الجنح بوقوع الجريمة، وينتقل إلى المحل الذي وقع فيه الحادث للمحافظة عليه، وضبط كل ما يتعلق بالجريمة ويفيد التحقيق وللقيام بإجراءات التي تقتضيها الظروف، وعليه أن يثبت جميع هذه الإجراءات في محضر التحري).

أما في القانون الفرنسي فينص على ذلك في المادة 18 من الإجراءات الجنائية (إذ يعتبر أن تلقي البلاغات يكون من اختصاص الضبطية القضائية).

وفي هذا الشأن نصت المادة 17 من قانون الإجراءات الجزائية الجزائري على أنه يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12-13 ويتلقون الشكاوى والتبليغات ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية، وعليه نجد أن المشرع الجزائري لم يحدد طريقة تقديم الشكوى من طرف

[1]-سعد أحمد محمود سلامة، التبليغ عن الجرائم، دراسة مقارنة، رسالة دكتورة أكاديمية الشرطة، القاهرة ، 2003، ص25.

[2]-راجع في ذلك نص 24 من قانون الإجراءات الجنائيات المصري والمادة 29 من ذات القانون فنصت المادة 24، يجب على مأموري الضبط القضائي أن يقبلوا التبليغات والشكاوى التي يرد إليهم شأن الجرائم وانم يبعثو بها فورا إلى النيابة العامة ويجب عليهم وعلى مرؤوسيهم أن يحصلوا على جميع الإيضاحات ويجروا المعاينة اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم أو التي يعلنون بها بأية كيفية وعليهم أن يتخذوا جميع الوسائل اللازمة للمحافظة على أدلة الجريمة.

[3]- فهد عبد الله العبيد العازمي، مرجع سابق، ص 15

الأشخاص المتضررين من الجريمة فقد تكون شفاهة، كما قد تكون مكتوبة وسواء كانت هذه الشكوى مقدمة من المضرور نفسه أو من محاميه[1].

أما البلاغات فتعني ما يرد إلى ضباط الشرطة القضائية من إخبار عن الجريمة سواء كانت شفاهة أو كتابة، بمعنى نقل العلم بوقوع حادث أو جريمة إلى السلطة المختصة بناءا على أسباب معقولة [2].

كما نصت المادة 18 من ق.ا.ج.ج على "يتعين على ضباط الشرطة القضائية أن تحرروا محاضر بأعمالهم وان يبادروا بغير تمهل إلى إخطار وكيل الجمهورية بالجنايات والجنح التي تصل إلى علمهم "[3]

لقد رأينا سلفا أن المشرع الجزائري لم يشترط وسيلة محددة من تلقي الشكاوى والتبليغات فقد تكون كتابة أو شفاهه بدليل تضمن نصت المادة 17 من قانون الإجراءات الجزائية لفظ.... ويتلقون الشكاوى والبلاغات وهو لفظ عام لم يحدد وسليه يحدد ذاتها مما يفتح المجال أمام القيام بهذا الأجراء " بأي وسيلة كانت ومنها استعمال تقنية الاتصال متمثلة في شبكة متمثلة في شبكة الانترنت والهاتف والخلوي..

واستكمالا للسياسة الجنائية للمشرع الجزائري في للمجال مكافحة الجريمة عموما والجرائم الالكترونية خصوصا " قامت قيادة الدرك الوطني بإنشاء وإطلاق خدمة عمومية جديدة عبر 48 ولاية باستعمال

باستعمال تكنولوجيا الإعلام والاتصال تحت اسم " الشكوى المسبقة والاستعلام عن بعد " حيث تدخل هذه الخدمة في إطار عصرية وسائل تنفيذ مهام وإحداث الدرك الوطني والتكفل الجيد شكاوى المواطنين، حيث يمكن هذا التنظيف المنجز من طرف مهندسي الإعلام الآلي لدرك الوطني المواطنين من إيداع البلاغات والشكاوى المسبقة عن طريق الانترنت وتأكيد لذلك تقوم وحدة الدرك الوطني في غضون 30 يوما مما يمكن أجهزة الضبطية القضائية من ربح الوقت والسرعة في البدء في إجراءات البحث والتحري عن الجرائم الإلكترونية .

ج- مكونات آلية تلقي التبليغات والشكاوى

ويتضح من المهام السابقة أن آلية تلقي البلاغات والشكاوى تتكون من المراحل التالية

- مرحلة الاستقبال والتوثيق بمحضر التحري

- مرحلة جمع المعلومات والأدلة.

[1]- يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في قانون العقوبات وقانون الإجراءات الجزائية والقوانين الخاصة، دار الجامعة الجديدة، الإسكندرية، مصر، 2019، ص 58.

[2]-مرجع نفسه ، ص59.

[3]م18 من قانون الإجراءات الجزائية الجزائري، المحدد بأمر 66-155 المؤرخ في 8 يونيو 1966 المعدل والمتمم.

- إحالة البلاغات والشكاوى إلى وكالات تطبيق القانون أو فرق العمل الخاصة المحلية أو الدولية وينبغي التنويه إلىإنالآلية لا تشتمل الإجراءات تجاه البلاغات والشكاوى، فهذه الإجراءات متنوعة بحسب نوع الشكوى أو البلاغ كما أنها متعددة منها جمع المعلومات وإجراء التحريات، ومنها التحقيق ومتابعة الإجراءات والجهات القضائية بعد انتهائها من التحقيق فيها كما أن جرائم الاعتداء على التوقيع الالكتروني ليست بمقدور أي شخص الإبلاغ عنها ما لم تتوافر لديه القدر على التعامل مع الجهاز الآلي أو نظم تقنية المعلومات[1] فالبلاغ عن الجرائم الانترنت قد يكون جوازي لأي بشخص علم بوقوع الجريمة أن يبلغ أو لا يبلغ مأموري الضبط القضائي سواء كان له مصلحة في ذلك أو لا يعكس الشكوى التي يجب أن تصدر من المتضرر أو من وكليه، خاصة وان هناك جهات تحجم من الإعلان والبلاغ عن هذه الجرائم خاصة البنوك والمؤسسات المالية خوفا من تزعزع ثقة العملاء بها أو قد يكون واجبا، وهذا ما أقرته لحنية خبراء مجلس أوروبا الإلزام بإبلاغ جهة خاصة والإلزام بإبلاغ سلطات إشرافية وتشكيل جهاز خاص لتبادل المعلومات، كذا إصدار شهادة امن خاصة.[2]

هـ- العناصر الأساسية لتحقيق في جرائم الاعتداء على التوقيع الالكتروني

يجب أن تتوافر في البلاغ والشكوى العناصر الأساسية اللازمة لتحقيق في الجريمة، كما يجب على المحقق أنيستظهر هو ما يلي

- إظهار الركن المادي:

أي النشاط والسلوك المادي في جرائم المنظومة التوقيعات الالكترونية ومعروفة هذا النشاط والمشروع فيه ونتيجته

-إظهار الركن المعنوي:

أي إظهار الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني

- تحديد وقت ومكان ارتكاب الجريمة:

[1]-فهد عبد الله العبيد العازمي، مرجع سابق ، ص162.

[2]-المرجع نفسه ، ص127.

تثير مسألة النتيجة الإجرامية في الجرائم الالكترونية مشاكل متعددة بخصوص مكان وزمان تحقق النتيجة الإجرامية وتثير أيضا إشكاليات القانون الواجب التطبيق لوجود يعدد دولي في هذا المجال ذلك أن جرائم التوقيع الالكتروني من الجرائم العابرة للحدود.[1]

- يجب على المحقق الجنائي أثناء القيام بالتحقيق مراعاة ما يلي :

- توفير معلومات مسبقة عن مكان وقوع الجريمة ومن المالك لهذا المكان ونوع وعدد الأجهزة المتوقع مداهمتها وشبكاتها التحديد إمكانية التعامل معها فنيا.

- الحصول على الاحتياجات الضرورية من الأجهزة والبرامج لاستعانة بها في الفحص والتشغيل.[2]

ثانيا: البيئة التي يتم من خلالها إجراء التبليغات والشكاوى في جرائم الاعتداء على التوقيع الالكتروني

نضرا الطبيعة الخاصة لجرائم الاعتداء على التوقيع الالكتروني يمكن القول بأنه " لتلقي الشكاوى والبلاغات عبر شبكة الانترنت أهمية بالغة في مجال مكافحة الجرائم على المستوى الإجرائي إذ يوفر اضباط الشرطة القضائية السرعة اللازمة في مباشرة إجراءات البحث والتحري بما يمكنهم من الكشف المبكر عن الجريمة ومرتكبيها وخاصة أن هناك إحجاما من طرف المتضررين في التبليغ عنها هذه الجرائم لأسباب عديدة قد تكون شخصية أو اقتصادية..الخ[3] ونضرا لما للبلاغ من أهمية في البحث الجنائي سارعت الدول إلى تطوير هذه الآلية تماشيا ومقتضيات العصر المتطور وذلك من خلال استحداث أجهزة.

-أجهزة تلقي التبليغات وشكاوى:

متخصصة لتلقي الشكاوى والبلاغات بواسطة شبكة الانترنت واتخاذ الإجراءات اللازمة للكشف عن الجريمة وملاحقة مرتكبيها ومن هذه المواقع نجد وزارة العدل الأمريكيةusdoj.go وموقع المباحث الفيدرالية Fbigov وموقع منظمة الانتزيولinterpol.int والمجلس الأوروبي col.govوأيضا موقع البلاغات للمخابرات المركزية الأمريكيةciaوكذلك منظمة الانترنت الأهليةIFCC.[4]

---

[1]-خالد ممدوح إبراهيم، مرجع سابق، ص218

[2]-فهد عبد الله العبيد العازمي، مرجع سابق ، ص166.

[3]-يزيد بوحليط، مرجع سابق ، ص316.

[4]-والذي أسسه مكتب التحقيقات الفيدرالي (FBI) والمركز الوطني لجرائم الياقات البيضاء (NW3C) في فرجينا الغربية بالو.م.أ،مناجل مكافحة ظاهرة الاحتيال عبر الانترنت.

-وفي فرنسا يتم الإبلاغ عن الجرائم الإلكترونية عبر الموقع الالكتروني لجهاز الشرطة الفرنسي Judiciaire gendarmerie défense. Gov. Frباعتباره الجهة المختصة بالتحقيق والتحري عن تلك الجرائم وموقع جمعية مزود الدخول وخدمات الانترنت

http://www.pointidecontact.net AFA

-وفي مصر يتم الإبلاغ عن الجرائم الإلكترونية عبر المواقع الإلكترونية لوزارة الداخلية عبر شبكة الانترنت www.moiegypt.gov.eg وموقع http//www.ccd.gov.eg[1]

ب- كيفية الإبلاغ وتلقي الشكاوي عبرالانترنت :

-أو عن طريق ملئ الاستثمار رقمية متواجدة في المواقع المتخصصة لتلقي تلك البلاغات والشكاوى بإرسال رسالة الكترونية إلى عنوان البريد لجهة التحقيق والتحري أو عن طريق ملئ استمارة الكترونية متاحة في مواقع البلاغات والشكاوى الرسمية والأهلية كموقع جمعية كمزودي الدخول وخدمات الانترنت AFA المنشأ خصيصا مع الحكومة الفرنسية في حملتها لمكافحة الإجرام عبر الانترنت

ويجب مليء استمارة البلاغ توضيح المعلومات الآتية

-تاريخ ورقت البلاغ

-المعلومات الخاصة بالمبلغ

-المعلومات المتعلقة بتفاصيل الواقعة

-نوع الجريمة وموضوع البلاغ

-ويجب على ملتقي البلاغ أن يعلم أن البلاغ هو مجرد تلقي لبعض المعلومات السريعة التي تمكنه من تحوير الجريمة بشكل مبتدئ.[2]

الفرع الثاني: التفتيش وضوابطه في جرائم الاعتداء على التوقيع الالكتروني:

لما كانت حريات الأفراد قد كفل لها القانون الحماية وكذا معظم دساتير الدول بعدة ضمانات وقام بتنظيمها بوضع العقوبات وتشريع الجرائم، ولما كان البحث عن الجرائم يستلزم الحصول على الأدلة وذلك سيلتزم بالتبعية القيام بالتفتيش وضبط الأدلة التي تفسد في الكشف عن الجرائم وتحديد مرتكبيها، فقد

[1]-فهد عبد الله العبيد العازمي، مرجع سابق، ص182.

[2]-حسام نبيل الشنراقي، مرجع سابق ، ص182.

واضح القانون كيفية ضبط الأدلة وشروطها، وذلك من خلال قواعد قانونية واضحة تطلب توافر ضوابط وشروط معينة لكل من التفتيش والأدلة وهذا ما سنتناوله في هذه الدراسة.

أولا- التفتيش في جرائم الاعتداء على التوقيع الالكتروني.

لما كان التفتيش اعتداء خطير على حريات وحقوق الإنسان التي كفلها له الدستور والقانون في كافة النظم القانونية، فقد عنيت التشريعات القانونية بتوضيح المقصود من التفتيش وضوابط

أ- المقصود بالتفتيش في البيئة الالكترونية

تضر الخطورة هذا الإجراء تكفل كل من الفقه والقضاء بمحاولة إعطاء تعريفات للتفتيش منها " إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون، يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بالغض النظر عن إرادة صاحبه[1]أو هو " هو إجراء من إجراءات التحقيق يهدف إلى البحث في مستودع السر عن أشياء تفيد في الكشف عن الجريمة المرتكبة ونسبتها إلى المتهم [2] كما عرفناه آخرون انه " الاطلاع على محل له جريمة للبحث عما يفيد التحقيق " [3] فالتفتيش ليس غاية في حد ذاته وإنما هو وسيلة لغاية تتمثل فيماي مكن الوصول من خلاله إلىأدلة مادية تسهم في بيان وظهور الحقيقة .[4]

ب- خصوصية التفتيش الواقع على منظومة التوقيعات الالكترونية

قد يتطلب التحقيق تفتيش شخص المتهم أو منزله قصد ضبط الأشياء المتحصلة من الجريمة وبالتالي فإجراء التفتيش قد ينصب على الكيان المادي للحاسوب وهذا لا يطرح أي مشكلة، ولكن تيار التساؤل حينما نكون يصدد تفتيش المكونات المعنوية فهي مجرد برامج وبيانات ومحررات الكترونية ليس لها مظهر مادي محسوس وهذا آثار جدل فقهي كبير وعلى هذا الأساس سنقوم ببيان هذا الجدل وكذا الضوابط التي يجب مراعاتها أثناء القيام بالتفتيش.

[1]-عبد الفتاح بيومي حجازي، مرجع سابق ، ص625.

[2] -أحمد عصام عجيلة، مرجع سابق ، ص406.

[3]-سليم علي عبده، التفتيش في ضوء قانون أصول المحاكمات الجزائية الجديد، دراسة مقارنة منشورات زين الحقوقية، بيروت، لبنان ، ط1 2006 ، ص25.

[4]-أحسن صادق المرصفاوي، أصول الإجراءات الجنائية في القانون ،بمنشأة المعارف ،الإسكندرية مصر ، 1982، ص 385.

ثانيا-مدى قابلية تفتيش المكونات المادية لتوقيع الالكتروني Hardware

يقصد بالمكونات المادية للحاسوب الأشياء الملموسة من أجزائه وأدواته التي تعمل بشكل متكامل لأداء مهمة فيمعالجة البيانات آليا [1]، وعليه يتكون الحاسوب عموما من إحداث أربعة وهي وحدات الإدخال ووحدات المعالجة ووحدات الإخراج ووحدات التخزين[2]، فوحدات الإدخال تتمثل في لوحة المفاتيح وشاشة اللمس ولنظام إدخال المرئي والصوتي، إضافة إلى وحدات الذاكرة الرئيسية التي تستخدم في الحفظ الدائم أو المؤقت لبيانات والمعلومات والبرامج كما تتمثل وحدات المعالجة في وحدة للتحكم أو وحدة المعالجة المركزية أما وحدات الإخراج فهي تتمثل في الشاشة والطابعة والراسم والأقراص المرنة والصلبة التي تعتبر، شهر تخزين البيانات والمحافظة عليها [3]،والواقع أن تفتيش المكونات المادية للحاسوب بأوعيته المختلفة بحثا عن الشيء الذي يتصل بجريمة الكترونية فقد وقعت بدخل في نطاق التفتيش، طالما تم وفقا للإجراءات المقررة قانونا كل ما هناك انه يتوقف حكم تفتيش تلك المكونات المادية على طبيعة المكان الموجود فيه " هل هو من الأماكن العامة أم من الأماكن الخاصة إذأن لصفة المكان أهمية خاصة في محل التفتيش فإذا كانت موجودة في مكان خاص كمسكن المتهم أو احد ملحقاته فلا يجوز تفتيشها إلا في المجالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونا في اغلب التشريعات كالقانون المصري، إلاأن القانون الجزائري قد خالف نصالمادة 64 من قانون الإجراءات الجزائية وأورد عليها استثناءات بموجب القانون رقم 06-22 المعدل والمتهم للأمور رقم 66-155 المتضمن قانون الإجراءات الجزائية ويتم وفقا لأحكام المادة 44 من ق.ا.ج.ج إذا يتطلب إذن مكتوبا من طرف وكيل الجمهورية أو قاضي التحقيق يستظهر عند دخوله المنزل كما يتضمن الإذن وصفا للجريمة موضوع البحث عن الدليل وحضور الشخص المعني وعليه يجب الانتقال إلى مكان تواجد جهاز الحاسوب أو احد مكوناته المادية [4]، فمن السهولة هنا ضبط جهاز الحاسوب ومكوناته وملحقاته وحجزها وتقديمها كدليل لإدانة المتهم، أما بالنسبة للاماكن العامة، فإذا وجد الشخص في هذه الأماكن وهو يحمل مكونات الحاسب السالفة الذكر أو كان مسيطرا عليها أو حائزا لها فإذا تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص ويتنفس الضمانات والقيود المنصوص عليها في هذا المجال.

[1]-يزيد بوحليط، مرجع سابق، ص 471.

[2]-هدى حامد قشقوش ، مرجع سابق، ص 28

[3]-يزيدبوحليط، مرجع سابق، ص 472.

[4]-المرجع نفسه، ص479.

ثالثا- مدى قابلية تفتيش مكونات الحاسب المعنوية في جرائم اعتداء على توقيع إلكتروني

لقد ثار خلاف تشريعي وفقهي بشأن مدى جواز تفتيش المكونات المعنوية للحاسوب تمهيدا لضبط الأدلة.

فذهب الرأي الأول إلى جواز تفتيش نظم الحاسوب ويستند في ذلك إلى عمومية نصوص التفتيش وذلك من خلال توسيع تفسير عبارة " ضبط " أنشئ لتشمل المكونات الحاسوب المادية وغيرمادية فمادة " 487" من قانون العقوبات الكندي تقضي مكانية إصدار أمر قضائي لتفتيش وضبط أي شيء تتوافر بشأنه أسس ومبررات معقولة تدعو للاعتقاد بأن جريمة قد وقعت أو يشتبه في وقوعها أو أن هناك نية لاستخدامه في ارتكاب جريمة أوانه تتيح دليلا على وقوع الجريمة [1]، وقد أخذت بعض التشريعات المقارنة بهذا الرأي ففي لوكسميورغ ينصرف معنى التفتيش إلى " كل الأشياء التي تكون مفيدة في إظهار الحقيقة " وكذلك القانون الإنجليزي الصادر في 29 يونيو سنة 1996 والذي يطلق عليه قانون الساعة استخدام الحاسب COMPUTER MISUSE A CTE[2] وعلى النقيض من ذلك هناك رأي آخر يري أنه إذا كانت الغاية من التفتيش المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم المادي لا ينطبق على الأدلة الإلكترونية، ذلك أن النبضات الإلكترونية أو الإشارات الالكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة وبالتالي لا تعتبر شيئا ماديا بالمعنى المألوف للكلمة وهو استجاب له المشرع الفرنسي وفقا لهذه المتغيرات وقام بتعديل نصوص التفتيش بالقانون رقم 545-2004 المؤرخ في 21 يونيو 2004 حيث قام بإضافة عبارة " المعطيات المعلوماتية " [3] في المادة 94 من قانون الإجراءات الجنائية الفرنسي لتصبح المادة على النحو التالي "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون مفيد ا لإظهار الحقيقة"

وفي مصر، فقد أدرج المشرع المصري مصنفات الحاسب الآلي من برامج وقواعد بيانات ومايماثلها من مصنفات تتعلق بحقوق المؤلف ضمن المصنفات المشمولة بالحماية والقانون وكذا تعديل مواد التفتيش بالمواد 26، 50منه بها يتناسب مع هذا الغرض لأن التقدم التقني قد تجاوز المفهوم التقليدي وهو المفهوم الذي أخذت به اتفاقية بودابيستفي شأن الجرائم الموقعة في 23 نوفمبر 2001 وذلك من خلال المادة 19 من

[1] -هلال عبد الله أحمد، تفتيش نضم الحاسب الآلي ونمانات المتهم المعلوماتي، ، دراسته مقارنة، دار النهضة العربية، القاهرة، مصر، 2006، ص 201.

2-Fer braches (David): A pathology of computer viruses Springer , verlage London,1992,p 233.

[3]- Article 94 du code de procedurepenalmodifé par loi n 2010 768 du 9 Juliet 2010, art,1 « les perquisitionssonteffectuéesdanstous les lieuxoù prevent se trouver des objects ou des donnéesinformatiquesdont la découverteserait utile à la manifestation de la vérité ،ou des biensdont la confiscation estprévue à l'article 131 – 21- du code penal ».

القسم الرابع حيث نصت على انه يجب على كل طرف أن يعتمد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لتمكين السلطات المختصة للبحث والوصول إلى نظام الكومبيوتر أو جزء منه أو المعلومات المخزنة به – الوسائط التي يتم تخزين معلومات الكومبيوتر بها ما دامت مخزنة في إقليمها[1]، ومما لا شك فيه أن المحررات الإلكترونية ككيان معنوي قد يكون محلا لهذه الإجراءات حيث يرتكز التفتيش على جمع معلومات تم تدوينها كمحررات الكترونية.

رابعا- مدى خضوع شبكات الحاسوب لتفتيش في جرائم الاعتداء على التوقيع الإلكتروني.

يظهرفي مجال الجرائم التي ترتكب باستخدام الشبكات بحيث يتم ارتكاب الجريمة عبر أجهزة الحسابات الآلية سواء الأخرى أو المتصلة بالحاسب الذي ارتكبت الجريمة في نظامه المعلوماتي وفي أماكن بعيدة عن الموقع المادي للتفتيش فقد يكون داخل اختصاص قضائي آخر أو حتى في بلد آخر.

ففي هذه الصورة يمكن التفرقة بين الفرضيات التالية

أ – اتصال حاسب المتهم بحاسب موجود في مكان آخر داخل الدولة:

أجازتبعض التشريعات المقارنة حلا لهذه المشكلة ففي الو. م. أ أجازت التوجيهات الداخلية الخاصة بإجراءات التفتيش أن يستند إذن التفتيش الصادر لمقر شركة معينة إلى فروعها الكائنة في نفس المكان وكذلك الحال بالسنة لكندا في المادة 1-2- a بمقتضى التعديل الصادر في 8 مارس 1996[2]

وقد نصت المادة 17 من فقرة أ من القانون الفرنسي رقم 39 2 لسنة 2003 بشان الأمن الداخلي الصادر 18 مارس 2003، بأنه يمكن لرجال الضبط القضائي أن يدخلوا من الجهاز الرئيسي على البيانات التي تهتم عملية البحث والتحري فنصت مادة 17 منه على انه " " يجوز لرجال الضبط القضائي من درجة ضباط وغيرهم من رجال الضبط القضائي أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم فيها التفتيش على البيانات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر مادامت هذه البيانات متصلة في شبكة واحدة من النظام الرئيسي أو يتم الدخول إليهاأو تكون متاحة المبدأ من النظام الرئيسي[3]، وتسمح الاتفاقية الأوروبية لجرائم الانترنت لعام 2001 لدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز كمبيوتر معين إلى غيره من الأجهزة المرتبطة به حالة الاستعجال، إذا كان

[1]-المادة 19 من القسم الرابع من اتفاقيةبوداسبت للإجرام المعلوماتي الموقعة في 23 نوفمبر 2001.

[2]-تنص المادة (a) (2. 1) على أنه " للقائم بتفتيش النظام وفقا لأحكام هذا الفصل أن يقوم بتفتيش أجهزة الكومبيوتر الأخرى المتواجدة في نفس المكان أو في نفس المبنى الذي صدر بخصوصه إذن بتفتيش الكومبيوتر المتواجد فيه لضبط وتفتيش البيانات التي تحتويها تلك الأجهزة أو البيانات المتاحة لهذه الأخيرة.

[3]- سعيد سيد قنديل، مرجع سابق، ص 143.

يتواجد به معلومات يتم الدخول إليها في هذا الجهاز من خلال الجهاز محل التفتيش وعلى العكس من ذلك فان هناك من التشريعات المقارنة مثل سويسرا وبلجيكا ما يقتصر إذن التفتيش على الأجهزة الموجودة في مكان محدد دون امتدادها إلى الأجهزة المرتبطة .[1]

ب- اتصال حاسب المتهم بحاسب موجود في مكان آخر خارج الدولة:

من الشبكات التي تواجه سلطات التحقيق في جميع الأدلة قيام بعض مرتكبي الجرائم بتخزين بياناتهم في نظم المعلومات خارج الدولة عن طريق شبكة الاتصالات البعدية وذلك لعرقله التحقيقات.[2]

وفي هذا الإطار صدر عن المجلس الأوروبي توصيات تجيز أن يمتد تفتيش الحاسوب إلى شبكة المتصل بها، ولو كانت تلك الشبكات تقع خارج إقليم الدولة، فتنص التوصية رقم 13 لسنة 1990 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات على أنه " لسلطة التفتيش عند التنفيذ تفتيش المعلومات وفقا لضوابط معينة تقوم بمد مجال تفتيش كمبيوتر معين يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة مادامت أنه من الضروري التدخل الفوري لقيام بذلك[3]، كما نصت المادة 2/19 من اتفاقية بودابيست التي تعالج التفتيش والضبط التي تعطي الدول بإمكانية التفتيش أو استخدام وسائل دخول مشابهة لبيانات الموجودة على أرض دولة أخرى وفي هذا الايطارأيضا نصت المادة 17 من فقرة 2 من قانون إلا من الداخلي الفرنسي " لمأموري الضبط القضائي أن يقوموا بتفتيش الأنظمة المتصلة، حتى ولو تواجدت في خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية [4]، وعلى المسار نفسه وبعدما نص المشرع الجزائري على تمديد التفتيش داخل الإقليم الوطني اتجه إلى تمديد تفتيش المنظومة المعلوماتية خارج الإقليم الوطني من خلال نص المادة 5/05 من قانون رقم 09-04 التي تنتصب على أنه " يجوز لسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي حالات المنصوص عليها في المادة 04 أعلاه " الدخول بغرض التفتيش ولو عن بعد... إلى...إذا تبين مسبقا بان المعطيات المبحوث عنها ولا يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع

[1] حسين إبراهيم، الحماية الجنائية لحق المؤلف عبر الانترنت رسالة دكتورة، دار النهضة العربية ،مصر، 2006 ص122.

[2] -هلالي عبد الله أحمد، مرجع سابق ص78.

[3] - سعيد سيد قنديل ، مرجع سابق 147.

[4] -Loi 18 mars 2003 pour la sécurité intérieure article 17/2:www le giframce ,gouv,frwaspd ,un textedeugorfnumjo 21/06/2020, على الساعة 14:30

خارج الإقليم الوطني فان الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.[1]

خامسا-ضوابط تفتيش الحاسب الآلي في جرائم التوقيع الالكتروني

تضمنت التشريعات الإجرائية على ضوابط معنية يجب إتباعها عند التعرض للحريات الشخصية بإجراء من الإجراءات الماسة بالحرية كالتفتيش وتنقسم الشروط العامة للتفتيش إلى نوعين من الشروط

أ- الشروط الموضوعية للتفتيش نظم الحاسوب:

يقصد بهذه الشروط بصفة عامة الضوابط اللازمة لإجراء تفتيش صحيح وهي في الغالب تكون سابقة وهي كالآتي:

1- سبب التفتيش في البيئة الالكترونية:

يتمثل هذا الشرط في وجود بجريمة على التوقيعات الالكترونية والتي يتمثل في كل فعل مرتبط باستخدام الحاسب الآلي لتحقيق أغراض غير مشروعة تمس التوقيعات الالكترونية وكذا تورط شخص أو عدة أشخاصفي ارتكاب جرائم التوقيع الالكتروني أو الاشتراك وكذا توفر دلائل قوية أو قرائن تفيد في الكشف عن المجرم المعلوماتي.[2]

- ففي مجال وقوع جريمة من جرائم التوقع الالكتروني سواء كانت جناية أوأجنحة فتجد إن المشرع الجزائري أدرج فصلا خاصا، الفصل السابع والخاص بجرائم السادس بأنظمة المعالجة الآلية للمعطيات كمار مد حماية جنائية لتوقيع الالكتروني من خلال قانون تنظيم الالكتروني رقم 15 سنة 2004 من خلال المادة 23 من ذات القانون أما باقي صور الإجرام الالكتروني لم يتعرض لها مما يتطلب تدخلا تشريعيا لسد هذا الفراغ ومواجهة هذه الصور المستحدثة للأجرام الالكتروني

- أما في مجال اتهام شخص أو شخص معنيين بارتكاب الجريمة والمشاركةفيها فينبغي أن تتوافر في حق الشخص المراد تفتيشه دلائل كافية تدعوا الاعتقاد بأنه قد ساهم في ارتكاب الجريمة سواء بوصفه فاعلا لها أو شريكا فيها.[3]

[1]- يزيد بوحيط ، مرجع سابق ، ص484.

[2] - حسام نبيل الشنراقي، مرجع سابق، ص 465.

[3]-فهد عبد الله العبيد العازمي، مرجع سابق ، ص262.

2- محل التفتيش:

محل التفتيش في الجريمة الالكترونية هو الحاسب الآلي ونظم معلوماته ومكوناته سواء المادية أو المعنوية بإضافة للأشخاص الذين يستخدمونه وقد سبق وان اشرنا إلى مكونات الحاسب الآلي المادية والمعنوية.

3- السلطة المختصة بالتفتيش:

بما أن التفتيش إجراءات من إجراءات التحقيق الابتدائي ومن اخطر الإجراءات التي تمس بحقوق وحريات الأشخاص عمدت معظم التشريعات المقارنة إلىإسناده لجهة خاصة لكي يتم وفقا إجراءات محددة قانونا فنجد المشرع المصري نص بتصريح العبارة من خلال المادة 91 و602 من قانون الإجراءات الجنائية على أنالقاضي التحقيق إصدارإذن بتفتيش شخص أو مسكن المتهم بشروط معينة ونص المادة 206 امن ذات القانون على عدم جواز النيابة العامة بالتفتيش لغير شخص المتهم أو غير منزله إلاإذا توافرت دلائل قوية على حيازة الأدلة على الجريمة [1]، هذا معناه أن الأصل أن يقوم قاضي التحقيق أو النيابة العامة بإجراءات التفتيش غير انه يمكن لمأموري الضبط أن يقوم بذلك في حالتي التلبيس لجناية أو جنحة معاقب عليها بالحسب لمدة تزيد عن 3 أشهر والانتداب من قبل المحقق المختصفي هذه الحالة يجب أن يحدد مكان المراد تفتيشه والشخص أو الأشياء المراد تفتيشها أو ضبطها وفي هذا سياق نجد نص م 50 من قانون الإجراءات الجنائية المصري تنص على انه " لا يجوز التفتيش إلا للبحث عن الأشياء الخاصة بالجريمة الجاري جميع الاستدلالات بشأنها[2]،أما بخصوص المشرع الجزائري فنجد انه حدد بوضوح الجهة المختصة سواء في مجال الإذن بوضع ترتيبات المراقبة الالكترونية أو في مجال الدخول بغرض التفتيش منظومة المعلوماتية أو جزء فيها منها فنجد نص المادة 04/أ من قانون رقم 09-04 السالف الذكر " إذ يختص النائب العام لدى مجلس قضاء الجزائر يمنح ضباط الشرطة القضائية المتبني لهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته المنصوص عليها بموجب المادة 13 من نفس القانون إذن بتفتيش لمدة ستة أشهر قابلة لتجديد إلى تمسح باللجوء إلى المراقبة الالكترونية [3]، فيما عدا هذه الحالة الخاصة وبموجب نص م 05 من القانون 09-04 " يجوز لسلطات القضائية المختصة وكذا الشرطة القضائية.... الدخول بغرض التفتيش " إذ يتعين الرجوع إلى المادة 37 من ق.ج.ج، سواء بالنسبة لوكيل الجمهورية أو قاضي التحقيق بموجب المادة

[1] -حسام محمد نبيل الشنراقي، مرجع سابق ص 459.

[2] -سعيد السيد قنديل، مرجع سابق ، ص 150

[3] -المادة 04 من قانون رقم 09- 04 ، السالف الذكر.

40، الذين ينصان على تحديد الاختصاص لكل من وكيل الجمهورية أو قاضي التحقيق في جرائم محددة من نيتها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

ب- الشروط الشكلية لتفتيش نظم الحاسوب في جرائم الاعتداء على التوقيع الالكتروني

بإضافة إلى الشروط الموضوعية لصحته إجراء التفتيش نظم الحاسوب وشبكة الاتصال الخاصة به هناك شروط أخرى ذات طابع شكلي يجب مراعاتها، وهذه الشروط تتمثل في ما يلي

- الحضور الضروري لبعض الأشخاص أثناءإجراء التفتيش في البيئة الالكترونية

بالنسبة لتفتيش الأشخاص لم يشترط التشريعات الإجرائية لصحة حضور شهود عند تفتيشهم أما فيما يتعلق بتفتيش المساكن وما في حكمها نجد المشرع المصري قد اشترط حضور شاهدين في حالة ما إذا كان التفتيش يباشر بمعرفة احد مأموري الضبط القضائي المادة 51 من قانون الإجراءات الجنائية المصري، والملاحظة في هذا السياق أم المشرع الجزائري ومن خلال التعديل الذي أجراه على قانون الإجراءات الجزائية بموجب قانون رقم06-22من المادة 45 منه حيث استغنى المشرع عن ضمانه حضور الأشخاص المحددين في الفقرة

الأولى من هذه المادة في جرائم معنية منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات.[2]

- الميقات الزمني لإجراء التفتيش في الجرائم الالكترونية

يقصد بضمانة الميقات في التفتيش أن يجريه القائم خلال فترة زمنية عادة ما يحددها المشرع وذلك حرصا على تضييق نطاق الاعتداء على الحرية الفردية وحرمة المسكن في حين نجد بعض التشريعات الإجرائية تركت آمر تحديد ذلك الوقت القائم بالتفتيش ومن ثم يقوم في كل الأوقات سواء ليلا أو نهارا، ومن بين تلك التشريعات قانون الإجراءات الجنائية المصري،[3] وعلى العكس من ذلك نجد أن المشرع الفرنسي والجزائري يحظران تفتيش المنازل وما في حكمها في وقت معين وهو محددفي القانون الجزائري من الساعة

[1]-مادتان 37 و40 من قانون الإجراءات الجزائية من الأمر رقم 66-155 المؤرخ في 23 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم من القانون 07/17 المؤرخ في 27 مارس سنة 2017.

[2]-سعيد السيد قنديل، مرجع سابق، ص151.

[3]- المرجع نفسه، نفس الصفحة

الخامسة صباحا إلى الساعة ثامنة مساءا وذلك من خلال المادة 47 من إجراءات جزائية[1]،إلا أن هناك حالات استثنائية يصح فيها إجراء التفتيش ليلا أو نهارا كجرائم المنظمة وعابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة آلية للمعطيات وجرائم تبييض الأموال وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف ويلاحظ آن المشرع الجزائري عندما استثنى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من حظر التفتيش ليلا، يكون قد أدرك فعلا ميزة هذه الجرائم من حيث قابلية الدليل الالكتروني للمحو والتدمير.

- محضر التفتيش في الجرائم الالكترونية

بعد قيام جهات التحقيقات التفتيش في البيئة الالكترونية فلابد أن يترجم مجهودات هذه الآلية في محضر تثبت فيه ما تقر من إجراءات وماأسفر عنه التفتيش من أدلة وهذا الأخير يستلزم مجموعة من الضوابط الشكلية التي يستجوبها القواعد العامة في المحاضر عموما فضلا إن يقوم به شخص متخصص في الحاسوب والانترنت وكذا إحاطة فاضي التحقيق أو عضو النيابة بهذه المعلومات والمحاضر التي تم تحريرها.[2]

ويجب أن يصاغ باللغة العربية أوأن يترجم المحضر إلى اللغة العربية إذا كان محررا بلغة أخرى باعتبار أن اللغة العربية هي اللغة الرسمية ويجب أن يشتمل أيضا على اسم من قام بإجراء التفتيش وتاريخ التفتيش وساعاته، أسماء الأشخاص الذين حضروا التفتيش وتوقيعاتهم مع الحضر، ومن الأشياء التي ضبطت بيان المكان أو الشخص الذي تم تفتيشه [3]

خامسا: ضبط الأدلة في مجال الاعتداء على التوقيع الالكتروني:

عقب التوصل لأدلة الالكترونية في مسرح الجريمة الالكترونية، يجب أن يتم جمع تلك الأدلة بشكل فني وفق لنظم معينة حتى تكون لها حجة أمام القضاء وتجدر الإشارة أن الضبط قد يرد على عناصر معلوماتية منفصلة مثل الديسكات والاسطوانات الممغنطة وهذا لا يثير أي مشكلة قانونية عند القيام بالضبط ولكن الصعوبة تثار عند ما يلزم ضبط النظام كله أو الشبكة كلها، ذلك لأنها تحتوي على عناصر لا يمكن فصلها، وعموما عملية الضبط تتطلب مجموعة من المراحل.

أ-مرحلة جمع الدليل: تعتبر هذه المرحلة من أهم المراحل التي يلجا إلى جهات التحقيق لكشف عن الحقيقة حيث إتباع الإجراءات التالية من خلالها.

[1]- المادة 47 من إجراءات الجزائية الجزائري " لا يجوز البدء في تفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحا وبعد ثامنة مساءا إلاإذا طلب صاحب المنزل أو وجهت نداءات من داخل أو في الأحوال الاستثنائية المقررة قانونا.

[2] سعيد السيد قنديل، نفس المرجع، ص 154.

[3] فهد عبد الله العبيد العازمي، مرجع سابق، ص280.

- تسجيل كل ما يتم من إجراءات في ملاحظات

- مراقبة الشاشة وتحديد ما إذا كانت معلقة أو مطفأة

- تسجيل الموديل والرقم المتسلسل للجهاز

- إزالة أي أقراص مدمجة موجودة لتجنب تلف الأدلة

- تسجيل كل الأفعال المرتبطة بتلاعب بجهاز لحفظ الموثوقية في المعلومات ومثال هذه الأجهزة تسجيلات الصوتية، أجهزة الرد الآلي.

1- مرحلة نقل وتخزين الأدلة:

إن الإجراءات التي تتخذ يجب أن لا تضيف أو تعدل أو تتلف البيانات المخزنة على الحاسب أو المواد المبرمجة كون أنها تتأثر بالرطوبة والحرارة ومعرضة للصدمات التي تؤدي إلى تلفها لذا يجب اخذ احتياطات خاصة لنقلها كحزم البرامج والأجهزة التي يصدر عنها أشعةأو موجات كهرومغناطيسية في حزم مضادة لمجلات الكهرومغناطيسية كالورق والحقائق البلاستكية

تفادي ثني أولي أوخدش حاملات البرامج كالديسكات والأسطوانات المبرمجة والأشرطة[1]

وفي هذا الإيطار نص المشرع الجزائري في المادة 6 من قانون رقم 09-04 السالف الذكر " عندما ما تكتشف السلطة التي تباشر التفتيش في المنظومة المعلوماتية معطيات مخزنة.... يتم نسخ كل المعطيات اللازمة لفهمها على دعامة تخزين الالكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية وفي جميع الأحوال على السلطة أن تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظمات المعلوماتية وهو ما ذهبت إليه المادة 27 من ق ا.ج تحت عنوان ضبط المعلومات المخزنة والتي تنص " تلتزم كل دولة طرف يتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط معلومات تقنية وعمل نسخة من معلومات تقنية وكذا الحفاظ على سلامة تقنية المعلومات، وأيضاإعادة تشكيل هذه المعطيات بما يخدم التحقيق بشرط عدم المساس بمحتواها وفقا لنص 316 من قانون نفسه وهذا تحت طائلة العقوبات وفقا لمادة 85 من قانون إجراءات الجزائية بإضافة إلى وضع تدابير أخرى كمصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواد التي تكون محلا للجريمة [2]

[1]-حسام محمد نبيل الشنراقي، مرجع سابق، ص 524.

[2] -يزيد بوحليط، مرجع سابق، ص 488 -489

- **مرحلة تقديم الدليل**: ويعتبر تقديم الدليل إلى المحكمة آخر الخطوات اللازمة لإدانة المتهم وتتضمن هذه الخطورة طريقة التقديم، ومؤهلات الخبير وطريقة جمع وتحليل الدليل، ومدى إقناع النتيجة التي انتهى إليها الخبير، لعقيدة المحكمة سواء إدانة المتهم أو براءاته

الفرعالثالث: الانتقال والمعاينة في جرائم التوقيع الالكتروني

لما كانت المعاينة لها أهمية كبيرة في مجال الجريمة التقليدية بالمقارنة بإجراءات كشف غموض الجريمة الأخرى لما تبينه من تصور لكيفية وقوع الجريمة وجمع الآثار والأدلة المادية والتنسيق بين الأدلة إلاأن دورها في مجال جرائم التوقيع الالكتروني والمعلومات بوجه عام ليس له نفس الأهمية والقدرة على كشف غموض تلك الجرائم، وذلك لما للأخيرة من ضيعته لا مادية مما يقلل كثيرا من فرص الاستفادة من معطيات مسرح الجريمة المعلوماتية ويرجع ذلك إلى سببين أو لهما أن الجرائم التي يقع على نظم المعلومات أو بواسطتها قلما يتخلق عن ارتكابها آثار مادية وثانية أن عدد كبيرا من الأشخاص قد تردد وعلى مسرح الجريمة خلال الفترة ما بين ارتكاب الجريمة واكتشافها مما يتيح المجال للعتب بالآثار المادية أوإزالتها مما يشكك في الأدلة المتحصلة من المعاينة[1] لذا تتطلب معاينة مسرح الجريمة ذات الطبيعة التقنية مهارات واعتبارات خاصة لما لهذا الإجراء من أهمية في مسالة استخلاص دليل الجريمة وإثباتها ولذلك سنين على التوالي مفهوم المعاينة، مدى صلاحية مسرح جرائم التوقيع الالكتروني بمعاينة، الضوابط الإجرائية والفنية لا لمعاينة في البيئة الرقمية.

أولا :مفهوم المعاينة: لم يحدد المشرع المقصود بالمعاينة، الأمر الذي دعا الفقه للتصدي لتعريفها حيث عرفها البعض بأنها " رؤية بالعين لمكان أو شخص أو شيء لإثبات حالاته وضبط كل ما يلزم الكشف الحقيقة [2] ويمكن تعريف المعاينة التقنية بأنها " ملاحظة وفحص حسبي مباشر لمكان أو شخص أو شيء له علاقة بالجريمة حالته والكشف والتحفظ على كل ما قد يفيد في الكشف الحقيقة عن الجريمة ومرتكبها[3]، كما اعتبرها جانب من الفقه بأنهاإثبات مباشر ومادي لحالة الأشخاص والأمكنة ذات الصلة بالحادث عن طريق رؤيتها أن فحصها فحصا حسيا مباشر.[4] مما يعني من خلال المفاهيم والدلالات السائقة أن جوهر المعاينة هو الملاحظة وفحص حسبي مباشرة لمكان أو شخص أو شيء له علاقة بالجريمة واثبات حالته والكشف والتحفظ على كل ما يقيد في الكشف عن الحقيقة أو هذا ما أخذه المشرع الفرنسي وفق المواد 92-93 من

[1]-أيمن عبد الحفيظ، مرجع سابق، ص 222.

[2]حسام محمد نبيل الشراقي، مرجع سابق، ص 351.

[3] -ياسر محمد الكومي، الحماية الجنائية والأمنية لتوقيع الالكترونية، دراسة، مقارنة، رسالة دكتورة في القانون الجنائي، جامعة جلوان، مصر، ص225.

[4]-أيمن رمضان محمد أحمد، مرجع سابق، ص 282

قانون الإجراءات الجزائية الفرنسي جمع الأدلة المستمدة من الواقع LES INDICATION TIRES DES FAITSبمعنى أن الدليل على وجود الجريمةيعد النتيجة من الملاحظة المباشرة سواء من معاينة المحقق أو قاضي التحقيق،[1] في الأحوال التي تقضيها الضرورة، ذلك أن المبادرة بالانتقال إلى مكان الجريمة لمعيلاته وضبط ما قد يوجد به أشخاص وأشياء، من شأنها أن تؤدي إلى المساعدة في جمع الأدلة المترتبة على ارتكاب الجاني لجريمته، قبل أن تمتد إليها يد العبث أو قبل زوال معالمها وحسنا فعل المشرع الجزائري حينما عاقبى

المساس بمسرح الجريمة من كل شخص ليس له الصفة بموجب المادة 43 من ق. إ.ج.جوكذا فعل نظيره المشرع الفرنسي بموجب المادة 55 من ق.إج.ف.[2]

حيث كان الهدف هو الحرص على المحافظة على مسرح الجريمة من كل تصرف يؤدي إلى طمس أثار الجريمة

ثانيا- مدى صلاحية مسرح جرائم التوقيع الالكتروني لمعاينته:

بما أن جرائم التوقيع الالكتروني تتم في بيئة الكترونية فان معاينة هذه الجرائم يتطلب التمييز بين المسرحين الجريمة المرتكبة، الأول مسرح تقليدي يقع على المكونات المادية للحاسب الآلي وثاني مسرح الكتروني يقع داخل بيئة الحاسب الآلي أي على المكونات المعنوية لحاسب الآلي وهذا ما سنتناوله من خلاله هذه الدراسة.

أ-الجرائم الواقعة على المكونات المادية للحاسب

وهذا الجزء يتطلب من المحقق الانتقال إلى مسرح الجريمة والتحفظ السريع على مكونات الأجهزة الالكترونية بكافة مستحملاتها قبل العبث بها وهذا ما نصت عليه المادة 94 من إجراءات جنائية المصري على أن تقاضي التحقيق ان يأمر يضبط جميع الخطيات، والرسائل والجرائد والمطبوعات والبرقيات عند إجراء المعاينة، إلا انه اشترط أن يكون ذلك بإذن مسبب ولمدة لا تزيد عن ثلاثين يوما[3]، ولاشك أن التحفظ على تلك

---

[1]-يزيد بوحليط، مرجع سابق، ص 322.

[2]-حيث نص المادة 43 من (ق.إ.ج.ج) على " يخطر في مكان ارتكاب جناية على كل شخص لا صفة له، أن يقوم بإجراء أي تغير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية... وإذا كان المقصود من طمس الآثار أو نزع الأشياء هو عرقلة سير العدالة عوقب على هذا الفعل بالحسب من ثلاثة أشهر إلى ثلاثة سنوات وبغرامة من 1000إلى 10.000 دج

article 55(CPPF)dans les lieu ou un crime a 2t2 commis , il est interdit , sous peine de l'amende pr2vue pour les contra ventions de la quatrième classe a toute personne non habilitée , de modifier avant les permi2res opération de l'enquête judicaire l'état des lieux et d y effectuer des prélèvements quelconques ....

[3]-ياسر محمد الكومي، مرجع سابق، ص 128.

المكونات سواء تعلقت بالمكون المادي لتوقيع الالكتروني أو الحاسب، أو المخرجات الناتجة عنه أمر تنوعه تلك المادة لقاضي التحقيق الذي يجوزله أن يندب احد مأموري الضبط القضائي في مباشرة ذلك.[1]

ب- الجرائم الواقعة على المكونات الغير مادية أو بواسطتها:

ويفترض في القائمين بهذه المعاينة الإلمام الجيد بأجهزة الحاسب الآلي وبرامجه نظرا الآن التفتيش يتم داخل جهاز الحاسب نفسه ما يجوزله من بيانات وبرامج، كما يتم التفتيش في شبكة الانترنت نفسها عن طريق بيانات المتهم على الشبكة كولوج إلى البريد الالكتروني لمتهم أو معرفة حسابه على مواقع التواصل الاجتماعي وكلمة المرور الخاص به،[2] ونظرا لما تحتويه هذه العملية من صعوبات تحول دون فاعلية المعاينة أو فائدتها لقلة الآثار المادية التي قد تتخلف في هذه الجرائم أو كثرة المترددين على مسرح الجريمة يلزم القيام بمجموعة من الإجراءات لتغلب على هذه الصعوبات يمكن إجمالها كآتي

- الإعداد الجيد المعاينة لعدم شرب الأدلة وإتلافها
- اصطحاب الخبراء المتخصصين لمرافقة فريق التحقيقات
- ما تحتويه سلة المهملات من الأوراق الملقاة أو الممزقة وشرائط وأقراص الممغنطة

ثالثا-الضوابط الإجرائية والفنية للمعاينة في البيئة الرقمية

مراعاة الطبيعية التقنية لمسرح الجريمة الالكترونية، وضع الفقه الجنائي مجموعة من الضوابط الإجرائية والإرشادات الفنية الواجب إتباعها وذلك لان مسرح الجريمة الالكترونية يختلف مسرح الجريمة التقليدية

أ- الخطوات الواجب إتباعها قبل الانتقال إلى المسرح الجريمة الإلكترونية (الضوابط الإجرائية)

تجد الإشارة أن معاينة مسرح الجريمة الالكترونية يختلف عن غيره من الجرائم بسبب طبيعة الدليل الالكتروني غير المرئي والقابل للمحو، لذا ينبغي قبل الانتقال لمسرح الجريمة القيام بخطوات الآتية الضوابط الإجرائية:[3]

[1]-أيمن رمضان محمد أحمد، مرجع سابق ، ص274

[2]-محمد علي سويلم، مرجع سابق، ص 230.

[3]-خالد ممدوح إبراهيم، مرجع سابق 157.

- توفير معلومات مسبقة عن مكان الجريمة، نوع وعدد الأجهزة وشبكات الاتصال الخاصة بها قصد تحديد إمكانية التعامل معها

- الحصول على الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل

- قطع التيار الكهربائي عن موقع المعاينة لشل فاعلية الجاني في القيام بأي فعل من شانه التأثير أو محو أثار الجريمة

- إعداد فريق تفتيش من المتخصصين والفنيين

- إعدادالأمروالإذن اللازم لقيام بالتفتيش

ب-الخطوات الواجب إتباعهاأثناء المعاينة:

قصد نجاح المعاينة لابد من مراعاة الجوانب الفنية الآتية " الضوابط الفنية

- تصوير الحاسوب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانة مع التركيز على تصوير الأجزاء الخلفية للحاسوب وتسجيل وقت وتاريخ ومكان النقاط كل صورة.[1]

- العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام والآثار الالكترونية

- ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام

- عدم نقل أي مادة الكترونية من مسرح للجريمة قبل إجراء اختبارات.[2]

- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب الآلي ذات الصلة بالجريمة وذلك لرفع ومعاهدات ما قد يوجد عليها من بصمات

- إعداد خصلة للمعاينة والتفتيش بحيث تكون الخطو واضحة ومفهومه لدى أعضاء الفريق

- السيطرة على المناطق المحيطة بمسرح الجريمة عن طريق إغلاق الطرق والمداخل

- السيطرة على الدائرة المحيطة بمكان الحادث، بوضح دراسات كافية لمراقبة التحركات داخل دائرة ورصد من الاتصالات الهاتفية من وإلى الموقع، مع إبطال أجهزة الهاتف النقال

[1]-علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، مصر، 2001، ص 33.

[2]-عبد الناصر محمد محمود فرغلي، الإثبات الجنائي بأدلة الرقمية من الناحيتين القانونية والفنية دراسة طبيعية مقارنة، المؤتمر العربي الأول لعلوم ادلة الجنائية والطب الشرعي من 12 الى 14 نوفمبر 2007، رياض، السعودية، ص 17.

- تأمين مسرح الجريمة والسيطرة على جميع أركانه ومنافذه والتحفظ على الأشخاص الموجودين.[1]

الفرع الرابع: الخبرة التقنيةفي جرائم الاعتداء على التوقيع الالكتروني

يتخذ المحقق الجنائي العديد من الإجراءات والوسائل التي تساعده على التوصل للجناة في جرائم الاعتداء على التوقيع الالكتروني ولما كان لا يستطيع أن يقوم بذلك الإجراءات بمفرده فقد أجاز له القانون الاستعانة بأهل الخبرة من قبل جهاز للتحقيق عند التعامل مع هذه الجرائم تعد ضرورة مكة لما هذه الجرائم من طابع فني خاص وهو ما سنتناوله في هذه الجزئية من خلال.

أولا- تعريف الخبرة التقنية في جرائم الاعتداء الالكتروني على التوقيع الالكتروني:

تعرف الخبرة بانتا " إبداءرأي فني من شخص مختص في شان واقعة ذات أهمية في الدعوى الجنائية"[2]، وبمعنى آخر هي " تنقيب وبحث يرتبط بمادة لتطلب معارف علمية أو فنية خاصة لا لتوافر لدى المحقق أو القاضي "[3]، كما تعرف بأنها " الاستشارة الفنية التي يستعين القاضي المحقق في مجال الإثبات لمساعدته في تقييم الأدلة، دون المسائل القانونية التي يحتاج تقديرها إلى معرفة فنية ودايره لا تتوافر عضو السلطة القضائية المختص بحكم عمله وثقافته[4]، فالعنصر المميز للخبرة عن غيرها من الإجراءات كالمعاينة والشهادة والتفتيش هو الرأيالفني للخبير في كشف الدلائل أو تحديد قيمتها في الإثبات والذي يتطلب معارف علمية وفنية خاصة لا تتوافر سواء لدى المحقق أو القاضي.[5]

ثانيا- أهمية الخبرة التقنية في مجال جرائم الاعتداء على التوقيع الالكتروني:

يعتبر دور الخبير في جرائم الاعتداء على التوقيع الالكتروني تمديد الأهمية وذلك نظرا لتطور والتقدم وسائل شبكات الاتصال والحاسبات المرتبطة بها، بصورة يعتذر على المتخصص ملاحقتها واستيعابها لدرجة يمكن القول معها الآن انه لا يوجد خبير قادر على التعامل مع كافة أنواع الجرائم التي ترتكب بواسطتها وذلك لقلة معرفته الدقيقة في سائر أنواع الحسابات والبرامج والشبكات[6]، لذلك يجب أن يتوافر لدى خبراء الحاسب الآلي المتدين للتحقيق المقدرة الفنية والإمكانيات العلمية والفنية في المسالة موضوع الخبرة، ومما يعكس أهمية دور الخبرة انه كثير ما تشغل جهات التحقيق في جمع الأدلة الالكترونية بل وان المحقق في كثير

[1]- داود سليمان على الحمادي، أحكام جريمة التزوي الالكترونية، دار النهضة العربية، القاهرة، مصر، 2008، ص 183.

[2] - داود سليمان على الحمادي، مرجع سابق، ص 174.

[3]-يزيد بوحليط، مرجع سابق ، ص329.

[4]- عبد الناصر محمد محمود فرغلي، مرجع سابق ، ص24.

[5]- خالد ممدوح إبراهيم، مرجع سابق، ص 284

[6]-عمر بن يونس، الجرائم عن استخدام الانترنت، رسالة دكتورة، جامعة عين شمس، القاهرة، مصر، 2004، ص 121.

في الأحيان يدمر الدليل الفني نتيجة حق منه ومن ناحية أخرى يجب على المحقق الجنائي أن يحدد مهمته المختبر على وجه الدقة وكذا الميعاد الذي يجب عليه تقديم فيه تقريره فاصل أن يقوم الخبير بمهامه أما جهات التحقيق والضبط لكن لا مانع أن يتم ذلك في غيابهم [1] وللخصوم الحق في الحضور أثناء مباشرة الخبير مهامه، ويجوز له أن يمنعهم من الحضور متى كان ذلك مبرر كذلك فان هناك بعض المسائل التي يتعين تضمينها في مهمة الخبير المعلوماتي وهي

- إمكانية نقل أدلةالإثباتإلىأوعية أخرى دون تلف وكيفية النظام المعلوماتي عند الحاجة

- تركيب الحاسب أو الشبكة وأنظمة الفرعية التي يستخدمها والمكان المحتمل لأدلة الإثبات وشكلها وهيئتها [2]ويتعين في هذا الصدد أن يكون الخبراء مؤهلين على دراية كافية بالجوانب التقنية والفنية لقيام بتحقيق في جرائم الاعتداء على منظومة التوقيعات الالكترونية

1- خطوات انجاز الخبرة التقنية في مجال الاعتداء على جرائم التوقيع الالكتروني

- تعيين الخبير: وفي هذا الإطار نجد نص المادة 92 من قانون الإجراءات الجزائية الإماراتي يقولها " إن اقتضى التحقيق الاستعانة بطبيب أو غيره من الخبراء....[3]

أما المشرع المصري فقد نص صراحة من خلال المادة 85/ 1 من قانون إجراءات الجزائية المصري بقولها " إذا استلزم إثبات الحالة الاستعانة بطبيب أو غيره من هذا الخبراء.....[4]

أما بالرجوع إلى المشرع الجزائري فنجده قد أجاز جهات التحقيق وللمحكمة تعيين خبراء سواء من تلقاء نفسها على طلب احد الخصوم حيث تنص المادة 143 من قانون الإجراءات الجزائية الجزائري على جهات التحقيق أو الحكم عندما يعرض عليها مسالة ذات طابع في أنتآمر يندب خبيرا إما بناءا على طلب النيابة إما من تلقاء نفسها أو الخصوم[5].

[1]-عبد الله حسين محمود، مرجع سابق، ص 120

[2]- أيمن رمضان محمد أحمد، مرجع سابق، ص 284

[3]-داود سليمان علي الحمادي، مرجع سابق، ص 188

[4]حسام محمد نبيل الشنراقي، مرجع سابق ، ص 440 .

5- المادة 143 من قانون الإجراءات الجزائية الجزائري السالف الذكر.

- **حلف اليمين:**أوحيت جل التشريعات المقارنة وقيل قيام الخبير التقني بأعماله أداء اليمين نظرا بخطورة وحماسته مهامه في إطار المنظومة الالكترونية وفي هذا السياق نجد المشرع الجزائري اوجب لضمان صحة تقرير الخبير ونيل وثقة أطراف الدعوى أن يقوم الخبير يحلف اليمين.[1]

- **الخضوع لرقابة القضائية:** عندما يباشر الخبير مهمته فهو تحت رقابة قاضي التحقيق أو القاضي الذي أمره يا جراء الخبرة .

- **انجاز الخبير لأعمال الخبرة بنفسه**: لابد على الخبير أن يقوم بأعمال الخبرة بنفسه وفي حدود ما نصعليه أمر وحكم الندب وان يستجيب لطلبات التي يقدمها أطراف الخصومة مثل سماع أي شخص قادرا على إعطاء معلومات فنية.

- **إبداع الخبرة التقنية**: بعد انتهاء الخبير من أعماله التي كلف يقوم بإيداع الخبرة التقنية خلال المدة المحددة وتقديم ما توصل إليه خبرته من نتائج إلى القاضي المختص [2]

4- الخطوات الفنية التي تحكم انجاز الخبرة في مجال الاعتداء على جرائم التوقيع الالكتروني

للخبير التقني في جرائم الاعتداء على التوقيع الالكتروني أن يقوم بمجموعة من الإجراءات حتى تمكنه من الوصول إلى الدليل المادي حيث يمكن إجمال هذه الإجراءات فيما يلي

- تحديد وحصر المواقع الإلكترونية التي كان الاعتداء على التوقيع الالكتروني محلالها وتحليلها فنيا وصولا إلى كيفية إعدادها ونسبتها إلى مسارها الذي أعدت فيه وتحديد عناصر حركتها وكيفية التوصل إلى معرفتها ومن ثم التوصل إلى معرفة الجهاز الحاسب الآلي الذي صدر منه

- الانتقال إلى الجهة التي رخصت بإصدار التوقيع الالكتروني لبيان الشرائط الفنية التي اتبعت لإصدار التوقيع الالكتروني والوقوف على مدى التطابق الفني بين التوقيع الالكتروني المستخدم في ارتكاب الجريمة التوقيع الالكتروني الصحيح والكيفية الفنية التي من خلالها الاعتداء عليه والحاسب الالكتروني والوسائط الفنية المستخدمة في ذلك وهنا يجب على الخير عند قيامه سؤال الأشخاص ذوي العلاقة بجرائم الحاسب الآلي بإجراءات الآتية

- ترتيب النقاط المطلوب استيضاحها من قبل الخبير

[1] حيث تنص المادة 145 من (ق.ا.ج.ج) على " يحلف الخبير المفيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا امام ذلكم المجلس....."

[2] يزيدبوحليط، مرجع سابق، ص 283

- سماع الشهود واستجواب المقيمين من قبل المحقق وذلك في حضور الخبير التقني والذي يجوز له توجيه أسئلة فرعية أثناء الاستجواب[1]

5- سلطة المحكمة في تقدير رأي الخبير التقني عن جرائم الاعتداء على التوقيع الالكتروني

يرى جانب من الفقه أن القاضي يضل الخبير الأعلى،حتى ولو كانت المسالة في مجال الانترنت قد تعرض لها خبير الانترنت وأخذ القاضي برأيه، بل وانه وحتى في حالة رفض الأخذبرأي الخبير فان القاضي ليس ملزما بسلوك محدد كاستعانة بخبير آخر قدم تقريرا فنيا [2] فمحاكمته الموضوع لها كامل السلطة في تقدير القوة الدليلية لتقرير الخبير وهناك رأي آخر يجدد الإشارة انه وان كان للمحكمة سلطة تقديرية لتقرير الخبير إلاأن ذلك لا يمتد إلى مسائل الفنية فلا يجوز لها تقييدها، إلا بأسانيد فنية وهذا ما قضت به محكمة النقض في إرساء حدود السلطة التقديرية لمحكمته الموضوع " لا يجوز للمحكمة ان تحل نفسها محل الخبير الفني في مسالة فنية...."[3]

موقف الجزائري بخصوص الخبرة التقنية:

لقد نظم المشرع الجزائري إلى حد ما انجاز الخبرة الرقمية بما يتوافق وخصوصية الجريمة الالكترونية وصعوبة التحقيق فيها لذا حاول وضع نصوص قانونية تسهل وضع ترتيبات لإجراء الخبرة الرقمية وذلك على عدة مستويات

-فعلى مستوى تعيين الخير فنجد نص م 144 من ق.ا.ج.ج والتي يتبين لنا كيفية الاختيار الخبراء كما أسلفنا سابقا كما نجد نص المادة 5 من قانون رقم 09-04 المؤرخ في 5 أوت 2009 والمتضمن القواعد الخاصة لوقاية من الجرائم المتصلة بتكنولوجيا العلام والاتصال، والتي مفادها تسخير السلطات المكلفة بتفتيش كل شخص له داريه بعمل المنظومة المعلوماتية.

-أما على مستوى استثناء الهيئات نجدأن المشرع الجزائري نص على إسناد هيئات بكوادر مؤهلة تقوم بإجراء الخبرة الرقمية كإسناد المعهد الوطني للبحث في عالم التحقيق الجنائي [4]وإسناد قيادة الدرك الوطني

[1]-ياسر محمد الكومي، مرجع سابق، ص 283.

[2]- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، دار النهضة العربية، مصر، 1999. ص 144.

[3]-الطعن رقم 145 لسنة 1982 الجلسة المنعقدة بتاريخ 1982/1/24م.

[4]-المرسوم الرئاسي رقم 04-432 المؤرخ في 2004/12/29 يتضمن إنشاء المعهد الوطني لبحث في علم تحقيق جنائي

للمركز الوطني لمكافحة الجريمة المعلوماتية الموجود بئر مراد رأيين بالجزائر العاصمة وإسناد المعهد الوطني للأدلة الجنائية وعلم الإجرام[1]، تأهيلا عن توفير الوسائل الحديثة في مجال تكنولوجيا الإعلام والاتصال.[2]

الفرع الخامس: الشهادة الالكترونية في مجال الاعتداء على التوقيع الالكتروني

أن الشهادة تعد من إجراءات التحقيق التي يستعين بها المحقق في الوصول لحقيقة الإجرامي وجمع الأدلة وكشف غموضها، وهي تقوم على إخبار شفوي يدلي به الشاهد في مجلس التحقيق بعدد اليمين القانونية ولا تقل الشهادة في جرائم التوقيع الالكتروني أهمية عنها في الجرائم التقليدية وغالب ما يكون الشاهد في المنظومة التوقيعات الالكترونية من الفنيين ذوي الخبرة والتخصص في تقنيات وعلوم الآلي وهذا ما سنعالجه في هذه الدراسة من خلال العناصر آتية

أولا: مدلول الشهادة الالكترونية في مجال جرائم الاعتداء على التوقيع الالكتروني

يمكن تعريف الشهادة بصفة عامة بأنهاالأقوال التي يدلي بها غير الخصوم أما السلطة التحقيق أو القضاة بشأن جريمة وقعت[3] أما عرفها جانب آخر من الفقه على أنها " الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت، سواء كانت تتعلق ثبت الجريمة وظروف ارتكابها وإسنادهاإلى المتهم أو براءته منها.[4]

أما الشهادة الالكترونية: فهي تطلق على نوعية من الشهادة لا يكون فيها الشاهد حاضرا جلسته التحقيق شخصته، وإنما تتم عبر وسائل الكترونية أو رقمية.

أ- مدلول الشاهد المعلوماتي في جرائم الاعتداء الالكتروني على التوقيع الالكتروني

يعرف الشاهد في جرائم الاعتداء على التوقيع الالكتروني بأنه ذلك الشخص الفني صاحب الخبرة المعلوماتية والتخصص في تقنية وعلوم الحاسب الآلي، والذي تكون لديه معلومات أساسية وجوهرية أو هامة لازمة للدخول في نظام المعالجة الآلية للمعطيات أو البيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن

---

[1]-المرسوم الرئاسي رقم 183-04 المؤرخ في 26 جوان 2004 يتضمن إحداث المعهد الوطني لأدلة جنائية وعلم الإجرام لدررك الوطني وتحديد قانونية الأساسي رقم: 41 المؤرخ في 27 /2004/6 ص18.

[2]-في أيطار المجهودات المبذولة من طرف السلطة القضائية بالجزائر –بخصوص تدريب وتكوين ضباط الشرطة القضائية والقضاة في مجال البحث والتحري عن الجرائم الالكترونية اشرف خبراء من الاستخبارات المركزية الأمريكية وعملاء من مكتب التحقيقات الفدرالي على تكوين ورشات حول مكافحة الجريمة المعلوماتية لفائدة ضباط الشرطة القضائية والقضاة تهدف إلى اطلاعهم على أخر التكنولوجيات لمحاربة الجريمة، مقال منشور على الموقع الرسمي http://www.djazairess.com/alkhabarعلى الساعة 9:24 16 أوت 2020.

[3]-إبراهيم الغماز، الشهادة كدليل إثبات في المواد الجزائية، رسالة دكتورة، كلية الحقوق، جامعة القاهرة، مصر، 1980 ، ص30

[4]-يزيد بوحليط، مرجع سابق، ص 341.

أدلة داخله ويطلق على هذا النوع من الشهود مصطلح " الشاهد المعلوماتي وذلك تمييزا له عن الشاهد التقليدي[1]، ويشمل الشاهد المعلوماتي بهذا المفهوم عدة أقسام.

ثانيا: فئات الشاهد التقني في جرائم الاعتداء على التوقيع الالكتروني

ومن فئات الشاهد المعلوماتي:

أ- **مشغلو الحاسب الآلي**: وهم الخبراء الذي تكون لهم الدراية التامة بتشغيل جهاز الحاسب الآلي والمعدات المتصلة به استخدام لوحدة المفاتيح في إدخال البيانات وتكون لديهم معلومات عن قواعد كتابة البرامج

ب- فئة المحلل: هو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين وتحليلها إلى وحدات منفصلة واستنتاج العلاقات الوظيفية منها، يقوم كذلك تتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات [2]

ج- المبرمجون: هم الأشخاص المتخصصون في كتابته البرامج ويمكن تقسيمهم إلى فئتين الأولى هم مخططو برامج التطبيقات والثانية هم مخططو برامج النظم [3]

د- مهندسو الصيانة الاتصالات: وهم المسئولين عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به [4]

هـ- مدير النظام وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية وقد نص المشرع الجزائري في هذا الخصوص ومن خلال نص المادة 5 من ق 09-04 المتعلق بقواعد الخاصة لوقاية من الجرائم المتصلة بتكنولوجيات الأعلام والاتصال أجاز لسلطات المكلفة بالتفتيش شخير كل شخص له داريه بعملاء المنظومة المعلوماتية[5]

ثالثا: التزامات الشاهد المعلوماتي في جرائم الاعتداء على التوقيع الالكتروني

[1]-خالد ممدوح إبراهيم ، مرجع سابق، ص 263.

[2]-حازم محمد جنفي ، مرجع سابق، ص 72.

[3]-محمد عمر بن يونس، مرجع سابق، ص 223.

[4]-عبد الله حسين علي محمود، مرجع سابق، ص 212.

[5]المادة 05 من قانون رقم 09-04 المتضمن القواعد الخاصة لوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السالف الذكر.

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج إلى نظام المعالجة الآلية للمعطيات سعيا عن أدلة الجريمة بداخله، لكن بالمقابل يثار التساؤل: هل أن الشاهد المعلوماتي ملزم يطبع ملفات البيانات المخزنة في ذاكرة الحاسوب ؟

أو هل يجوز له الإفصاح عن كلمات المرور السرية الخاصة بتنفيذ البرامج ؟

اختلف الفقه المقارن في الإجابة على هذا السؤال بين مؤيد ومعارض ويمكن بلورة هذا الاختلاف في اتجاهين رئيسين

أ- الاتجاه الأول:

ير ى أصحاب هذا الاتجاه انه ليس من واجب الشاهد وفقا للالتزامات التقليدية لشهادة أن يقوم بطبع ملف البيانات والإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة ويميل إلى هذا الاتجاه الفقه الألماني والتركي حيث يرى عدم ا لزام الشاهد المعلوماتي بهذا الالتزام [1] وفي فرنسا توجد بعض الفئات الممنوعة بنص القانون من الإفصاح عن بعض البيانات التي تكون بحوزتها مثل المحامين والأطباء متى تعلقت بأسرار مهنتهم ومن ثم فمتى كان تحت يدأي كان من هؤلاء مستند يحمل توقيعا مزورا متعلقا بسير من أسرار مهنته أو كان محلا للتلاعب، فلا يجوز إلزامه بتقديمه أو الشهادة بشأنها [2]

ب- الاتجاه الثاني:

يرى أنصار هذا الاتجاه أن من الالتزامات التي يجب أن يقوم بها الشاهد هي طبع ملفات البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة ففي فرنسا جانب من الفقه في غياب النص التشريعي يكون الشاهد مكلفا بالكشف عن كلمة المرور السرية التي يعرفها وشفرات تشغيل البرامج [3] ماعدا حالات المحافظة على سر المهنة وهذا ما أقرته المادة 18 من اتفاقية بودابست عام 2001 شأن جرائم الحاسب عندما ما ألزمت الغير ليس فقط بتقديم عساه يكون تحت يده، وإنما أيضا بالتحفظ والإفصاح عن بيانات المستندات الالكترونية التي يعتقد أنها محلا للتلاعب أو المحو والتي من شأنها الكشف عن الجريمة وتحديد هويته مرتكبها، وقد وضع المشرع الجزائري أمام الشاهد بصفة عامة كل الوسائل التي يمكنه من

[1] -يزيد بوحليط، مرجع سابق ، ص 346.

[2] -Francillon (Jacques) , Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France, Revue internationale de droit pénal, 1993.p309.

[3] هشام محمد فريد رستم، جرائم الحاسب الآلي كصورة من صور الجرائم الاقتصادية المستحدثة محلية الدراسات القانونية ،جامعة سيوط،لعدد،1 1990 ص117.

الإدلاء بشهادته دون زيارة أو نقصان وتحت طائلة العقوبات في حالة عدم الحضور أو رفضه لشهادة بعد تصريحه بمعرفة الجاني[1]

ثالثا: شروط التزام الشاهد المعلوماتي في جرائم الاعتداء على التوقيع الالكتروني

لا ينشأ التزام الشاهد بإعلام في جرائم الاعتداء على التوقيع الالكتروني إلاإذا توفرت ثلاثة شروط

أ:أن تكون جريمة من جرائم الاعتداء على التوقيع الالكتروني قد وقعت بالفعل سواء كانت جناية أو جنحة

ب:أن يكون الشاهد المعلوماتي على علم ومعرفة بالمعلومات المتصلة بالنظام المعلوماتي محل الواقفة

ج:أن تقتضي مصحة التحقيق الحصول على هذه المعلومات الجوهرية [2]

المطلب الثاني:إجراءات المستحدثة لجمع الدليل في جرائم اعتداء على التوقيع الالكتروني

ذكرنا سالفا من خلال الفرع الأول مجموعة من الإجراءات التقليدية للحصول على الدليل الالكتروني وتبين من خلالها من الصعوبات التي تخيط بها في ذلك نظرا كفايتها وفقا ليتها مما يسهل الكثير من المجرمين الإفلات من العقاب لذا أصبح من الضروري أن تواكب التشريعات المختلفة الطبيعية الخاصة لهذا الجرائم من خلال الاعتماد على وسائل متطورة وحديثة لكشف عن الجريمة والقبض على مرتكبيها وعدم إفلات المجرم من العقاب فمن هذا النوع المستحدث من الجرائم.

الفرع الأول: في مجال اعتراض وتسجيل بيانات المستند الالكتروني في جرائم الاعتداء على التوقيع الالكتروني

تعتبر هذه الإجراءات مكسباها لسلطات البحث والتحري في الكشف عن الجرائم المحددة قانونا ومنها جرائم التوقيع الالكتروني إذ يعتبر اعتراض وتسجيل بيانات المستند الالكتروني المتضمن التوقيع الالكتروني من أهم الإجراءات التقنية اللازمة لتعقب الدليل في جرائم الاعتداء على التوقيع الالكتروني والمحافظة عليه.

أولا: مفهوم اعتراض المراسلات:

[1]- المادة 98 من القانون الإجراءات الجزائية الجزائري، السالف الذكر.

[2]-هلالي عبد الله أحمد، مرجع سابق، ص 78.

يقصد باعتراض المراسلات انه إجراء تحقيقي يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطات القضائية في الشكل المحدد قانونا يهدف الحصول على دليل غير مادي للجريمة ويتضمن من ناحية إشراق السمع إلىالأحاديث ويتم بواسطة الوسائل السلكية واللاسلكية [1]

أ- المقصود بمضمون السجل الالكتروني محل الاعتراض:

هو ذلك البيان الذي يعد أداة لإثبات ما إذا كان الاتصال مشروعا من عدمه، كما لو انطوى على تهديد بارتكاب جريمة من جرائم الاعتداء على التوقيع الالكتروني، كما انه يمتد ليشمل أيضا كل بيان يفيد في تحصل دليل الكتروني في جريمة وقعت بالفعل أو بالأحرى يرجع وقوعها في فترة وخبيرة ويتعين وفقا لما تقدم أن يكون اعتراض محتوى المستند الالكتروني قد تم أثناء اتصال الالكتروني أو رسالة أو معلومة منقولة بواسطة الاتصال .[2]

ب- بيانات محتوى المستند الالكتروني المتضمن التوقيع الالكتروني

وفي هذا السياق نص المادة 8 من القسم الثامن عشر من القانون الأمريكي /2000

على تعريف تلك البيانات بأنها " البيانات أو المحتوى والمضمون الذي يتضمنه الاتصال الالكتروني وترتيبا على ذلك يمكننا القول أن جميع البيانات الجوهرية التي يتضمنها المستند الالكتروني والتي يكون محلا للاعتداء أو تلك التي يستخدم في تزوير التوقع الالكتروني أوإعداد برامج لإتلافه أو تعيله هي بيانات جوهرية يتعين على رجال الضبط ألزم مقدمي خدمات التصديق ومقدمي في خدمات الحاسب الآلي بتقديمها حتى يتسنى تحليلها والوصول من خلال الدليل الالكتروني المؤدي لإدانة المتهم في تلك الجرائم

وقد حرصت اتفاقية بودابست على تحويل السلطات التحقيق ذلك الحق من خلال بقي المادة 19 على تعويض سلطة التحقيق القيام بإجراءات اللازمة لضمان قيام سلطاتها بالبحث أو الدخول إلى المنظومة كمبيوتر فتصبح السلطات قادرة على توسيع عملية البحث بسرعة.

ج- بيانات تتعلق بالمشترك والمستهلك في المستند الإلكتروني المتضمن التوقيع الالكتروني

وهي تلك البيانات التي ورد النص عليها الفقرة الثانية من المادة من القسم الثامن عشر من القانون الأمريكي والتي من شأنها الوقوف على شخصية المشترك كاسم، عنوان موقف مجالات البيانات التي تقدم المشترك عند اشتراكه وتطبيقا لذلك اعتبر القضاء الأمريكي أن أي بيانات تخص المستهلك من شأنها الربط

[1]-يزيد بوحليط، مرجع سابق، ص 360.

[2]-أيمن رمضان محمد أحمد، مرجع سابق ، ص278.

بين المستند الالكتروني محل التزوير وشخصية مرتكبي الجريمة تساهم في تحديد المتهم في جريمة الاعتداء على التوقيع الالكتروني.[1]

د- موقف المشرع الجزائري من اعتراض المستند الالكتروني :

لقد اغفل المشرع الجزائري تعريف اعتراض المراسلات ولكنه بالمقابل اكتفى بتنظيم هذه العملية بموجب المادة 65 مكرر 05 من ق.ا.ج.ج " إذا اقتضت ضروريات التحري في الجريمة المتلمس بها أو التحقيق الابتدائي... في الجرائم الآلية للمعطيات....يجوز لوكيل الجمهورية أنأذن اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية وضع الترتيبات التقنية دون موافقة العينين، من اجل النقاط وتثبت وبث وتسجيل الكلام أو النقاط صور لشخص أو عزة أشخاص يتواجدون في مكان خاص[2].

أما بالرجوع لنص المادة 46 من التعديل الدستوري المؤرخ في 2016/3/6 والتي تنص " لا يجوز انتهاك حرمة حياة مواطن الخاصة وحرمة شرفة يحميها القانون، سرية المراسلات والاتصالات الخاصة.... وعليه يضمن الدستور بسرية المكالمات الهاتفية وكل الاتصالات بأشكالها المختلفة من التنصت والمراقبة والنشر أو الاطلاع أو الاعتراض تحت طائلة العقوبات، كما نص المشرع أيضا على سرية المراسلات بموجب المادة 105 الفقرة الأخيرة من القانون رقم 2000 – 3 المؤرخ في 2000/8/5 تحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية كما نص أيضا على سرية البيانات المتعلقة بالتصديق الالكتروني بنص المادتين 42-43من القانون رقم 15-04 المؤرخ في 2015/02/01 يحدد القواعد العامة لتوقيع والتصديق الالكتروني على مؤدي خدمات التصديق الالكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة شهادات التصديق الالكتروني الممنوحة.[3]

ثانيا: التدابير التقنية لاعتراض بيانات السجل الالكتروني

يلزم لاتخاذ اعتراض محتوى المستند أو السجل الالكتروني، اتخاذ بعض التدابير التقنية بغرض بتسيير عملية جميع المعلومات أو تسجيلها أو تأكيد لذلك نصت المادة 21 من اتفاقية بودابست على التدابير التقنية التي يجوز لسلطة التحقيق اللجوء إليها عند اعتراض محتوى بيانات السجل الإلكتروني.

-تجمع أو تسجيل البيانات من خلال لتطبيق واستخدام الوسائل الفنية على أراضي ذلك الدولة الطرفة بالاتفاقية.

[1]-أيمن رمضان محمد أحمد، المرجع السابق، ص 278.

[2]-المادة 65 مكرر 05 من قانون إجراءات الجزائية الجزائري السالف الذكر.

[3]-المادتان (42-43) من القانون رقم 15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين الجزائر السالف الذكر

-ألزم جهاز تقديم الخدمة المعلوماتية، في حدود قدرته الفنية بما يأتي.

-تجمع أو تسجيلمن خلال تطبيق واستخدام الوسائل الفنية والتعاون ومساعدة السلطات المختصة في تجميع أو تسجيل، مضمون البيانات وتسجيلها ويجب على تلك السلطة أن تتوخى السرية التامة عن اعتراض من مضمون البيان الالكتروني وذلك حفاظا على سرية البيانات التي تم اعتراضها ومؤدي ذلك أن الإفصاح عن تلك البيانات لا يكون إلا عندما تكون جريمة الاعتداء على التوقيع الالكتروني.[1]

ثالثا: السلطة المختصة بإصدارإذن الاعتراض

السلطة القضائية هي المختصة عموما بإصدار هذا الإذن ويعد ذلك ضمانة لازمة لمشروعية الاعتراض على الاتصالات السلكية واللاسلكية فيالقانون المصري حيث أنها ضمانة ضد أجهزة الدولة على حرمة الحياة الخاصة، ولا يشترط أن يقوم قاضي التحقيق أو النيابة العامة في حالة صدور إذن من القاضي الجزائي، بتنفيذ أمر الاعتراض، بل لهما أن يعهد ذلك لمأمور الضبط القضائي، إلاأن المشرع الجزائري خالف ذلك وأجاز لو كمل الجمهورية المختصة أن بإذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية وذلك في المادة 65 مكرر 05 م قانون الإجراءات الجزائية الجزائري.

رابعا: مدة الاعتراض

حرصت معظم التشريعات المعاصرة على تحديد مدة معنية للاعتراض منها من التعسف وإساءة استعمال السلطة، غير أن هذه التشريعات لم تنشر على وتيرة واحدة في شان هذه المراقبة فمنها من حدد المدة بأمد قصير كالتشريع المصري ،حيث حددها بثلاثين يوما قابلة للتجديد لمدة أو مدد أخرى مماثلة طبقا لتحديد الوارد في نص المادتين 90، 206 من إجراءات المصري، أما المشرع الجزائري فنص على مدة الإذن لمدة أقصاهاأربعة 4 أشهر قابلة لتجديد حسب مقتضيات التحري أو التحقيق وهذا ما نصت عليه المادة 65 مكرر 5 من ق.ا.ج.ج[2]

الفرع الثاني: في تسجيل الأصوات وإجراءات القيام به

[1]-هلالي عبد الله أحمد، مرجع سابق، ص 182

[2]-أيمن رمضان محمد أحمد، مرجع سابق، ص 190 .

يعتبر إجراء تسجيل الأصوات من الإجراءات الخفية مثل اعتراض المراسلات، الهدف منه تمكين أجهزة البحث والتحري من اكتشاف الحقيقة سنتناول أولا مفهوم تسجيل الأصوات ثم سنتطرق ثانيا إلى الإجراءات المتعلقة به

أولا:مفهوم تسجيل الأصوات " النقل المباشر والآلي لموجات الصوتية من مصادرها بنبراتها ومميزاتها الفردية وخواصها الذاتية بما تحمل من عيوب في النطق شريط التسجيل لحفظ الإشارات الكهربائية على هيئة مخطط مغناطيسي بحيث يمكن إعادة سماع الصوت والتعرف على مضمونه [1] وهي تلك المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة في مكان خاص أو عام، ويتم ذلك عن طريق حفظ الحديث على جهاز معد لذلك لاستمتاع إليه مرة أخرى [2] وفي هذا الإطار نجد أن المشرع الجزائري نص من خلال نص المادة 65 مكرر 05 قانون الإجراءات الجزائية الجزائري السابقة الذكر على تسجيل أحاديث المتهم [3] حيث أجاز المشرع وضع ترتيبات تقنية دون علم وموافقة المعنيين من اجل تسجيل الأحاديث في الأماكن العامة أو الخاصة حيث اخذ المشرع الجزائري بالمذهب الموضوعي حيث طبيعة الحديث أساس الحماية الجنائية بغض النظر عن المكان الذي أجرى فيه وهو المعيار الذي اخذ به المشرع الفرنسي أيضا [4]لما أن المشرع المصري تأثر بالقانون الفرنسي واصدر القانون رقم 37 لسنة عام 1982 بمقتضاه أضيف المواد 309 مكرر أ اعتنق من خلالها معيار المكان الخاص لتحديد طبيعة الحديث وإضفاء حماية عن المحادثات الخاصة ذلك انه يسبغ حمايته على المحادثات التي تدور في أماكن خاصة ويتطلب شر وطنا وإجراءات خاصة للاعتداء بالدليل المستمد من التسجيل لذلك من الأفضل تعديل هاتين المادتين على نحو يكفل الأخذ بطبيعة الحديث وبمكان صدور وسبب طبيعة الحديث فقط كالنهج الذي أخذ به المشرعين الفرنسي والأمريكي [5]

ثانيا: إجراءات الفنية لتسجيل الأصوات

تسجيل الأصوات من الناحية الفنية يمكن أن يتم بعدة طرق.

يتم تسجيل عن طريقأجهزة التسجيل السلكية واللاسلكية: هي أجهزة تعمل عن طريق إخفاء ميكروفون داخل المكان المواد سماع المحادثات التي تدور فيه وتوصيل هذا الميكروفون بواسطة أسلاك

[1]-ياسر محمد الكومي، مرجع سابق، ص 250.

[2]-حازم محمد حنفي، مرجع سابق، ص 74.

[3]-المادة 65 من قانون الإجراءاتالجزائية الجزائري السالف الذكر.

[4]-يزيد بوحليط، مرجع سابق، ص 370-371.

[5]-حازم محمد حنفي.مرجع سابق ص 128. 129.

دقيقة... التي غيرها من الأنظمة المستخدمة [1] ويتم تسجيل الأصوات طبقا لتشريع الجزائري بتسخير أعوان مصالح الاتصالات السلكية واللاسلكية سواء العمومية أو الخاصة لتكفل بالجوانب التقنية لعملية وهذا بموجب المادة 65 مكرر 8 إذن التسجيلات الصوتية الحديثة لها حجية كبيرة في الإثبات الجنائي لان التقنيات الالكترونية المتطورة لتسجيل لا تحتمل الخطأ، وبإمكان الخبراء كشف أي تعديل أو تلاعب بواسطة تقنية عالية الكفاءة

الفرع الثالث:التقاط الصور

إن عملية التقاط باعتبارها إحدى وسائل البحث والتحري الحديثة، هي استثناء عن المبدأ العام الذي يمنع التقاط الصور دون رضا صاحبها لما فيها من مساس بحرمة الحياة الخاصة المحمية قانونا ومن خلال هذه الدراسة سنقوم بتحديد

أولا: تعريفالتقاط الصور: لقد عرف جانب من الفقه الجنائي الصورة " بأنها امتداد ضوئي لحجم الإنسان وهي لسبب لها فكرة أو دلالة إلا الإشارة إلى الشخصية صاحبها [2]حيث أن التصوير المرئي " يعتمد على توثيق مشاهد متحركة ويقوم هذا الإجراء أساسا على استخدام الكاميرات أو أجهزة خاصة لالتقاط صورة للمشتبه فيه على الحالة التي كان عليها وقت التصوير بما تتخلله من صور حيث لحادثة معنية

ثانيا: أجهزة التصوير المرئي التي تستخدم في تسجيل الأحداث والجرائم هي

- التصوير المرئي بكاميرات السنيما والتلفاز
- التصوير المرئي بكاميرات الفيديو
- التصوير المرئي بالكاميرات الرقمية وهو ما يسمى بالكاميرات الديجيتال
- التصوير المرئي بكاميرات الهاتف الخلوي
- التصوير المرئي عن طريق أجهزة مراقبة وكاميرات خاصة
- التصوير المرئي بكاميرات السرية
- التصوير عن طريق القرصنة الالكترونية

ثالثا: موقف التشريعات المقارنة من الدليل الالكتروني المتحصل من التصوير المرئي

[1]-حازم محمد حنفي.مرجع سابق ، ص 130.

[2]-طارق سرور، مرجع سابق، ص310

- جرم المشرع المصري بموجب المادة 309 مكرر من قانون العقوبات تسجيل الأحاديث والنقاط أو نقل بجهاز من الأجهزة أيا كان نوعه صورة شخص في مكان خاص، حيث أجازت المادة 95 من قانون الإجراءات الجنائية " لقاضي التحقيق أو لقاضي الجزائي أن يقوم بإجراء تسجيلات لأحاديث تجري في مكان خاص

مما يعني حجية التصوير المرئي في الإثبات الجنائي تخضع لما تخضع له سائر الأدلة الجنائية الأخرى من ضرورة توافرها على المشروعية أي مشروعية الدليل الجنائي أما بخصوص إجراء التصوير المرئي في الأماكن العامة نجد نص المادة 21 من قانون الإجراءات الجنائية أجازت لجهات التحقيق القيام بتصوير المتهم حال وجوده في مكان عام [1]

- أما المشرع الجزائري فقد اعتبر عملية النقاط الصور الفوتوغرافية من الإجراءات الجديدة لمكافحة الجرائم المستحدثة ومنها الجرائم الالكترونية، غير انه ومثل الإجراءات السابقة لم يتطرق إلى تعريف هذا الإجراء، وإنما نص على محال تطبيقه وتوضيح إجراءات القيام به فبالرجوع لنص مادة 65مكرر05والاتجاه في فحواها " إذا اقتضت بأنظمة المعالجة الآلية المعطيات يجوز لوكيل الجمهورية المختص وضع الترتيبات التقنية دون موافقة المعنيين من اجل النقاط... في أماكن خاصة أو عمومية [2]

- وان منح الإذن للقيام بهاذ العملية حسب ما ورد في المادة 65 مكرر 5ق.ا.ج.ج مقتصر على وكيل الجمهورية أو قاضي التحقيق

وعلى خلاف تسجيل الأصوات التي تتم في أماكن عمومية أو خاصة واستثنى المشرع الجزائري النقاط الصور في الأماكن العمومية، غير انه سمح بهذا في بعض القوانين الخاصة كالترصد الالكتروني والاختراق بموجب المادة 56 من القانون 06 -01 المتعلق بالوقاية من الفساد ومكافحته [3]

أما عن المدة فقد نصت المادة 65 مكرر 7 ..... يسلم الإذن مكتوبا لمدة أقصاها أربعة 04 أشهر قابلة للتجديد حسب مقتضيات التحري أو التحري أو التحقيق فمن نفس الشروط الشكلية والزمنية.

- ذهب القانون العقوبات الفرنسي القديم بموجب المادة 2/367 المضافة بالقانون الصادر في 17 يوليو 1970 وبموجب المادة 227 /1 من القانون الفرنسي الجديد لسنة 1994، إلىأن التصوير يعد

[1]-حازم محمد حنفي، مرجع سابق، ص133.

[2]-راجع في ذلك المادة 65 مكرر 5 من (ق.ا.ج.ج)

[3]-تنص م 56 من رقم 06-01 المؤرخ في 20 /2/ 2006 المتعلق بالوقاية من الفساد ومكافحته على " من اجل تسهيل جمع الأدلة المتعلقة بالجرائم عليها في هذا القانون، يمكن اللجوء إلى التسليم المراقب أوإتباعأساليب تحري خاصة كالترصد الالكتروني والاختراق على نحو المناسب وبإذن من السلطة القضائية المختصة (ج ر) رقم 14 المؤرخة في 2006/03/08، ص 12

جريمة معاقب عليها من تم هذا التصوير في مكان خاص وتعبير رضا صاحب الشأن مما جعل هذا الدليل المتحصل عن طريق التصوير، دليلا غير مشروع وبمفهوم المخالفة فان التصوير الذي يجري في الأماكن العامة وبرضا صاحب الشأن يعد مشروعا والدليل المتحصل عنه دليلا صحيحا وقبولا، كما جرم قانون العقوبات الفرنسي في المادة 226/1 من الفقرة الثانية أفعال الاحتفاظ أو الإعلان أو التسهيل أو الإعلان للجمهور أو الغير والاستعمال علنا في السر، أي تسجيل تم الحصول عليه بأحد الطرق المبنية في النص السابق – هو ما يؤكد الحماية الجنائية الخاصة التي أضفناها المشرع الفرنسي على تلك التسجيلات المرئية ومن ثم فان الدليل المتحصل من طريق جريمة لن يعتد به في الثبات الجنائي.[1]

[1]-حازم محمد حنفي، مرجع سابق، ص 128

المبحث الثاني: الاختصاص في جرائم الاعتداء على التوقيع الالكتروني

لقد ساهم التطور المذهل في علوم الحاسب الآلي في تجاوز حدود الدولة، مما أصبح من الممكن أن ترتكب أفعال النسخ والبحث غير المشروع في دولة بينما يكون الجاني موجودا في دولة أخرى، هذا ما ترتب على أن الاختصاص بالنظر في تلك الجرائم سوف ينعقد لأكثر من دولة من بين الدول التي ارتكبت في إقليمها مما يؤدي إلى التنازع في قوانين تلك الدول، ومن ناحية أخرى يعتبر تحديد القضاء المختص بالنظر في الجرائم الاعتداء على التوقيع الالكتروني من أهم الصعوبات الحديثة التي أسفر عنها التعامل التقني للحاسب الالكتروني عن بعد، مما يؤدي إلى صعوبة تحديد المحكمة الجنائية المختصة بالنظر في فعل الاعتداء، كما وان دراسة سلطة المحكمة في تقدير الدليل الالكتروني تستلزم شروط مشروعة، ذلك أنه لا محل لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناء القاضي إلى حد الجزم واليقين.

وتطبيقا لذلك سوف نقسم دراسة هذا المبحث إلى مطلبين:

المطلب الأول: الاختصاص التشريعي والقضائي للنظر في جرائم الاعتداء على التوقيع الالكتروني

المطلب الثاني: سلطة القاضي الجنائي في قبول الدليل الإلكتروني لجرائم الاعتداء على التوقيع الالكتروني.

المطلب الأول: الاختصاص التشريعي والقضائي فينظرفي جرائم الاعتداء على التوقيع الالكتروني

يعتبر تحديد الاختصاص في مجال جرائم الاعتداء على التوقيع الالكتروني سواء كان اختصاص تشريعيا أم قضائيا من أهم الصعوبات الحديثة التي نتج عنها التعامل التقني لبرمجيات الحاسب الآلي ويرجع هذا السبب إلى تعقد شبكة الانترنت وتنوع طرق استخدامها من جهة ومن جهة أخرى تجاوز جرائم التوقيع الالكتروني الحدود الجغرافية للدولة كونها جرائم عابرة للحدود.

الفرع الأول:الاختصاص التشريعي بنظرفي جرائم الاعتداء على التوقيع الالكتروني.

سنعرض في هذا الفرع لمعايير الاختصاص التشريعي في جرائم الاعتداء على التوقيع الإلكتروني وتحديد القانون الجنائي الواجب التطبيق كون أن أفعال الاعتداء تمر بعدة دول، كما أن النتيجة غالبا ما تتحقق في عدة دول وما يصاحب ذلك من تعدد التشريعات الجنائية الواجبة التطبيق

أولا:مبدأ إقليمية النص الجنائي وجرائم الاعتداء على التوقيع الالكتروني

يعتبر مبدأ الإقليمية من أهم المبادئ التي تحدد الاختصاص القضائي والقانون الواجب التطبيقي عند ارتكاب أي فعل من نشأته الإضرار بمصالح الغير فبمجرد القاعدة القانونية فإن كل الأشخاص المحاطين بها

يخضعون لأحكامها دون استثناء ولا يجوز لأي منهم الاعتداء بجهله القانون وهذا ما يمثل نطاق تطبيق القاعدة القانونية من حيث المكان، وعليه يعد مبدأ إقليمية النص الجنائي هو من المبادئ المستقرة في قوانين كل دول العالم، وقد تم اعتماده في التشريعات الجنائية لكل الدول وعليه سنتطرق إلى دراسة هذا المبدأ من خلال.

أ-مفهوم مبدأ الإقليمية:

يقصد بمبدأ الإقليمية أن قانون العقوبات يبسط أحكامه على جميع الجرائم التي ترتكب على الإقليم الخاضع لسيادة الدولة، سواء كان مرتكب الجريمة وطنيا أو أجنبيا، فكل دولة تضع قوانينها الجزائية والجزائر كباقي الأمم تريد أن تخضع جميع الأشخاص الموجودين على ترابها لقوانينها، جزائريون كانوا أم أجانب، فالمادة الثالثة من قانون العقوبات.

تنص على أنه يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية[1]:"فمبدأ الإقليمية هو تطبيق قانون الدولة التي ارتكبت على إقليمها وداخل حدودها السياسية الجريمة، ونفاذ سلطات قضائها في متابعة ومحاكمة من ارتكب تلك الجريمة بغض النظر عن جنسية الجاني أو المجني عليه، أو نوع الجريمة المرتكبة وطبيعتها أو تصنيفها، كما لا يؤخذ بعين الاعتبار بالمصالح التي تعرضت للاعتداء ويمكن القول كذلك "أن مبدأ الإقليمية يطبق على الجرائم التي ترتكب داخل إقليم الدولة مهما كانت طبيعتها أو وصفها، فهو يتمتع بقدر كبير من الإطلاق والعموم.

ووفقا للرأي السائد في الفقه والقضاء الجنائي العربي والأجنبي، فإنه لا يشترط أن ترتكب الجريمة بكمالها داخل إقليم الدولة حتى يسري قانونها، إذ يكفي أن يتحقق أحد العناصر المكونة لها داخل هذا الإقليم، وبالتحديد يكفي أن يتحقق جزء من ماديات الجريمة أي النشاط أم النتيجة وهذا ما ينطبق على الجرائم المرتكبة عبر الأنترنت إذ يكون النشاط الإجرامي داخل دولة أما النتيجة الإجرامية تتحقق في إقليم دولة أخرى [2]

ب- إعمال مبدأ الإقليمية على جرائم الاعتداء على التوقيع الالكتروني وفق لتشريعات المقارنة:

نصت المادة 2/113 من القانون الفرنسي رقم 92/673 على تطبيق القانون الفرنسي على الجرائم المرتكبة على إقليم الدولة متى كان أحد عناصر الجريمة قد وقع على هذا الإقليم وقد نص المشرع المصري

[1]-بن شيخ حسين، مبادئ القانون العام، دار هومة لنشر والتوزيع، بوزريعة الجزائر سنة 2002، ص44.

[2]-عمار عبيد محمد الغول، نطاق تطبيق القانون الجنائي من حيث المكان وفق لمعطيات التكنولوجيا المعاصرة، رسالة دكتورة، كلية الحقوق، جامعة القاهرة ، 2006.ص15.

على هذا المبدأ في المادتين 1 و1/2 واللتان تطمئنا سريان القانون المصري على كل من يرتكب في القطر المصري جريمة من الجرائم المنصوص عليها فيه، وكل من يرتكب في خارج القطر فعلا يجعله فاعلا أو شريكا في جريمة وقعت كلها وبعضها في القطر فعلا يجعله أو شريكا في جريمة وقعت كلها، وبعضها في القطر المصري [1] وقد ساير المشرع الجزائري ذات النهج عندما أخذ بمبدأ الإقليمية من خلال نص المادة 3 من قانون العقوبات ينصها على "يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية "كما تنص المادة 586 من قانون إجراءات الجزائية الجزائري يقولها"تعد مرتكبة في الإقليم الجزائري كل جريمة تكون عمل من الأعمال المميزة لأحد أركانها المكونة بها قد تم في الجزائر " كما نصت المادة 585 أيضا "على كل من كان في إقليم الجمهورية شريكا في جناية أو جنحة مرتكبة من الخارج يجوز أن يتابع من اجلها ويحكم عليه يميزها بمعرفة جهات القضاء الجزائرية إذا كانت الواقعة معاقب عليها في كل القوانين الأجنبي والجزائري شرط أن تكون تلك الواقعة الموصوفة بأنها جناية أوجنحة ثبت ارتكابها بقرار نهائي من الجهة القضائية الأجنبية.أما في الجرائم ذات النتيجة والتي يمكن أن يتحلل الركن المادي فيها إلى عناصر ثلاثة هي العقل والنتيجة والعلاقة السببية التي تربطها كجرائم القتل فإن تحقق أي عنصر من هذه العناصر في إقليم أي دولة كاف لاعتبار أن الجريمة وقعت في تلك الدولة وبالتالي تكون محاكمتها صالحة للنظر في القضية على أن العقل يعد صالحا لتحديد الجريمة فلا حكم في الجرائم التي تقع على متن السفن كما نصت المادة 590 من ذات القانون " تختص الجهات القضائية الجزائرية بالنظر في الجنايات والجنح التي ترتكب في عرض البحر على البواخر والتي تحمل الراية الجزائرية أيا كانت جنسية مرتكبها..." كما نصت المادة 591 من نفس القانون " على انه تختص من الجهات القضائية الجزائرية ينظر في الجنايات والجنح التي ترتكب على متن الطائرات الجزائرية، أي كانت جنسية مرتكبها..[2] ومن خلال النصوص القانونية نستنتج ان المشرع الجزائري أخضع مبدأ إقليمية في جرائم الاعتداء على التوقيع الالكتروني وفقا لقواعد العامة.

كما ساير القضاء الأمريكي ذات النهج حيث طبقت محكمة واشنطن مبدأ إقليمية النص الجنائي في قضية سكوت ليفين والتي ارتكبت بعض أجزاءها داخل الدولة والبعض الآخر خارجها، حيث قضت بمعاقبته بالسجن 96 شهرا بتهم الدخول غير المشروع على برنامج الحاسب الآلي لعدد 120 عميل بشركة Little Rock والدخول غير المشروع على حساب اثنتين من العملاء والتسبب في عرقلة العدالة، وذلك باستثناءمكنة من فض مفاتيح التشفير الخاصة بتلك الشركة، والحصول على بيانات العملاء السرية لما يجاوز مليون عميل

[1] هدى قشقوش ، مرجع سابق.ص64.

[2] -راجع المواد 591.590.585.586 من قانون إجراءات جزائية جزائري.

وأرقام حسابهم وهواتفهم، ومحل إقامتهم وتمكن بذلك من الدخول على الحساب الخاص ببعض العملاء والامتلاء على أرصدتهم.

وفقا لمبدأ إقليمية النص الجنائي يجب تطبيق القانون رقم 04/15 على الجرائم التي تقع داخل النطاق الإقليمي لدولة بغض النظر عن جنسية مرتكبها، وسواء كان وطنيا أم أجنبيا، فقواعد قانون العقوبات تخاطب كل من تواجد في الإطار الإقليمي لدولة، ويلتزم بذلك احترام الأوامر والنواهي الجنائية وإلا تعرض لتطبيق العقوبة المقررة لمخالفتها ويستوي في ذلك أن تكون جريمة الاعتداء على التوقيع قد وقعت كلها داخل القطر الإقليمي، أم أن احد أجزاءها فقط هو الذي تحقق حتى ينعقد الاختصاص وإذا كانت جريمة الاعتداء على التوقيعات الالكترونية متتابعة الأفعال فيكفي في هذه الحالة أن يتحقق جزء من حالة الاستمرار وفقرة من فقرات التتابع ومثال ذلك تطبيق القانون المصري على الجاني الذي قام بإعداد برنامج بقصد إتلاف توقيع الكتروني أو الامتلاء على مستند الكتروني أو الدخول أو الإقامة غير المشروعة على نظام الحاسب الالكتروني، حيث أنها تعتبر من الجرائم المستمرة [1] وتطبيقا لذلك ما قضت به محكمة كاليفورنيا بمعاقبة سان ديجو أحد خبراء الحاسب الآلي بتهمة الدخول غير المشروع على قاعدة بيانات المستندات الالكترونية[2] فقد قضت المحكمة باختصاصها إقليميا لمجرد وقوع فعل من أفعال تتابع تلك الجريمة داخل الولاية بالرغم من إقامة أحد الفاعلين الأصليين خارج الولايات المتحدة وارتكابه أجزاء من السلوك المادي بالخارج.

كما أن الاختصاص بتطبيق قانون التوقيع الالكتروني 04/15 لا يقدم على الحالات التي يكون فيها الشخص فاعلا أصلا بل ينصرف أيضا إلى الحالات التي يساهم فيها باعتباره شريكا في جريمة من جرائم الاعتداء على التوقيع الالكتروني سيماوان اغلب جرائم التوقيع الالكتروني تتم من خلال تشكيل منظم يستهدف فالمساس بسرية المستند الالكتروني ويشمل إقليم الدولة الأراضي الإقليمية والمياه الإقليمية والقضاء الإقليمي والسفن والطائرات الجزائرية.

ثانيا: مبدأ شخصية القواعد الجنائية في جرائم الاعتداء على التوقيع الالكتروني.

يقتضي الإلمام بشخصية القوانين التطرق بتعريف المبدأ ومن ثم تطبيقاته في التشريعات المقارنة

[1]-تقابل ذلك المادة 586 من قانون إجراءات الجزائية الجزائري.

[2]-وتوصل من خلال ذلك إلى فك شفرة ورموز البيانات الخاصة تمهيدا لاستخدامها على نحو غير مشروع فتمكن هذا الأخير من الدخول على الموقع الالكتروني وتدمير البيانات الموجودة وتحويل المبالغ.

أولا: مفهوم المبدأ الشخصية.

يقصد بمبدأ الشخصية في جرائم الاعتداء على التوقيع الالكتروني سريان القانون الجنائي لدولة على كل من يحمل جنسيتها أيا كان مكان وجوده ولمبدأ شخصية النص الجنائي وجهان: إيجابي، فيعني، تطبيق القانون الجنائي للدولة على كل شخصا ينتمي إلى جنسيتها بصرف النظر عن مكان وقوع جريمته وأيا كانت جنسية المجني عليه في الجريمة ويعرف هذا المبدأ بمبدأ الشخصية الإيجابية أما الوجه السلبي فيعني.. سريان القانون الجنائي لدولة على كل جريمة يكون المجني عليه منتميا إلى جنسية الدولة ولو كان مرتكبا هذه الجريمة أجنبيا وارتكبها خارج إقليم الدولة وهذا ما يعرف بمبدأ الشخصية السلبية على أساس أن جنسية المجني عليه لا تبرر سلطة العقاب إلى الخارج [1].

ثانيا: إعمال مبدأ الشخصية النص الجنائي في جرائم الاعتداء على التوقيع الالكتروني وفقا لتشريعات المقارنة.

لقد أخذ المشرع المصري بمبدأ الشخصية القواعد الجنائية في المادة الثالثة من قانون العقوبات والتي تنص على "كل مصري ارتكب وهو في خارج القطر فعلا يعتبر جنائية أوجنحة في هذا القانون يعاقب بمقتضى أحكامه إذا عاد إلى القطر وكان الفعل معاقبا عليه بمقتضى أحكامه إذا عاد إلى القطر وكان الفعل معاقبا عليه بمقتضى قانون الذي ارتكب فيه.

ويستفاد من النص السابق توافر الشروط اللازمة لتطبيق القانون المصري على جرائم الاعتداء على التوقيع الالكتروني استنادا إلى مبدأ الشخصية وهي:[2]

1-أن يكون مرتكب جريمة الاعتداء على التوقيع الالكتروني حاملا الجنسية المصرية وقت ارتكاب الجريمة أو يستوي أن يكون الجاني حاملا لا كثر من جنسية طالما أن إحداها هي الجنسية المصرية.

2-أن تكون الجريمة المرتكبة من جنح الاعتداء على التوقيع الالكتروني المنصوص عليها في ق 2004/15.

3-أن يكون فعل الجاني معاقبا عليه وفق قانون البلد الذي ارتكب فيه ولا شك أن غالب التشريعات الأجنبية تعاقب على الاعتداء على التوقيع الالكتروني.

4-عودة الجاني إلى الإقليم المصري سواء عاد إلى القطر بإرادته أو مكرها.

[1]-حنان محمد حسن علي، مبدأ الإقليمية الجنائي في القانون والشريعة الإسلامية رسالة ماجستير، جامعة الخرطوم، السودان، 2008، ص24.

[2]-محمود محمد مصطفى، مرجع سابق، ص 123.

أما المشرع الجزائري نص على هذا المبدأ وفقا للإطار العام حسب المادة 582 من قانون الإجراءات الجزائية على أن "كل واقعة موصوفة بأنها جناية "معاقب عليها من القانون الجزائري ارتكبها جزائري خارج إقليم الجمهورية يجوز أن يتابع ويحاكم عليها في الجزائر غير أنه لا تجوز أن تجري المحاكمة أو المتابعة إلا إذا عاد إلىالجزائر، ولم يثبت انه حكم عليه في الخارج ويثبت في حالة الحكم بإدانة أنه قضى العقوبة أو سقطت عنه بالتقادم أو حصل العفو عنها.[1]

وفقا لهذا النص نستنتج مجموعة من الشروط لتطبيق هذه المادة وهي كآتي:

- يجب أن تكون الجناية منصوص عليها في القانون الجزائري والأجنبي.
- أن ترتكب الواقعة في الخارج.
- أن يكون الجاني جزائري سواء قبل وبعد ارتكاب الجريمة.
- عودة الجانب إلى الجزائر.
- عدم الحكم عليه في الخارج تطبيقا لمبدأ "عدم جواز محاكمة الشخص عن نفس العقل مرتين.

و يأخذ المشرع الفرنسي بمبدأ الشخصية في جانبه الإيجابي والسلبي فالنسبة لجانب تنص المادة 2/113 من قانون العقوبات على أن يطبق القانون الفرنسي على كل جناية يرتكبها فرنسي خارج الجمهورية، ويطبق هذا القانون أيضا على الجنح التي يرتكبها فرنسي خارج فرنسا إذا كانت الوقائع المكونة لها معاقب عليها في قانون الدولة التي ارتكبت فيها وتطبق هذه المادة حتى ولو كان المتهم قد اكتسب الجنسية الفرنسية بعد ارتكابه الواقعة السنوية إليه[2].

وقد طبق القضاء اليمنى مبدأ الشخصية النص الجنائي في قضية سرقة مبلغ مالية طائلة باستخدام الكمبيوتر من شركة كنديان نكس بتروليم حيث تمكن المتهمون في هذه الجريمة من سرقة مال منقول مملوك لتلك الشركة، بأن قام المتهم الأول الذي يعمل في الشركة باستخدام جهاز الكمبيوتر الخاص بأحد زملائه وفتح نظام الحوالات مستخدما كلمة السر الخاصة بزميله وكلمة السر المكملة الخاصة بالموظف الأجنبي، وسحب مبلغ ثلاثة مليون وأربعون ألف وستمائة وسبعة وعشرون دولار أمريكي من حساب الشركة المجني عليها من طرف بنك أوف أمريكا، وتحويلها على دفعات إلى عدة بنوك في ماليزيا إلى حساب المتهمين وقد تم تحويلها إلى البنوك في اليمن إلى حساب المتهم آخر حيث ارتكبت الأفعال المكونة لجريمة خارج إقليم

[1]-المادة 582 من قانون إجراءات الجزائية الجزائري، السالف الذكر.

[2]-أيمن رمضان محمدا حمد، مرجع سابق، ص372.

الجمهورية اليمنية وتحديد في دولة ماليزيا، إلا أنه وتطبيقا لمبدأ الشخصية النص الجنائي اختص القضاء اليمني بنظر في الدعوى حيث قضي بإدانة المتهمين [1].

ثالثا: مبدأ عينية القواعد الجنائية في جرائم الاعتداء على التوقيع الالكتروني.

يقتضي الإلمام بمبدأ عينية القوانين التطرق إلى تعريف وبيان شروطه وثم إعماله على جرائم الاعتداء على التوقيعات الالكترونية

أ:تعريف مبدأ عينية النص الجنائي.

يعني مبدأ عينية النص الجنائي تطبيق القانون الجنائي الوطني على كل جريمة تمس مصلحة أساسية لدول، أيا كان مكان ارتكابها، وجنسية من ارتكبها وبغض النظر عن كون العقل معاقبا عليه أو غير معاقب عليه في قانون الدولة التي ارتكبت فيها، وذلك يعني أن القانون الجنائي لدولة خلافا لما يقرره، مبدأ الإقليمية يمتد بشمل تلك الجرائم ولو وقعت خارج نطاقها الإقليمي ودون اعتبار لجنسية من ارتكبها، فهذا المبدأ يجعل الضابط في تحديد سلطان النص الجنائي أهمية المصلحة التي تهدرها الجريمة دون استلزام أي شرط آخر يتعلق بالمكان أو بالشخص الجنائي [2].

ب: شروط تطبيق مبدأ العينة

تتلخص شروط مبدأ العينة فيما يلي:

ج-المساس الجريمة بمصالح الدولة الأساسية.

أي أن المصلحة المعتدى عليها ليست مصلحة طردية خاصة بالفرد وإنما الأمر يتعلق بمصلحة خاصة بالدولة ذاتها وهي تمثل جوهر الدولة، ويمثل الاعتداء عليها اعتداء على ذات الدولة ومهددا لكيانها ووجودها وأمنها.

د-أن يكون الجاني أجنبيا.

يجب أن يكون الجاني أجنبيا، ويفترض القبض عليه داخل إقليم الوطني وان يتم تسليمه حسب إجراءات تسليم المجرمين [3].

[1]-أيمن رمضان محمدا حمد، مرجع سابق ، ص 380.

[2]-محمد نجيب حسني ، مرجع سابق.ص 133.

[3]-أحسن بوسقيعة، الوجيز في القانون العام، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2011، ص 111.

ر-ان ترتكب الجريمة خارج إقليم الدولة.

أي أن يكون هذا الاعتداء الذي مس المصالح الأساسية للدولة قد ارتكب خارج إقليمها وهذا المبدأ يعد أصله التاريخي في مبدأ الشخصية في وجه السلبي.

رابعا: إعمال مبدأ عينة الجنائية في جرائم الاعتداء على التوقيعات الالكترونية.

لقد وسع المشرع الفرنسي من نطاق مبدأ العينة حيث نفذ المادة 112 من قانون العقوبات الفرنسي على أن يطيق هذا القانون على الجنايات والجنح التي ترتكب خارج إقليم الجمهورية والتي تشكل اعتداء على المصالح الأساسية للأمة المنصوص عليها في الباب الأول من الكتاب الرابع من المواد 401-1414-9 من نفس القانون أما القانون الجزائري فقد نص على مبدأ عينة حسب المادة 588 من قانون الإجراءات الجزائية الجزائري " كل أجنبي ارتكب خارج الإقليم الجزائري بصفته فاعل أصلي أو شريك جناية أوجنحة ضد سلامة الدولة الجزائرية أو تزيينا لنقود أو أوراق مصرفية وطنية متداولة قانونا بالجزائر تجوز متابعته ومحاكمته وفقا لأحكام القانون الجزائري إذا القي القبض عليه في الجزائر أو حصلت الحكومة على تسليمه[1].

كما نجد المادة 15 من قانون 04/9 يقولها "تحت من المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون لمرتكبها أجنبي وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني [2].

فعدد ما يتم الاعتداء على المؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني من خلال جرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تكون الدولة الجزائرية عي المسؤولية لردع مثل هذه الاعتداءات.

خامسا: مبدأ عالمية النص الجنائي في جرائم الاعتداء على التوقيع الالكتروني.

تقتضي دراسة مبدأ عالمية النص الجنائي بيان مفهومه وتطبيقاته على جرائم التوقيع الالكتروني

أ: مفهوم مبدأ العالمية.

يقصد بهذا المبدأ أن يكون لكل دولة ولاية القضاء في أية جريمة يصرف النظر عن مكان وقوعها أو مساسها بمصالحها، أو جنسية مرتكبها أو المجني عليه فيها فجريمة الاعتداء على التوقيع الالكتروني تتطلب

[1]-المادة 588 من قانون إجراءات جزائية الجزائري السالف الذكر.

[2]-المادة 15 من قانون 09-04 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال السالف الذكر.

تطبيق مبدأ العالمية لأنه وبعد التطور الهائل في تكنولوجيا المعلومات والاتصالات أصبحت عمليات الدخول غير المشروع على أنظمة معالجة البيانات والمساس بالمحتوى الخاص بالمستند الالكتروني بتزويره أو إتلافهيمكن حدوثها خارج إقليم الدولة ومن أشخاص لا يحملون جنسيتها، غير أن آثار تلك الجريمة لا شك يمس بمصالح الاقتصادية لدولة أخرى [1].

ب: إعمال مبدأ عالمية النص الجنائي في جرائم اعتداء على التوقيع الالكتروني

لقد أخذ التشريع الفرنسي في المادة 113-10 بمبدأ عينة أو عالمية النص الجنائي في عدد معين من الجرائم الماسة بآمن وسلامة الدولة عن جهة وتزييف العملة المنصوص عليها في المادتين 442-443 من نفس القانون.

أما المشرع المصري لم يتضمن فما يتم الاعتراف بمبدأ عالمية النص الجنائي كأصل عام واستثناء من ذلك حدد المشرع المصري بعض الجرائم في الفقرة الثانية من المادة الثانية من قانون العقوبات وهذه الجنايات المذلة بآمن الدولة وجنايات التزوير وتقليد العملة وتزييفها والمنصوص عليها بموجب المواد 206.203.202، من قانون عقوبات المصري وقد ساير المشرع الجزائري ذلك النهج حيث أكدت المادة 588 اختصاص القضاء الجزائري بنظر جنح وجنايات امن الدولة وتزييف العملة إذا ما كان المتهم أجنبيا.[2]وكذا صدور قانون رقم 09.04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال حيث أثار في المادة 16 منه "يمكن في حالة الاستعجال ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل قبول طلبيات المساعدة القضائية، إذا ما وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس، أو البريد الالكتروني وذلك تقريرا لما توفره هذه الوسائل من شروط أمن كافية لتأكد من صحتها [3].

بإضافة على مصادقة الجزائر لعديد من الاتفاقيات كاتفاقية مع باريس لحماية الملكية الصناعية واتفاقية إنشاء المنظمة العالمية للملكية الفكرية الموقعة في ستوكهولم "1967 واتفاقية 2003 المتعلق بحقوق المؤلف وفيها اعتبر برنامج الحاسب مصنفة أدبي مكتوب.. إلى غيرها من الاتفاقيات.

الفرع الثاني: الاختصاص القضائي في جرائم على التوقيع الإلكتروني.

يعتبر تحديد القضاء المختص بنظر في جرائم الاعتداء على التوقيع الالكتروني من أهم الصعوبات الحديثة التي أسفر عنها التعامل التقني للحاسب الالكتروني عن بعد، ويرجع السبب في ذلك إلى أن تعقد

[1]-أحمد حسام طه، مرجع سابق، ص155.

[2]-أيمن رمضان محمد أحمد، مرجع سابق، ص367.

[3]-مادة 16فترة 2من قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة لتكنولوجيا الإعلام والاتصال السالف الذكر.

شبكة الانترنت وتنوع طرق استخدامها والطبيعة وخاصية لهذه الجرائم كونها تحدث في بيئة افتراضية واجتيازها لحدود الجغرافية التي ارتكبت فيها وتجرأ ركنها المادي وتوزعه على أكثر من مكان بحيث يمكن وقوع السلوك في مكان في حين تحقق النتيجة الإجرامية الضارة في نطاق إقليم دولة أخرى أدى إلى صعوبة تحديد المحكمة المختصة بنظر بمثل هذه الاعتداءات وعلى هذا الأساس ثار خلاف فهي وقضائي كبير حول تحديد المحكمة الجنائية المختصة بنظر في جرائم الاعتداء على التوقيع الالكتروني.

أولا: تنازع الاختصاص القضائي في جرائم الاعتداء على التوقيع الالكتروني.

ثار خلاف فهي وقضائي كبير حول تحديد المحكمة الجنائية المختصة في الجرائم بمنظومة التوقيعات الالكترونية على النحو آتي:

1: موقف الفقه والقضاء :

سنبين موقف الفقه والقضاء على النحو التالي:

أ-موقف الفقه.

لقد حاول الفقه حل مشكلة تنازع الاختصاص وانقسم إلى ثلاث اتجاهات.

-مذهب السلوك أو النشاط الإجرامي:

وفقا لهذا المعيار ينعقد الاختصاص للمحكمة التي يقع في نطاقها النشاط الإجرامي، ولسب بمكان حصول النتيجة أو الآثار المترتبة عليه، بدعوى أن اتخاذ آثار العقل كمناط لتحديد مكان وقوع الجريمة تكتنفه بعض الصعوبات، يمكن إجمالها في أنه معيار مرن وفضفاض فضلا عن أن معيار حصول النشاط ييسر عملية الإثبات وجمع أدلة الجريمة وان المحكمة التي لها ولاية النظر الدعوى تكون قريبة من مسرح الجريمة ناهيك أن الحكم يكون أكثر فعالية [1].

ويضيف المؤيدون لهذا الاتجاه حججا أخرى، منها أن حدوث الضرر في مكان معين مرده في الغالب أسباب لا إرادة لمقترف السلوك فيها، وأن من شأن تطبيق قانون الدولة التي تحقق في نطاقها الضرر لا يتفق واعتبارات العدالة نظرا لجهل الجاني بهذا القانون الذي يتم إعماله بحقه، وفي الغالب ليس ممكنا العلم به

[1]-صالح شين، الحماية الجنائية لتجارة الالكترونية دراسة مقارنة، رسالة دكتورة في الحقوق، جامعة ابوبكر بلقايد، تلمسان، 2013/2012.ص 244.

إذا حينما أقدم على ارتكاب العقل الذي أتاه يعتقد مشروعيته وفقا للقانون البلد الذي وقع فيه السلوك، وإذابه غير ذلك في قانون البلد الذي تحقق فيه الضرر [1].

-مذهب مكان تحقق النتيجة:

على الرغم من الحجج التي ساقها مؤيد والمذهب الأول، فإن هذا الاتجاه تعرض لجملة من الانتقادات من جانب آخر من الفقه، أبرزها أن هذا المذهب لا يعبر اهتماما للمكان الذي تحقق فيه الضرر الذي كان الجاني يسعى إلى تحقيقه، والآثار الضارة هي التي تعبث الفزع في نفوس الناس، في حسن أن مكان وقوع السلوك لا يعدوا وأن يكون مصدر الضرر لسبب ما، كما أن تمام الجريمة لا يكون إلا في المكان الذي ظهرت فيه 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 العقل أو درجة الخطأ، كذلك يعد حصول الضرر شرطا أساسيا لقيام المسؤولية المدنية فتنفي هذه المسؤولية بانتفاء الضرر [3].

لكن يؤخذ على هذا الاتجاه أنه لا يراعي مصلحة المتهم بجره إلى أماكن بعيدة للمحاكمة مما يؤدي إلى بطئ إجراءات التقاضي وإطالة الخصومة.

المذهب المختلط. أمام الانتقادات التي تعرض لها كل الاتجاهين السابقين، برز اتجاه ثالث يرى أن ينعقد الاختصاص للمحكمة التي يقع في نطاقها النشاط الإجرامي أي مكان حصول النشاط العمل التنفيذي،وكذلك المكان الذي تحققت فيه النتيجة أو الذي من المتوقع أو المنتظر تحققها فيه، وهذا الاتجاه حظي بقبول اغلب الفقه [4]. وهذا الاتجاه أخذت به بعض التشريعات المقارنة ومنها قانون العقوبات النرويجي، وكذا الدنمركي والألماني والإيطالي، كما تبنته المحاكم في بعض الدول ومنها فرنسا في عدد من الأحكام.

-و بالوقوف على المبررات التي استند إليها كل اتجاه، ترى أن الرأي الأخير هو الراجح لكونه تجاوز المآخذ التي اعترت المذهبين الآخرين، وفي الوقت ذاته استجمع ميزات كل منهما، فهو يوسع من نطاق الحماية

[1]-وقد حظي هذا الاتجاه بتأييد جانب كبير الفقه سواء في فرنسا أو مصر، لسبب هذا فحسب بل اتجهت إليه بعض التشريعات المقارنة ومنها القانون النمساوي والمجري.

[2]-صالح شين، مرجع سابق.ص243.

[3]-ومن المبررات التي سبقت لتقرير هذا الاتجاه أن الأخذ به يحقق وحدة الجريمة وعدم الفصل بين عناصرها، كذلك يمتاز هذا الاتجاه في نظر المدافعين عنه بأنه أكثر واقعية على اعتبار أن الضرر له مظهر خارجي ملموس خلافا للنشاط الذي قد لا يكون كذلك متى اتخذ صورة الامتناع، والسلوك السلبي.

[4]-ويجد مبرره في ان الركن المادي للجريمة يقوم على ثلاث عناصر وهي العقل (النشاط الإجرامي) والنتيجة والعلاقة السببية، ما يعني الجريمة تعد واقعة في كل مكان تحقق فيه علم من عناصر الركن المادي.

الجنائية ويتيح مرونة أكثر في مد نطاق الاختصاص لا سيما وأن بعض الأفعال مجرمة في ذاتها، ولا ينجم عنها أي ضرر مادي، ومنها ما تمتد أثاره الضارة لدولة أو دول أخرى غير التي وقعت فيها النشاط، الأمر الذي يحدد مصالحها الحيوية.

وينبغي إلا يترك لمحض اجتهادات الفقه والقضاء، وإنما يلزم تدخل المشرع لتحديد معايير الاختصاص التي يفر من عدم تضييق نطاقها بحيث يكون من الملائم أن ينعقد الاختصاص لقانون أي بلد أطرت به الجريمة، ومن المتوقع أن تشكل خطورة على مصالحه الحيوية، ولو كان مكان وقوعها خارج نطاق إقليمها[1].

ومن المناسب تبني مبدأ الاختصاص العالمي من أجل تجنب الكثير من المشاكل الناجمة عن تحديد مكان وقوع الجريمة أو ترتب آثارها الضارة [2].

ب-موقف القضاء من تنازع الاختصاص القضائي في جرائم الاعتداء على التوقيع الالكتروني.

القضاء الفرنسي:

قضت المحاكم الفرنسية باختصاصها ولو حدثت الواقعة في الخارج وتطبيقا لذلك قضت المحكمة الابتدائية بباريس باختصاص المحاكم الفرنسية، إذا كان مركز البث موجودا خارج الإقليم الفرنسي ويقوم الجهاز بينها في فرنسا فينعقد الاختصاص للمحاكم الفرنسية غير أنه يجب الأخذ بعين الاعتبار قاعدة التجريم المزدوج بين القانون الفرنسي وقانون الدولة التي صدر منها البث [3].

و خلاصة القول أن الجرائم المعلوماتية وخاصة جرائم الماسة بمنظومة التوقيعات الالكترونية لا تجدها حدود جغرافية خلافا لجرائم التقليدية "المعروفة"، الأمر الذي تجعلها في الكثير من الأحيان تستعصي على الخضوع للقوالب القانونية التي تحكم للمسألة الاختصاص المكاني ومن ثم فإن الطبعة الخاصة لهذا الصنف من الجرائم المستحدثة يتطلب تجاوز المعايير التي طرحها الفقه للتغلب على مشكلة تنازع الاختصاص.

-موقف القضاء الأمريكي.

لقد تصدى القضاء الأمريكي لمشكل الاختصاص القضائي المعلوماتي في أكثر من مناسبة، تشير التطبيقات القضائية إلى أنه يكفي لامتداد ولاية القضاء إلى جريمة وقعت في الخارج أن تكون آثارها قد مست بمصالح أمريكية أو عرضتها للخطر تأسيسا على مبدأ الاختصاص الشخصي، ومن ذلك ما قضت به محكمة

[1]-صالح شنين، مرجع سابق، ص 247.

[2]-حسام نبيل الشنراقي، مرجع سابق، ص 320.

[3]-أحمد حسام طه، مرجع سابق، ص237.

ولاية ميتوسيتا الأمريكية Minnesotaباختصاصها بنظر بكل جريمة تقع عبر الانترنت من لاس فيغاس بولاية نيفادا الذي وصل إلى ولاية مينوسيتا التي يحظر قانونها لأمثل هذه الألعاب، وتكرس هذا الاتجاه القضائي تطبيقا لمبدأ النتيجة الإجرامية ونجد كذلك قضية ريتشارد بنيميلي الذي قدم لمحكمة جورجيا لارتكابه جريمة التسبب عمدا في تعطيل برامج الحاسب الآلي وقطع الاتصالات الالكترونية من الولايات حيث قام خلال سنة 2006 عندما كان يعمل مستشارا لنظام الحاسب الآلي في شركة systèmesand serviceبإعاقة الموظفين عن أداء عملهم وهدد بشكل واضح بيانات المستندات الالكترونية وقد تسبب ذلك في خسارة قدرها 50.000 دولار [1].

موقف القضاء الإنجليزي:

تبنى القضاء الإنجليزي حلولا مشابهة بنظر في الدعاوى الناشئة عن إساءة استخدام الانترنت متى كانت ثمة ارتباط بين الواقعة المرتكبة وبريطانيا عملا بقانون إساءة استخدام الحاسوب الصادر سنة 1990 فلكي ينعقد الاختصاص للمحاكم الإنجليزية فيكفي امتداد آثار الواقعة إلى بريطانيا ولو كانت هذه الواقعة قد حدثت في الخارج، وبصرف النظر عن محل إقامة الجاني [2].

ثانيا: معاييرالاختصاص القضائي في جرائم الاعتداء على التوقيع الالكتروني.

نظرا لخصوصية جرائم التوقيع الالكتروني في البيئة الالكترونية وتجزأ كيانها المادي بوقوع السلوك الإجرامي في نطاق بلد معين وتحقق آثاره الضارة في نطاق بلد آخر أدى هذا إلى تنازع الاختصاص أي أن العقل يتنازعه قانونان، قانون دولة الإقليم على أساس مبدأ الإقليمية وفي الوقت ذاته يخضع لقانون دولة الجاني عملا بمبدأ الشخصية ليس هذا فحسب، بل قد ينعقد الاختصاص لدولة ثالثة متى كانت الجريمة ماسة بمصالحها الحيوية وفقا لمبدأ العينية ولتغلب على هذه الصعوبات أوجدت التشريعات معايير لتحديد الاختصاص القضائي فنحص بدراسة.

أ-موقف التشريع الجزائري مسألة الاختصاص القضائي في جرائم الاعتداء على التوقيع الالكتروني.

نص المشرع الجزائري على ثلاثة معايير تحكم الاختصاص المكاني وهي المحكمة التي ارتكبت الجريمة في نطاق إقليمها، أو المحكمة التي تفيض على المتهم في نطاقها، أو المحكمة التي يقيم المتهم في دائرتها، وفضلا عن ذلك قد ينص المشرع في بعض الأحوال ودون مراعاة إلى شخص المتهم أو صفته أو حالته وكذا لجسمه

[1]-جميل عبد الباقي الصغير، مرجع سابق. ص61.

[2]-صالح شنين، مرجع سابق، ص 248.

وخطورة الجريمة سواءا كانت تحمل وصف مخالفة أو جنحة أو جناية على استحداث محاكم معينة لنظر إلى هذه الجرائم وذلك لتحقيق العدالة ونظرا لظروف الخاصة لهذه الجرائم.

1-الاختصاص المحلي بجهات القضائية في جرائم الاعتداء على التوقيع الالكتروني.

تتعدد الجهات القضائية على مستوى إقليم الدولة الواحدة، وتختلف بذلك المهام التي أسندها المشرع لكل جهة قضائية على مستوى إقليم الدولة الواحدة، وتختلف بذلك المهام التي أسندها المشرع لكل جهة قضائية على حدة، حسب درجتها وحسب نوع القضايا التي يوكل لها مهام الفصل فيها، وحسب نطاقها الإقليمي الذي تمارس اختصاصها فيه.

الاختصاص المحلي لوكيل الجمهورية.

يتحدد الاختصاص المحلي لوكيل الجمهورية وفقا لنص المادة 37 من قانون الإجراءات الجزائية بمكان وقوع الجريمة ومحل إقامة أحد الأشخاص من المشتبه في مساهمتهم في الجريمة أو بالمكان الذي تم القبض على هؤلاء الأشخاص [1].

فأصل وطبقا لنص المادة 37 من قانون الإجراءات الجزائية أن اختصاص وكيل الجمهورية يجب أن لا يتعدى مكان وقوع الجريمة،أو محل إقامة احد الأشخاص المشتبه فيهم أو مكان القبض على هؤلاء ولكن نظرا لخصوصية جرائم التوقيع الالكتروني واحتمال ارتكابها في مجموعة من الأماكن واختراقها الحدود الجغرافية أو رد المشرع الجزائري استثناء من هذا المبدأ تماشيا والتطورات الحاصلة في مجال التكنولوجيا وتقنية المعلومات فبموجب المادة 2/37 من قانون الإجراءات الجزائية الجزائري أجاز المشرع تمديد الاختصاص المحلي لوكيل الجمهورية ليشمل كافة الإقليم الوطني [2] وعليه اصدر المشرع الجزائري المرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/5 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق أين وزعت المواد من 2إلى5 منه الاختصاص المحلي لبعض المحلي لبعض المحاكم

[1]-راجع في ذلك المادة 1/37 من قانون الإجراءات الجزائية الجزائري.

[2]-تنص المادة (2/37) من (ق.إ.ج.ج) يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجزائر الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

[1]و تجدر الإشارة إلى أن المحاكم التي تمتد تمديد اختصاصها "اصطلح على تسميتها بأقطاب الجزائية أو محكمة القطب المتخصص ".

-و من ناحية أخرى نجد أن المشرع وتحسبا لهذا النوع من الجرائم التي يتم غي علام افتراضي نص على مجموعة من الإجراءات لتسهيل عملية البحث والتحري عن هذه الجرائم فقد نص وبموجب المادة 144 مكرر -144 مكرر 2 على توسيعه لاختصاص المحلي لنيابة العامة في مجال الجرائم الالكترونية واجبرها أن تباشر إجراءات المتابعة تلقائيا [2].

ويتعين على ضباط الشرطة القضائية طبقا للمادة 40 مكرر 01 من القانون السابق أن يخبر وكيل لدى المحكمة الكائن بها الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابع له المحكمة المختصة [3] والذي يطالب طبقا للمادة 40 مكرر 2 من هذا القانون بالإجراءات فورا إذا اعتبر أن الجريمة تدخل ضمن اختصاص المحكمة المذكورة في المادة 400 مكرر من هذا القانون، وهذه الإجراءات تتعلق بتحريك الدعوى العمومية أو مباشرتها أو رفعها مجرد أن يتبين لنائب العام أن الجريمة تدخل ضمن اختصاصه [4].

-الاختصاص المحلي لقاضي التحقيق.

يقصد بالاختصاص المحلي لقاضي التحقيق المجال الذي يباشر فيه قاضي التحقيق عمله في التحقيق ويتحدد الاختصاص المحلي لقاضي التحقيق حسب المادة 40 من قانون الإجراءات الجزائية الجزائري بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو محل القبض على أحد هؤلاء الأشخاص [5].

ومثلما فعل المشرع مع تمديد الاختصاص لوكيل الجمهورية وللأسباب نفسها نص على تمديد الاختصاص المحلي لقاضي التحقيق ليشمل كافة الإقليم الوطني، وذلك حسب نص المادة 2/40 من ق.إ.ج.ج[6] كما تشير أيضا إلى أن تمديد الاختصاص المحلي لقاضي التحقيق مشمولا كذلك بأحكام المرسوم التنفيذي

[1]-المواد من (2-05) من المرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/5 المتضمن تمديد الاختصاص المحلي بعض المحاكم ووكلاء الجمهورية وقضاة تحقيق رقم 63 المؤرخة في 2006/10/8.ص30.

[2]-المادتان (144مكرر) و(144مكرر2) من قانون العقوبات الجزائري.

[3]-جباري عبد المجيد، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة دار هومة، الجزائر 2012، ص112.

[4]-راجع المادتين 40مكرر 1 و40 مكرر 2 من القانون إجراءات الجزائية الجزائري.

[5]-عدلت المادة 40 بالقانون رقم 14/04 المعدل والمتمم. المتضمن قانون الإجراءات الجزائية الجزائري

[6]-تنص المادة 2/40 من قانون إجراءات الجزائية الجزائري على "يجوز تمديد الاختصاص المحلي لقاضي التحقيق دائرة اختصاص محاكم أخرى، عن طريق التنظيم في جرائم..... والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ".

رقم 06-348 المؤرخ في 2006/10/5، سابق الذكر كما نجد أن المشرع الجزائري وبموجب نص المادة 4/47 من ق.إ.ج.ج نص على "عندما يتعلق الأمر بجرائم المخدرات، والجرائم المنظمة عابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإنه يجوز لقاضي تحقيق إجراء تفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين لقيام بذلك.

الاختصاص المحلي لضبطية القضائية.

غالبا ما تبدأ الإجراءات الجزائية في الدعوى العمومية بمرحلة البحث والتحري أي مرحلة جمع الاستدلالات التي تتولاها أصلا الضبطية أو الشرطة القضائية ولقد حدد قانون الإجراءات الجزائية الجزائري أحكام الضبط القضائي في المواد 65.63.55.42.28.12 وتشمل الضبطية القضائية ضباط الشرطة القضائية وأعوانهم وبعض الموظفين المنوطة بهم بعض مهام الشرطة القضائية، وتنفيذا للسياسة الإجرائية لمشرع الجزائري بخصوص مكافحة الجرائم الالكترونية خاصة في مجال البحث والتحري [1] أجازت المادة 7/16 تمديد اختصاصات ضباط الشرطة القضائية في حالة البحث والمعاينة إلى كافة الإقليم الوطني ويعمل هؤلاء تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا ويعلم وكيل الجمهورية المختص إقليميا بذلك [2] كما يلتصق بمهام الضبط القضائي إعمال المعاونة والمساعدة حسب نص المادة 20 من قانون الإجراءات الجزائية الجزائري المنوطة بأعوان الضبط القضائي الذين تبينهم المادة 19 من قانون الإجراءات الجزائية الجزائري

ومن ناحية أخرى، يمكن لضباط الشرطة القضائية وأعوان الشرطة القضائية في حالة عدم اعتراض وكيل الجمهورية تمديد عمليات المراقبة لأشخاص الذين يوجد ضدهم مبرر يحمل على الانتباه، وهذا حسب المادة 16 مكرر من ق.إ.ج.ج " والتي نصت على "يمكن لضباط الشرطة القضائية وتحت سلطة أعوان الشرطة القضائية ما لم يعترض على ذلك لضباط الشرطة القضائية وتحت سلطة أعوان الشرطة القضائية ما لم يعترض على ذلك وكيل الجمهورية المختص بعد إخباره، أن يمدد وعبر كامل الإقليم الوطني عمليات

[1]-يزيد بوحليط، مرجع سابق، ص 394.

[2]-المادة (7/16) من قانون إجراءات الجزائية الجزائري.

مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الانتباه فيهم بارتكاب الجرائم المبنية في المادة 16 من نفس القانون [1].

الاختصاص المحلي لمحاكم الجنح.

يتحدد الاختصاص المحلي لما حكم الجنح طبقا لنص المادة 324 من قانون الإجراءات الجزائية الجزائري بمكان وقوع الجريمة أو بمحل إقامة احد الأشخاص المتهمين أو شركائهم، أو بمكان الذي تم دائرته القبض على احد هؤلاء الأشخاص حتى ولو تم القبض عليهم لسبب آخر [2] غير أن المشرع الجزائري وبموجب المرسوم التنفيذي رقم 06.348 المؤرخ في 2006/10/5 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، أين وزعت المواد من 2-5 منه الاختصاص المحلي لمحكمة سيدي محمد ووكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس القضائية للجزائر، شلف، الأغواط، البليدة، البويرة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس، تيبازة، عين الدفلى.

كما يمتد الاختصاص المحلي لمحكمة قسنطينة ووكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس القضائية لقسنطينة، أم البواقي، باتنة، بجاية، بسكرة، تبسة،جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج، الطارف، الوادي، خنشلة، سوق أهراس، ميلة.

ويمتد الاختصاص المحلي لمحكمة ورقلة ووكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس القضائية لورقلة، أدرار، تمنراست، ايليزي، تندوف، غرداية [3].

وعليه نستنتج أن المشرع الجزائري وفي سبيل تسهيل عمل الأجهزة القضائية المكلفة بالتحريات والتحقيقات وفي إطار مواجهة الجرائم الالكترونية مدد الاختصاص لكل من وكيل الجمهورية واختصاص قاضي التحقيق واختصاص محاكم الجنح على مسمى الأقطاب المتخصصة.

ب-موقف التشريعات المقارنة من مسألة الاختصاص القضائي في جرائم توقيع الكتروني.

لقد تباينت مواقف التشريعات المقارنة في تجديد القضاء المختص بالنظر في جرائم الاعتداء على التوقيع الإلكتروني وفي ما يلي موجز لمواقف التشريعات المقارنة.

---

[1]-هذه الجرائم هي الجرائم المخدرات، جريمة المنظمة العابرة للحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بتشريع الخاص بالصرف.

[2]-راجع المادة 329 من القانون رقم 04/14 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري

[3]-المواد من 2-05 من المرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/5 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق (ج.ر) رقم 63 المؤرخة في 2006/10/8 ص30.

1-موقف التشريع المصري من مسألة الاختصاص القضائي في جرائم التوقيع الإلكتروني.

في التشريع المصري وطبقا لقانون رقم 2004/15 نجد أنه لم ينص على تحديد جهات التحري والتحقيق والحكم في هذه الطائفة من الجرائم، مما يعني إعمال القواعد العامة في الاختصاص التي تقضي بوجود ثلاث معايير تحكم الاختصاص المكاني وهي المحكمة التي ارتكبت الجريمة في نطاقها، أو المحكمة التي يقيم المتهم في دائرتها، أو المحكمة التي تم القبض على المتهم في نطاقها.[1]

و فضلا عن ذلك فإن الاختصاص النوعي لجرائم التوقيع الالكتروني يعتمد على تقسيم المشرع للجرائم نوعيا بالنظر إلى جسامتها إلى جنايات، جنح، مخالفات وفقا لهذا التقسيم يختص محكمة الجنح ينظر في المخالفات، والجنح عدا الجنح التي تقع بواسطة الصحف أو غيرها، وفي ضوء ما تقدم سنقوم بدراسة.

-الاختصاص المحلي للمحاكم بنظر من جرائم الاعتداء على التوقيع الالكتروني.

لقد نص المشرع المصري على ثلاثة معايير تحكم الاختصاص المكاني وهي المحكمة التي ارتكبت الجريمة في نطاقها الإقليمي، أو المحكمة التي قبض على المتهم في نطاقها أو المحكمة التي يقيم المتهم في دائرتها وهذه المعايير الثلاثة متساوية لا تمييز لا بها على الآخر، بحيث يجوز تحريك الدعوى الجنائية الناشئة عن جرائم الاعتداء على التوقيع الالكتروني أمام أي من هذه المحاكم [2].

ولا يختلف الاختصاص المكاني لسلطة التحقيق عما سبق، حيث تسري ذات المعايير الثلاثة السابقة على الاختصاص المكاني لسلطة التحقيق.[3]

-الاختصاص النوعي للمحاكم بنظر في جرائم الاعتداء على التوقيع الالكتروني.

يعتمد هذا المعيار على تقسيم المشرع للجرائم نوعيا بالنظر إلى جسامتها إلى جنايات، جنح، مخالفات ووفقا للمشرع المصري تختص محكمة الجنح الجزائية بنظر المخالفات والجنح ما عدا الجنح التي تقع بواسطة الصحف أو غيرها من طرف النشر على غير الأفراد وانه بالرجوع لنص المادتين 23 و24 من قانون التوقيع الالكتروني المصري، قد نص على أن عقوبة جميع جرائم الاعتداء على التوقيع الالكتروني هي الحسب أو الغرامة أو إحدى هاتين العقوبتين ومن ثم تعد هذه الجرائم من قبل الجنح كأصل عام وينعقد الاختصاص لمحكمة الجنح بنظر لنوعية الجرائم من قبيل الجنح كأصل عام وينعقد الاختصاص لمحكمة الجنح بنظر لنوعية الجرائم، إلا أنه ولما كان المشرع قد استهل هاتين المادتين بعبارة مع عدم الإخلال بأي عقوبة أشد

[1]-راجع نص المادة 15 من قانون إجراءات الجنائية المصري.

[2]-محمود نجيب حسني، المرجع السابق، ص187.

[3]-محي الدين عوض، مشكلات السياسية الجنائية المعاصرة في جرائم نظم المعلومات، دار النهضة العربية، القاهرة، مصر، 1994. ص357.

منصوص عليها في قانون العقوبات، أو أي قانون آخر، فإن مؤدى ذلك انه وكلما كان الاعتداء على التوقيع الالكتروني بشكل جناية، فإن الاختصاص في هذه الحالة ينعقد لمحكمة الجنايات كما هو الحال لوكان التوقيع الالكتروني قد توافرت فيه شروط المحرر الرسمي وتم تزويره ففي هذه الحالة تشكل الواقعة جناية تزوير محرر رسمي أو استعماله فيما زور من أجله، وينعقد الاختصاص بنظرها لمحكمة الجنايات [1].

2-موقف التشريعات الأخرى حول مسألة الاختصاص القضائي في جرائم الاعتداء على التوقيع الالكتروني.

يمنح قانون العقوبات الفنلندي الاختصاص للقضاء الوطني بمكان وقوع الجريمة وبمكان حدوث نتائج الجريمة التي وقعت، أو بمكان المقصود حدوثها فيه في حالة الشروع وفقا للمادة 4 من قانون العقوبات الفنلندي.

أما القانون الإنجليزي وضع قواعد خاصة للاختصاص في مجال جرائم الكمبيوتر بمقتضى قانون 1990 بموجب المادة 5 حتى ولو لم يحدث الفعل المجرم على الإقليم الإنجليزي أو تواجد المتهم على هذا الإقليم، وإنما يكفي أن تقوم دلائل قوية بين الجريمة والقانون الإنجليزي.

و يسري أيضا القانون الهولندي على تجميع البيانات الذي يقع خارج البلاد إذا كان المسئول عنه يقيم في البلاد [2]

أما في القانون الفرنسي فيمتد اختصاص القضاء هناك في جرائم الانترنت التي وقعت في الخارج عملا بقانون العقوبات الجديد متى كانت الظروف الواقعة تبرر مصلحة فرنسا في إعمال قانونها عليها[3]

المطلب الثاني: سلطة القاضي الجنائي في قبول الدليل الالكتروني في جرائم الاعتداء على التوقيع الالكتروني.

يعد قبول الدليل الخطوة الإجرامية الأولى التي يمارسها القاضي تجاه الدليل الجنائي بصفة عامة والدليل الالكتروني بصفة خاصة وذلك قبل البدء في تقديره للتأكد من مدى صلاحيته وملاءمته لتحقيق ما قدم من أجله، وقبول القاضي الجنائي للدليل الالكتروني في الإثبات لابد وأن يستند على أساس وهذا الأساس هو مبدأ الاقتناع القضائي للقاضي الجنائي وحدوده في مجال المحررات الالكترونية.

[1]-أيمن رمضان محمد أحمد، مرجع سابق ، ص386.

[2]-صالح شنين، مرجع سابق، ص255.

[3]-جميل عبد الباقي الصغير، مرجع سابق، ص73.

فجل التشريعات وأحكام القضاء المقارنة تتجه في أغلبها إلى الاعتداء بحجية مخرجات الحاسب الآلي باعتبارها أدلة إثبات أمام القاضي الجنائي وذلك في إطار مجموعة من الشروط والتي سوف نبينها من خلال الفروع الآتية.

الفرع الأول: أساس قبول الدليل الالكتروني في الإثبات الجنائي.

في الواقع، أن موقف القوانين أن موقف القوانين المقارنة فيما يتعلق سلطة القاضي الجنائي في قبول الدليل الالكتروني بالنسبة لجرائم التوقيع الالكتروني يخضع إلى نظام الإثبات السائد في الدولة، وتنقسم هذه النظم إلى ثلاث فئات.

الفئة الأولى: وهي القوانين اللاتينية والتي تبني مبدأ حرية الإثبات ومنها سلطة القاضي في قبول جميع الأدلة، وهنا تكون جميع طرق الإثبات مقبولة، ما لم يستعيد المشرع بعضها صراحة [1].

الفئة الثانية: وهي القوانين الأنجلوسكسونية، حيث تقيد من حرية الإثبات في مرحلة الفصل في مسألة الإدانة أو البراءة إما في مرحلة تحديد العقوبة فيسود مبدأ حرية الإثبات[2].

أما الفئة الثالثة: وهي تأخذ بنظام الأدلة القانونية، بحيث تحدد الآلة التي يجوز للقاضي الجنائي قبولها، كالقانون الهولندي 339 من قانون الإجراءات الجنائية والقانون الألماني الذي يحدد على سبيل الحصر وسائل الإثبات التي يتعين على القاضي قبولها [3]

و على هدى من ذلك منقسم هذا الفرع إلى:

أولا: مبدأ حرية الإثبات الجنائي كأساس لقبول الدليل الالكتروني النظام اللاتيني

تتبنى الدول التي تتأثر قوانينها بالصياغة اللاتينية في مجال الإثبات الجنائي مبدأ حرية الإثبات ومنها سلطة القاضي في قبول جميع الأدلة، حيث يمثل هذا المبدأ لب نظام الإثبات الحر [4]و يطلق عليه أيضا مبدأ الاقتناع القاضي، ومنه يعني هذا المبدأ، "حرية جميع الأطراف في اللجوء إلى كافة وسائل الإثبات للتدليل على صحة ما يدعونه، فلسفة الاتهام أن تلجأ إلىأية وسيلة لإثبات وقوع الجريمة على المتهم أو يدفع المتهم كذلك

[1] -أحمد عصام عجيلة، مرجع سابق، ص480.

[2] -أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، الطبعة الثانية، دار النهضة العربية، القاهرة 2006 هامش رقم 12ص14.

[3] -سعيد السيد قنديل، مرجع سابق، ص194.

[4] - محمود نجيب حسني، شرح قانون الإجراءات الجنائية، مرجع سابق، ص 375.

بكل الوسائل، ويستظهر القاضي الحقيقة بكل ذلك أو بغيره من طرق الإثبات[1] وبمقتضاه يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته.

-فقد اقر التشريع المصري المبدأ حرية القاضي في الاقتناع بموجب المادة 1/302 من قانون الإجراءات الجنائية في قولها. " يحكم القاضي في الدعوى حسب العقيدة التي تكون لديه بكامل حريته " وقد أكدت على ذلك محكمة النقض فقضت بأن " العبرة في المحاكمات الجنائية هي باقتناع القاضي بناءا على الأدلة المطروحة عليه بإدانة المتهم أو ببراءته وله أن يستمد اقتناعه من أي دليل يطمئن لديه طالما له مأخذه الصحيح في الأوراق [2]

المشرع الفرنسي سار على نفس النهج واعتمد هو كذلك على هذا المبدأ وذلك من خلال المادة 427 من قانون الإجراءات الجزائية حيث نص "مالم يرد نص مخالف، يجوز إثبات الجرائم بجمع طرق الإثبات، وبحكم القاضي بناءا على اقتناعه على الشخصي[3] وهذا النص وإن كان مخصصا لمحاكم الجنح، إلا أن مبدأ حرية الإثبات يطبق أما جميع أنواع المحاكم الجنائية إلا إذا نص القانون على خلاف ذلك.

وكذلك اقر المشرع الجزائري مبدأ حرية الإثبات الجنائي في المادة 212 من ق.إ.ج.ج التي تنص على "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي تخص فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا للاقتناع الشخصي.

وتكمن الأسباب الداعية لضرورة إعمال مبدأ حرية الإثبات في نطاق نظرية الإثبات الجنائي فيما يلي.

-إن حرية الإثبات تعد نتيجة منطقية لمبدأ قضاء القاضي بمحض اقتناعه والتي تتبع في نفس الوقت السماح للقاضي بالاستعانة بجميع وسائل الإثبات التي يقتنع ويطمئن إليها لتمكين القاضي من أداء رسالته في إرساء العدالة بين المتقاضين.

-إنالإثبات في الدعوى الجنائية يرد على وقائع قانونية –مادية أو نفسية –يصعب بل يستحيل الحصول على دليل مسبق لها.

- إن موضوع الإثبات في الدعوى الجنائية يرد على وقائع قانونية تنتمي إلى الماضي، لذلك للمحكمة أن تستدعي بكل الوسائل الممكنة كي يعتد لها رواية ما حدث

[1]-أحمد عصام عجيلة، مرجع سابق ، ص486.

[2]- أحمد عصام عجيلة، مرجع سابق، ص 487.

[3]-جميل عبد الباقي صغير، مرجع سابق، ص 420.

- من المسلم به أن قرينة البراءة تلقي عبئ الإثبات كلية على عاتق سلطة الاتهام مما جعلت مهمته هذه الأخيرة جد صعبة.[1]

- إن طبعة المصلحة التي تحميها الدعوى الجنائية تختلف عن تلك التي تحميها الدعوى المدنية

- مبدأ حرية الثبات بعد ثبات إقرار ضمني من المشرع بعدم قدرة الأدلة التقليدية والتي لو تم صرها كأدلة إثبات على مواجهة الجرائم المستحدثة ومنها الجريمة الالكترونية وعلى ذلك تلاحظ أن الدلائل الالكتروني شأنه في ذلك شأن الأدلة الأخرى التي تم ذكرها على سبيل المثال في القانون، مقبول مبدئيا في الثبات الجنائي بصفة عامة، أوالإثبات في مجال جرائم التوقيع الالكتروني بصفة خاصة.

أ-النتائج المترتبة على تطبيق مبدأ حرية الثابت الجنائي

يقدم أعمال حرية الثبات للقاضي الجنائي في الجرائم الالكترونية أن القاضي الجنائي يتمتع بدور إيجابي في توفير إيجابي في توفير وقبول وتقدير الدليل الجنائي بما في ذلك الدليل الالكتروني وهو ما سنتناوله في النقاط التالية:

1- الدور الإيجابي للقاضي الجنائي في توفير الدليل الالكتروني

يؤدي القاضي الجنائي دورا هاما، بل لعله أكثر الأدوار أهمية في الدعوى الجنائية، وبصفة خاصة في شأن عملية الإثبات، وحتى يتضح لنا هذا الدور المهم للقاضي الجنائي يتعين لنا أن يقوم بتحديد مفهوم هذا الدور بداية ثم تعرض لأهم مظاهر الدور الإيجابي للقاضي الجنائي.

- مفهوم الدور الإيجابي للقاضي الجنائي في توفير الدليل الالكتروني

ويقصد به عدم التزام القاضي بما يقدمه له أطراف الدعوى من أدلة، وإنما له سلطة بل وواجب عليه أن يبادر من تلقاء نفسه إلى اتخاذ جميع الإجراءات لتحقيق الدعوى والكشف على الحقيقة العقلية فيها [2]وفي ذلك يختلف دور القاضي الجنائي عن دور القاضي المدني في هذا المقام، فإذا كان عمل هذا الخير مجرد قبول الأدلة المقدمة من الخصوم في الدعوى، فليس له أن يبادر من تلقاء نفسه إلى البحث عن أي دليل أو تقدمه أو يوجه احد الأطراف إلى تقديم دليل يعينه، بينما القاضي لا يتخذ هذا الدور السلبي.

ويختلف دور القاضي الجنائي بالنسبة لدليل الالكتروني بحسب النظام الإجرائي السائد في الدولة، ففي النظام الاتهامي يكون دور القاضي سلبيات لان هذا النظام ينظر إلى الدعوى الجنائية من قبل طرفيها نظرة

[1] سعيد السيد قنديل، مرجع سابق ، ص 198.

[2] -محمد محمود مصطفى، مرجع سابق، ص 419.

متساوية أما في النظام التقني فيكون ذو القاضي إيجابيا في تحقيق الدعوى الجنائية [1] ومن الدول التي يأخذ بالنظام الأخير في مصر وفرنسا وتجدر الإشارة أن المقصود بالقاضي ليس هو قاضي الحكم فحسب وإنما يشمل أيضا قضاء للتحقيق باعتبار أن مشكلة الإثبات قد تثور في أي مرحلة كانت عليها الدعوى الجنائية بل يمكن أن تثور قبل ذلك أي في مرحلة جمع الاستدلالات أيضا.

- مظاهر الدور الإيجابي للقاضي في توفير الدليل الالكتروني

ومن مظاهر ذلك للقاضي الجنائي في مصر، ما نصت عليه المادة 291 من قانون الإجراءات الجنائية والتي جرى نصها على انه " للمحكمة أنتأمر ولو من تلقاء نفسها أثناء نظرا الدعوى بتقديم أي دليل تراه لازما لظهور الحقيقة [2] كذلك يعد من مظاهر الدور الإيجابي للقاضي الجنائي في القانون المصري ما نصت عليه المادة 274 من قانون الإجراءات الجنائية حيث خطرت استجواب المتهم ما لم يقبل هو بذلك، غير أنها أضافت انه إذ ظهر المتهم أثناء المرافقة والمناقشة لبعض الوقائع ترى لزوم تقديم إيضاحات عنها من المتهم لظهور الحقيقة بلغته القاضي إليها ويرفض له بتقديم تلك الإيضاحات.[3]

وفي مواد الجنايات فقد افرد القانون للإجرائي الفرنسي نصا خاصا منح بموجبيه رئيس محكمة الجنايات سلطة تقديرية خاصة للقيام بجمع الإجراءات التي تقدر فائدتها في الكشف عن الحقيقة المادة 310 من قانون الإجراءات الجنائية الفرنسي.

ومن مظاهر الدور الإيجابي للقاضي الجنائي في البحث عن الدليل الالكتروني، انه بإمكان القاضي الجنائي أن يأمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام والولوج إلى داخله، كإفصاح عن كلمات المرور السرية والفرات الخاصة بتشغيل البرامج المختلفة، كذلك للقاضي الجنائي سلطة الأمر بتفتيش نظم الحاسب الآلي بمكوناته المادية والمعنوية وشبكات الاتصال متى ما قدره ضرورة ملائمة هذا الإجراء وفي مجال البحث عن الدليل الالكتروني نجد أن الخبرة التقنية تعد من اقوي مظاهر التعامل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات، فهي تؤدي دورا لا يستهان به خاصة مع نقص المعرفة القضائية الشخصية لظاهرة الحاسب الآلي والانترنت.[4]

---

[1]-عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، 2010، ص191..

[2]-أحمد عصام عجليه، مرجع سابق ، ص 490

[3]-محمد زكي أبو عامر، القيود القضائية على حرية القاضي الجنائي في الاقتناع، مجلة القانون والاقتصاد، العدد 51، 1991 ، ص120

[4]-سعيد السيد قنديل، مرجع سابق ، ص201.

ثانيا: مبدأ الإثبات المقيد كأساس لقبول الدليل الالكتروني النظام الأنجلوساكسوني

ويسمى هذا النظام أيضا بنظام الأدلة القانونية وفيه تكون الأدلة محصورة ومحددة تسلف من قبل المشرع، بل إن قوتها الدليلية محددةولا يجوز للقاضي أن تخرج عليها، ويبني حكمه على خلالها، ويعني نظام الأدلة القانونية أنالمشرع هو الذي يحدد للقاضي الأدلة التي يجوز أن يقبلها في حالة معنية، فيحظر عليه أن يقبل أدلة سواها.[1]

ويثير قبول الأدلة المتحصلة من الوسائل الالكترونية مشكلات عديدة في ظل القواعد الأنجلوساكسوني للإثبات الجنائي والتي تعتنق كمبدأ أساسي الإثبات بالشهادة.

أ- مدى اعتبار الدليل الالكتروني شهادة سماع

يقصد بالشهادة السماعية أو كما يطلق عليها البعض بالتسامع عن الغير والانجليزية Hearsay بيان أو تقرير شفوي أو كتابي يحدث خارج المحكمة ويقدم إليها من اجل الحقيقة أو بعبارة أخرى من اجل إثبات أمر حدث خارج الجلسة وكان صادقا.[2]

أما في الفقه الإنجليزي فيسوده أساسيان الأول ما قال به Wignore على أن شهادة السماع هو دليل شفوي مستند يقدمه شخص ما إلى المحكمة على أساس انه عبارات أو سلوك صدر من أخر خارج المحكمة، يتوقف قبوله أو استعباده على مقدار الثقة التي تتوافر لدى المحكمة فيما أدلى به خارج المحكمة، أما التعريف الثاني والذي قدمه Mogran فقد قال فيه " أن الشهادة السماع هي دليل يقدم من خلال شخص نقلا لعبارات آو سلوك صدر خارج المحكمة من شخص آخر، ويؤكد أولا يؤكد مسألة معنية لإثبات الحقيقة في تلك المسألة ويعتقد من يقدمه في صحته.[3]

والفارق بين التعريفين أن التعريف الأخير يجعل من شهادة يجعل من شهادة السماع دليلا غير جازم أي انه مجرد دلالة لا يرتق لمستوى الدليل، وهذا التعريف هو السائد حاليا في معظم التشريعات التي تأخذ بنظام الانجلوامريكي.[4]

- الأصل في شهادة أنها لا يعول عليها كدليل، حيث يمكن الحكم على مقتضاه، ويرجع السبب في ذلك إلى عدم الثقة في شخص الذي يدلي به خارج المحكمة مع ذلك لا تعني هذه القاعدة أن يكون النقل عن

[1]-يوسف بن سعيد الكلباني، مرجع سابق ، ص417.

[2]-رمزي رياض عوض، حماية المتهم في النظام الانجلو امريكي، دار النهضة العربية، القاهرة ، 1998 ، ص33.

[3]-أحمد عصام عجيلة، مرجع سابق ، ص43

[4]-رمزي رياض عوض ، مرجع سابق ، ص34

الغير،سواء كان نطقا أو كتابة يتم تجاهله نهائيا، بل هناك حالات استثنائية يتم فيها قبول شهادة السماع كدليل في الدعوى الجنائية واهم هذه الحالات هي:

- أقوال المحني عليه التي نطق بها قبل وفاته، إخبار احد أعضاء الاتفاق الجنائي، التسجيلات الرسمية، البيانات والمعلومات التي يتم عليها من الكمبيوتر، التقرير التلقائي، النطق بمفهوم الانطباعية

ويجدر الإشارةإلىأن قبول الدليل الالكتروني على أساس استثناء قاعدة شهادة السماع لا يطيق على جميع أنواع سجلات الحاسوب ذلك لان محاكم الفدرالية الأمريكية قسمت هذه الأخيرة إلى ثلاث أنواع.[1]

- سجلات الحاسوب المخزنة: تحتوي بيانات بشرية، مثل المخرجات من برنامج الكتابة من الكمبيوتر.
- سجلات الحاسوب المتوالدة: وفيها يقوم الجهاز بتدوين البيانات التي تصح أن تقدم مباشرة إلى محكمة، فهي ليست من قبلي شهادة السماع وتتوقف قيمته الثبوتية على ماذا كان جهاز الكمبيوتر يعمل بطريقة أم لا.
- أما بالنسبة لسجلات التدخل الإنساني ومعالجة الكمبيوتر: هو سجل تجمع بين التدخل الإنساني ومعالجة الكمبيوتر، وان كان جزءا منها يعد شهادة السماع وهو الصادر عن الإنسان إلا انه لا بعد هذا النوع من السجلات شهادة سماع.

ب- قاعدة الدليل الأفضل "the best evidencerule كدليل الكتروني:

ويقصد بهذه القاعدة، انه في حالة الدليل الكتابي يعتد بالنسخة الأصلية للمحرر ويمكن أن تعتبر الكتابة الموجودة داخل الجهاز في صور الكهرومغناطيسية من قبيل النسخة الأصلية، وبالتالي لا يصطدم بقاعدة أفضل دليل ونعتد بالمحررات الالكترونية باعتبارها نسخة أصلية كما يقصد بها أيضا " لأجل إثبات محتويات كتابة أو سجل أو صورة فان أصل الكتابة أو السجل أو الصورة يكون مطلوبا [2]

بمعنى انه لا يجوز تقديم الصورة لإثبات محتوى الأصل بصفة عامة حين يقدم احد الأطراف تأبيد الدعوى دليلا يستند إلى عدة دعائم ومن ثم فعليه أن تقدم أفضل نموذج وهو ما عين بان تكون الأدلة الواجب تقديمها أولية وليست ثانوية، أصلية لا بديلة، وان يكون الدليل المقدم هو أفضل ما يتاح الحصول عليه بالنسبة لطبيعة وظروف القضية [3] فقد قرر القانون الأمريكي هذه القاعدة بموجب المادة 1002 من

[1]-سعيد السيد قنديل، مربع سابق ، ص203.

[2]-أحمد عصام عجليه، مرجع سابق ، /ص494

[3]- Jack blogna, Corporate Fraud: The Basics of Prevention and Detection, Butterworth-Heinemann, (July 1, 1984), p45.

قانون الإثبات الأمريكي والتي تقمني على أن حجية الكتابة أو التسجيل أو الصورة من بتقديم الأصل إلاإذا نص القانون على خلاف ذلك، ومع ظهور المستندات الالكترونية استدعى الأمرإلى تفسر هذه القاعدة لكي تتلائم مع عصر المعلومات وقد استجاب بعض التشريعات كالقانون الأمريكي والانجليزي لهذه المستجدات حيث قام المشرع الأمريكي باستخدام مدلول موسع للكتابة والتسجيلات يشمل الحروف أو الكلمات أو الأرقام أو ما يعادلها مكتوبة باليد أو منسوخة على الأدلة أو مطبوعة أو ثم تصويرها أو تنخ شكل نبضات مغناطيسية بتسجيل ميكانيكي أو الكتروني.....

أما بالنسبة للقانون الإنجليزي فقد تم قبول صدور المستندات أو جزء منها بموجب المادة 27 من قانون العدالة الجنائية لسنة 1988

ج- شروط قبول الدليل الالكتروني الإثبات في النظام الانجلوساكسوني

اتجه التشريع والقضاء في دول النظام الانجلوساكسوني إلىالأخذ بالدليل الالكتروني، وفيما يلي سنوضح هذه الشروط على النحو التالي

- **في انجلترا:** قبل المشرع الإنجليزي الدليل الإنجليزي كدليل في الإثبات وذلك خروجا على الأصل العام الذي تبيناه القانون الإنجليزي في عدم قبول الشهادة السماعية، ومع ذلك فان القاضي الإنجليزي يستطيع أن يتعبد هذا النوع من الدليل إذا وجدت أدلة أخرى أوإذا لم يطمئن إليها وقد قبل المشرع الإنجليزي مخرجات الحاسب من المحررات الالكترونية في الإثبات في بعض الحالات ينص صريح نص المادة 69التي نصت على انه " في أية إجراءات لا يقبل البيان المتضمن في مستند صادر عن طريق الحاسب كدليل على أية واقعة واردة فيه إلاإذاتبين [1]

- عدم وجود أسباب معقولة للاعتقاد بان البيان يفتقر إلى الدقة بسبب الاستخدام غير مناسب أو الخاطئ للحاسوب

- إن الحاسب كان يعمل في جمع الأحوال بصورة سلمية وإذا لم يكن كذلك فانه لم يثبت أن هناك جزء منه لم يكن يعمل فيه بصورة سليمة أو كان عدم انتظامه ناتجا عن عيب لم يكن مؤثرا في استخراج المستند أو دقة محتوياته

[1]-أحمد عصام عجيلة، مرجع سابق ، ص496.

- الوفاء بآية شروط متعلقة بالمستند والمتعلقة بالطريقة أو بالكيفية التي يجب أن تقدم بها المعلومات الخاصة بالبيان المستخرج عن طريق الحاسب [1]

- **في الولايات المتحدة الأمريكية:**

لجا المشرع الفيدرالي الأمريكي إلى تعديل قانون الإثبات وهذا تماشيا تطور تكنولوجيا المعلومات مشتملا بذلك الدليل الالكتروني فقد جاء في المادة 1001 نبدأ أ بخصوص الكتابة والتسجيلات فقد وسع من مدلول الكتابة يشمل الحروف والأرقام والكلمات أو ما يعادلها، كتوبة على اليد أو منسوخة على الآلة الكاتبة أو مطبوعة أو تم تصويرها أو اتخذت شكل نبضات مغناطيسية أو أي شكل آخر من تجميع المعلومات، ولقد ذهب القانون الأمريكي إلى العد من ذلك حال توسعه في مدلول عرض الدليل الالكتروني، وذلك بنص المادة 1001 [2] من قانون الإثبات الأمريكي بأنهإذا كانت البيانات مخزنة في حاسب أو جهاز مماثل فان مخرجات الطابعة أولية مخرجات أخرى يمكن قراءتها بالنظر إلى ما تم إظهارها وتبرز انعكاسا دقيقا للبيانات، تعد بيانات أصلية، ويفهم من خلال هذه المادة انه يقبل الدليل الالكتروني كمخرجات الحاسب الآلي من المحررات الالكترونية المطبوعة كدليل أصلى كامل كالنسخة المطابقة للأصل.[3]

ثالثا: نظام الإثبات المختلط:

يعتبر نظام الإثبات المختلط نظام وسط أي نظام توفيقي بين نظام الإثبات الحر ونظام الإثبات المقيد، حيث تتراوح أحكامه بين التقييد والإطلاق، فيجنب لعشق القاضي في نظام الإثبات الحر وخروجه عن الدور السلبي المحض للقاضي في النظام المقيد بان يمنح له حرية في تقدير ما يعرض عليه من أدلة[4] فهو نظام توفيقي بين النظامين عندما يحدد القانون أدلة معنية للإثبات في بعض الوقائع دون الأخرى، أو يطلب شروطا في بعض الحالات، أو يعطي القاضي الحرية في تقدير الأدلة كقانون البياني الذي يحصر طرق الإثبات المقبولة في أقوال المتهم وشهادة الشهود والخبرة المنجزة من طرف الخبراء [5]

---

[1]- هشام محمد فريد رستم ، مرجع سابق ، ص189

[2]- وقد عرفت المنظمة الدولية للأدلة الحاسب النسخة المطابقة للأصلبأنها نسخته رقمية رقيقة لكل البيانات أو المعلومات الموجودة في البنود الأصلية لمزيد من المعلومات حول دور هذه المنظمة في تقييم أدلة الحاسب انظر الموقع الالكتروني للمنظمة www.ioce.org بتاريخ 2020/08/17 على الساعة 11:00.

[3]- يزيد بوحليط، مرجع سابق، ص408

[4]- يزيد بوحليط، مرجع سابق ، ص 409

[5]- هلالي عبد الله أحمد، مرجع سابق، ص59.

الفرع الثالث: ضوابط الدليل الالكتروني وأثره على اقتناع القاضي

يقتضي الحديث على ضوابط الدليل الإلكتروني وأثره على اقتناع القاضي الجنائي بيان مضمون مبدأ الاقتناع القضائي وما يعنيه في مجال الإثبات الجنائي ثم بيان قيود وضوابط التي ترد علمي هذا المبدأ.

أولا:تعريف مبدأ الاقتناع القضائي.

إن كل عملية قضائية التي يجريها القاضي الجنائي غايتها النهائية التوصل إلى الحقيقة الواقعة فكل نشاط أو جهد ذهني يبذله القاضي خلال إجراء هذه العملية لا تبدي أن يرمي من ورائه إلى استظهار الحقيقة الوقائع كما حدثت في الواقع أو العالم الخارجي لا كما يصورها الخصوم، ولا يمكن أن يصل إليهاإلا بعد حصوله على أدلة ثانية وبعد اقتناعه الشخصي بحدوثها فماذا يعني هذا المبدأ وماهي ضوابطه ؟و ماهي القيود التي ترد عليه ؟ "فهو يعني" الأثر النهائي لعملية استبدال واستنتاج تتلاقى فيها جميع الأدلة القضائية المطروحة بالدعوى والتي تصب في بوتقة واحدة هي ذاتية القاضي، دعائمها العقل والمنطق والوجدان الحي للقاضي حيث يقوم فيها بالتمحيص والتقدير والموازنة بين أكثر الأدلة عمقا واتصالا بالحقيقة، فيحدد الحكم على أساسها [1].

كما ذهب جانب من الفقه إلى تعريفه بأنه " التقدير الحر المسبب لعناصر الإثبات في الدعوى وهو البديل عن نظام الأدلة القانونية، كما عرف بأنه، تلك الحالة الذهنية أو النفسية أو ذلك المظهر الذي يوضح وصول القاضي باقتناعه لدرجة "اليقين بحقيقة " واقعة لم تحدث تحت بصره بصورة عامة [2]

و لقد أقرت معظم التشريعات الحديثة هذا المبدأ، حيث نص عليه المشرع الفرنسي لأول مرة في المادة 342 من قانون التحقيقات الجنائية وذلك من خلال التعليمات التي تلقي على المحلفين قبل دخولهم للمداولة، وإذا كان هذا النص قد ألغى بمقتضى قانون 25 نوفمبر 1941 وتنطبق هذه القاعدة أمام كل الجهات القضائية الجنائية حيث كرست المادتين 427-536 من قانون الإجراءات الجنائية الفرنسي فالمادة

[1]- حازم محمد حنفي، المرجع سابق.ص237.

[2]- مفيدة سويدان، نظرية الاقتناع الذاتي القاضي الجنائي، دراسة مقارنة، رسالة دكتورة، كلية الحقوق، جامعة القاهرة 1990، ص 179.

327 نصت على هذا التطبيق أمام محكمة الجنح، أما المادة 536 تتطبق أمام محكمة المخالفات حيث تحيل إلى تطبيق المادة 427.[1]

أما المشرع الجزائري فقد كرس مبدأ الاقتناع القضائي بموجب المادة 307 من ق إجراءات الجزائية وهي مستوحاة من المادة 353 من القانون الفرنسي حيث تنص على "يتلو الرئيس قبل مغادرة المحكمة كما كرست المادة 212 أيضا هذا المبدأ من قانون إجراءات الجزائية الجزائري حيث نفذ على أنه "يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ماعدا الأحوال التي ينص فيها على غير ذلك وللقاضي أن يصدر حكمه تبعا لاقتناعه ".[2]

كما وقد نص المشرع المصري لهذا المبدأ في المادة 302/أ من قانون الإجراءات الجناية المصري حيث نصت على أنه "يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته "و تؤكد هذا المبدأ أيضا المادة 1/291 و300 من هذا القانون وهما يشيران بجلاء إلى الدور الإيجابي للقاضي الجنائي وعدم اقتصاره على ما يقدمه له الخصوم، وذلك من أجل وصوله إلى الحقيقة الفعلية في الدعوى.[3]

و من التشريعات التي حصرت على تأكيد هذا المبدأ أيضا نجد قانون الإجراءات الجنائية الاتحادي السويسري الذي كان ينص في المادة 3/169 منه على أنه القضاة يقدرون في حرية مدى صدق الشهود والقوة التدليلية لكل الأدلة المقدمة.

و قد يتبنى المشرع السوري مبدأ حرية القاضي الجنائي في الإثبات حيث تنص المادة 175 من قانون أصول المحاكمات الجزائية الصادر بالمرسوم 112/بتاريخ1950/03/13 على أنه "تقام البيئة وفي الجنايات والجنح والمخالفات بجميع طرق الإثبات ويحكم القاضي حسب قناعته الشخصية مما يفيد حرية القاضي الجنائي في تكوين قناعته [4].

ثانيا:نطاق تطبيق مبدأ الاقتناع القضائي.

لقد ثار خلاف حول المجال الحقيقي لتطبيق مبدأ الاقتناع القضائي سواء من حيث طبيعة القضاء ومن حيث مراحل الدعوى الجنائية.

[1]- سعيد السيد قنديل، مرجع سابق. ص223.

[2]- يزيدبولحيط، مرجع سابق، ص 414.

[3]- أحمد حسام طه، مرجع سابق، ص 406.

[4]- حازم محمد حنفي، مرجع سابق.253.

فالنسبة للأولى: يمتد تطبيق مبدأ الاقتناع القضائي إلى كافة أنواع المحاكم الجنائية سواء كانت محاكم الجنايات أم الجنح أو المخالفات وإن كان المشرعان الجزائري والمصري لم يحدد ذلك صراحة في المواد المقررة لهذا المبدأ [1] بخلاف المشرع الفرنسي.

أما بالنسبة للثانية: فإذا كان مبدأ الاقتناع القضائي شرع أصلا لكي يطبق أمام قضاة الحكم، إلا ذلك لا يعني أبدا أن نطاق تطبيقه مقصور على هذه المرحلة بل هو يمتد كذلك ليشمل مرحلة التحقيق الابتدائي، حيث أن هذا المبدأ يطبق أيضا أمام قضاة التحقيق والإحالة، فهم يقدرون مدى كفاية الأدلة وعدم كفايتها للاتهام دون الخضوع لقواعد معينة ولا لرقابة محكمة النقض ولكنهم يخضعون في ذلك لضمائرهم واقتناعهم الذاتي فحسب، وقد قضت محكمة النقض المصرية بأن المقصود من كفاية الأدلة في قضاء الإحالة أنها تسمح بتقديم المتهم للمحاكمة مع رجحان الحكم بإدانته وهو المدى الذي يتفق وظيفة ذلك القضاة كمرحلة من مراحل الدعوى الجنائية [2]

ثالثا: تقدير القضاة لدليل الالكتروني.

يخضع الدليل العلمي إلى تقدير القاضي الجنائي واقتناعه وفي هذا الخصوص ينبغي أن نميز بين أمرين.

ظروف وملابسات التي وجد فيها الدليل: فتقدير القاضي لا يتناول الأمر الأول، وذلك لأن قيمته الدليل تقوم على أسس علمية دقيقة، وبالتالي لا حرية في مناقشة الحقائق العلمية الثابتة.

ذلك أن مجرد توافر الدليل العلمي لا يعني أن القاضي ملزم بالحكم بموجبه مباشرة سواء بالإدانة أم البراءة، دون بحث في الظروف والملابسات فالدليل العلمي ليس آلية معدة لتقرير اقتناع القاضي بخصوص مسألة غير مؤكدة [3].

و على ذلك فإننا لا نذهب مع الاتجاهات الفقهية القائلة بأن نظام الأدلة العلمية سيكون نظام المستقبل ويسجل الخبير في القضاء فيكون الدور له وليس للقاضي، فيجعل رأي الخبير هو الحاسم لاقتناع القاضي.

رابعا:الضوابط التي تحكم اقتناع القاضي الجنائي لدليل الالكتروني.

إن القاضي الجنائي وان تمتع سلطة واسعة في تقديره للأدلة بما في ذلك الدليل الإلكتروني حيث ترك له المشرع سلطة واسعة، فله أن يتحرى الحقيقة بكافة الأدلة دون إلزامه بقيمة مسبقة لدليل ما حتى ولو كان دليلا علميا كدليل الالكتروني، أو تحديده لنوع معين من الأدلة لا يجوز الإثبات بغيرها، غير أن السلطة

[1]- راجع المواد (212، 307) من قانون الإجراءات الجزائية الجزائري والمواد (291/302، 1) من قانون الإجراءات الجنائية المصري.

[2]- سعيد السيد قنديل، مرجع سابق.ص225.

[3]- جميل عبد الباقي الصغير، مرجع سابق.ص23.

ليست مطلقة بل تخضع لمجموعة من الضوابط وهي بمثابة صمام أمان إزاء الخراف القاضي عند ممارسته لها كي لا تختل الأحكام [1].

أ-الضوابط المتعلقة بمصدرالاقتناع:

في هذا الشأن يحكم اقتناع القاضي بالأدلة الالكترونية مايلي.

شروط قبول الدليل الالكتروني:

إن القاضي ليس حر في تقدير أي دليل كان، بل هو حر في تقدير الدليل الالكتروني المقبول في الدعوى أي تم الحصول عليه بطريقة مشروعة إعمالا بمبدأ الشرعية الإجرائية، وبالتالي يستبعد في مقابل ذلك سائر الأدلة الالكترونية غير المقبولة، لأنها لا تدخل فمن عناصر تقديره [2] وعليه لا يجوز للقاضي الاستناد إلى دليل استمد من إجراءات باطلة لأن ما بني على باطل فهو باطل.

شروط وضعية الدليل الالكتروني: من القواعد الأساسية في الإجراءات الجنائية أنه لا يجوز للقاضي أن يبني حكمه على أدلة لم تطرح لمناقشة الخصوم في الجلسة، وهو ما يعبر عنه بوضعية الدليل، ومقتضى ذلك أن يكون للدليل أصل ثابت في أوراق الدعوى، وأن تتاح للخصوم فرصة الإطلاع عليه ومناقشته، ويقوم هذا الشرط على مبدأ الشفوية والمواجهة في المحاكمة الجنائية [3] وهو من المبادئ الأساسية في الإجراءات الجنائية نص عليه كل من المشرع الجزائري بموجب المادة 2/212 من ق.إ.ج.ج [4]، إذ ينبغي على القاضي أن يطرح كل دليل مقدم في دعوى المناقشة أمام الخصوم في الجلسة حتى يكونوا على بينة مما يقدم ضدهم من أدلة، وقد سار المشرع المصري على نفس المنهج وهذا حسب ما ورد بنص المادة 302 من قانون الإجراءات الجنائية المصري يقولها، "و مع ذلك لا يجوز له أي القاضي أن يبنى حكمه على أي دليل لم يطرح أمامه في الجلسة ". وقد عبرت عنه أيضا محكمة النقض المصرية بقولها " من المقرر أن لمحكمة الموضوع أن تستخلص من جماع الأدلة والعناصر المطروحة أمامها على سياق البحث الصورة واقعة الدعوى جسما يؤدي إليه اقتناعه وأن تطرح ما يخالفها من صور أخرى لم تقتنع بصحتها مادام استخلاصها شائعا ومستندا إلى أدلة مقبولة في العقل والمنطق ولها أصل في الأوراق [5].

---

[1]- يزيدبوحليط، مرجع سابق ، ص414.

[2]- محمد زكي أبوعامر، مرجع سابق، ص139.

[3]- يزيدبوحليط، مرجع سابق ، ص415.

[4]- نص المادة 2/212 من قانون الإجراءات الجنائية الجزائري ينص على "ولا يسوغ للقاضي أن يبني قراره الأعلى الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضور يا أمامها.

[5]- سعيد السيد قنديل، مرجع سابق، ص 236.

كما يشمل الدليل الالكتروني على عناصر أساسية تتيح فرصة الخصوم في الاطلاع على الدليل الالكتروني والرد عليه إذ يجب على القاضي أن يطرح كل دليل مقدم في الدعوى للمناقشة أمام الخصوم حتى يكونوا على بينة مما يقدم ضدهم من أدلة ليتمكنوا من مواجهة هذه الأدلة والرد عليها، وذلك احتراما لحقوق الدفاع.

و يتطلب مبدأ المواجهة نوعين من الضمانات منها مبدأ مواجهة المتهم بالتهمة المستوية إليه وان يمنح له الوقت الكافي لتحضير دفاعه وكذا الاستعانة عند الاقتضاء بمترجم أما النوع الآخر من الضمانات، يتمثل في السماح لكل طرف بتقديم ما لديه من مستندات، وسؤال الشهود إثارة أي دفوع، إيداع مذكرات.

كما يشمل على عنصر آخر أكثر أهمية يتمثل في ضرورة أن يكون لدليل الالكتروني أصل في أوراق الدعوى،ومن اجل ذلك أوجب المشرع تحرير محضر الجلسة لإثبات وقائع الدعوى الجنائية وأدلتها لكي يتمكن قاضي الموضوع أو أي من الخصوم من الرجوع إلى هذا المحضر وذلك منعا لتحكم وتحقيقا لعدالة، وبإضافة إلىذلك، فإن هذا التدوين يمكن المحكمة المطعون أمامها من مراجعة الحكم المطعون فيه وتقديره من حيث الخطأ والصواب [1].

ب-الضوابط المتعلقة بالاقتناع ذاته.

يتيح مبدأ الإثبات الجنائي حرية كبيرة للقاضي في تقدير عناصر الإثبات بما في ذلك الأدلة الرقمية وعليه فإن تقدير كفاية أو عدم كفاية الدليل الالكتروني في إثبات الجريمة الالكترونية ومنبتها إلى مرتكبها أمر متروك لمحكمة الموضوع المعروض عليها الدليل، ولا تخضع في ذلك لرقابة محكمة النقض التي يقتصر دورها على مراقبة المنطق القضائي لمحكمة الموضوع عن طريق رقابتها على صحة تسب بالحكم [2] وبناء على ذلك سوف نعرض القيود التي تحكم الاقتناع ذاته إلى.

- بلوغ الاقتناع القضائي درجة اليقين.

و هذا يستوجب أن تقترب اقتناع القاضي بدرجة اليقين قدر المستطاع وأن يتجلى القانون والتخمينات، ويمكن أن يصل إلى يقين بمن طريق المعرفة الحسية التي تدركها حواس من خلال معاينة هي الأدلة، واستقراءات واستنتاجات ليصل إلى الحقيقة التي يهدف إليها ويتجنب أن يصدر حكمه استنادا إلى معايير غير منطقية [3].

[1]- محمود نجيب حسني، مرجع سابق، ص210.

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص276.

[3]- يوسف بن سعيد الكلباني، مرجع سابق، ص 426.

- توافق الاقتناع القضائي مع مقتضيات العقل والمنطق

و معنى ذلك أن يكون استخلاص محكمة الموضوع لوقائع الدعوى استخلاص معقولا سائغا، لمعيار معقولية الاقتناع بما في ذلك الأدلة الرقمية، أي أن تكون هذه الأدلة مؤدية إلى مارتبه الحكم عليها من غير تعسف في الاستنتاج ولا تعارض مع مقتضيات العقل والمنطق [1] وفي ذلك قضت محكمة النقض المصرية " أنه وإن كان من حق محكمة الموضوع أن تستخلص الواقعة من أدلتها وعناصرها المختلفة إلا أنشرط ذلك أن يكون هذا الاستخلاص سائغا يؤدي إليه ظروف الواقعة وأدلتها وقرائن الأحوال فيها [2].

- مناقشة الأدلة الالكترونية.

إذا كانت مخرجات الوسائل الالكترونية تعد أدلة إثبات في أوراق الدعوى التي ينظرها القاضي، فإنه يجب عليه مناقشتها أمام الخصوم ويترتب على ذلك أن بهذه المخرجات سواء كانت مطبوعة أم بيانات معروضة على كانت بيانات مدرجة في حاملات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية، تكون محلا للمناقشة عند الاعتماد عليها كأداة أمام المحكمة [3] وتأسيسا على ذلك يجب أن تدبي شفاهة وفي حضور جميع الخصوم، أي أن القاضي لا يمكن أن يؤسس اقتناعه الأدنى عناصر الإثبات التي صرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى كما ينبغي على جراء الأنظمة المعلوماتية على اختلاف تخصصاتهم [4] فإذا كان القاضي الجنائي يحكم باقتناعه هو وليس باقتناع غيره، فإنه يجب عليه أن يعيد تحقيق كافة الأدلة القائمة في الأوراق لكي يتمكن من تكوين اقتناعه، ويترتب على ذلك المبدأ أن القاضي لا يمكنه أن يحكم في الجرائم الالكترونية استنادا إلى علم شخصي له أو استنادا إلى رأي الغير إلا إذا كان الغير من الخبراء وقد ارتاح ضميره إلى التقرير المحرر منه فقرر الاستناد إليه ضمن باقي القائمة في أوراق الدعوى المعروضة عليه، بحيث أن الاقتناع الذي يكون قد اصدر حكمه بناءا عليه متولد من عقيدته هو وليس من تقرير الخبير [5] ففي فرنسا نص قانون الإجراءات الجنائية في الفقرة الثانية من المادة 427 على هذه القاعدة الهامة بالقول "لا يجوز للقاضي أن يؤسس حكمه إلا على أدلة طرحت عليه

[1]- يزيدبوحليط، مرجع سابق، ص416.

[2]- يوسف بن سعيد الكلباني، مرجع سابق، ص 203

[3]- هلالي عبد الله أحمد، مرجع سابق، ص104.

[4]- محمد فهمي طلبه، مرجع سابق، ص21.

[5]- يوسف بن سعيد الكلباني، مرجع سابق، ص426.

أثناء المحاكمة ونناقش أمامه في مواجهة الأطراف وكذلك فإن قاعدة وجوب مناقشة الدليل الجزائي من القواعد الأساسية في القانون الإنجليزي [1].

ثالثا: القيود الواردة على حرية القاضي الجنائي في قبول الدليل الالكتروني.

إذاكان من المسلم به أن للقاضي الجنائي حرية الاستعانة بكافة وسائل الإثبات اللازمة بما في ذلك الدليل الالكتروني لتكوين عقيدته، فإنه يثور التساؤل حول نطاق هذه الحرية وما إذا كانت حرية مطلقة أو نسبية ؟ وإذا لما تعمقنا في دراسة هذه السلعة لا نجدها مطلقة وتحكيمية، بل وشع المشرع، لها مجموعة من القيود ومن جهة أخرى يكتسب هذا القيد أهمية كبرى نتيجة التقدم الهائل الذي تحقق في السنوات الأخيرة في شأن الوسائل الفنية للبحث والتحقيق والتي تسمح أكثر فأكثر لاختراق مجال الحياة الخاصة

أ- مشروعة الدليل الالكتروني

يجب أن تكون الأدلة الرقمية تم الحصول عليها من الوسائل الالكترونية بصورة مشروعة غير مخالفة لأحكام الدستور ولا لقانون العقوبات وأن تكون مبنية على قواعد الأخلاق والنزاهة واحترام القانون، فمبدأ مشروعية الدليل الجنائي بالنسبة لمخرجات الوسائل الالكترونية يتطلب ضرورة صحة إجراءات الحصول على هذه المخرجات بما يتفق والقواعد القانونية والأنظمة الثانية في وجدان المجتمع المتجهز، وعلى ذلك يجب أن تكون إجراءات جمع الأدلة المتحصلة من الوسائل الالكترونية ضمن الإطار العام الذي حدده الدستور [2]و إلا تكون باطلة ولا تصلح لأن تكون أدلة يتبنى عليها الإدانة في المواد الجنائية".

و على ذلك يجب أن تكون عقيدة القاضي واقتناعه بإدانة قد استمد من مخرجات كمبيوتر تم الحصول عليها بالطرق والإجراءات القانونية وليس بناءا على معلوماته الشخصية أو على ما قد يكون قد رآه بنفسه أو حقيقة في غير مجلس القضاء، لأن القاعدة هي أن لا يحكم إلا بناءا على التحقيقات ففي القانون الفرنسي نجد أن الإثبات الجزائي حر شرط أن يكون قد تم الحصول عليه وفقا لطرق قانونية ومشروعة فرغم أن قانون الإجراءات الجنائية الفرنسي لم يتضمن إليه نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة القضائية حتى بعد تعديلاته الأخيرة إلا أن العفة والقضاء كانا بجانب هذا المبدأ سواء في مجال التعقيب عن الجرائم التقليدية أم في مجال التنقيب عن جرائم الحاسب الالكتروني أما في هولندا، فإذا يؤدي

[1]- فهد عبد الله العبيد العازمي، مرجع سابق، ص360.

[2]-مأمون محمد سلامة، قانون الإجراءات الجنائية معلقا عليه بالفقه والقضاء، القاهرة، دار الفكر العربي، مصر، 1981، ص 372.

إلى نتيجة مؤداها ضرورة محو هذه البيانات وعدم إمكانية استخدامها كدليل جنائي بسبب مبدأ استبعاد الأدلة غير القانونية [1]

ب- مشكلة تغليب المصلحة العامة الخاصة "مشروعة الدليل"

و هي الحالة التي يكون فيها الدليل الالكتروني غير مشروع كأثر النقدي على الحياة الخاصة من جهة وفي نفس الوقت يعد وسيلة إثبات الجرائم التي تهدد أمن ونظام المجتمع الأخلاقي فأي المصلحتين أولى بالرعاية، فإذا كان البعض يشكك في مشروعية الدليل الالكتروني باعتباره طريقة لتدخل في حياة الخاصة للأفراد، لا سيما في مجال الجرائم الجنسية، حيث يكون السلوك الجنسي برضاء المشتركين فيه، إلاأننا نرى أن الاستعانة بالوسائل العلمية الحديثة مثل الانترنت واستخدامه كدليل على وقوع جريمة نشر المطبوعات الفادحة يستهدف المصلحة العامة، وإذا تم التسليم بالقول بأن هناك تعد على الحريات أفراد فإنه يعد تمثيل للغاية، ومما يتعين الاعتداء به هو مدى خطورة العدوان أو المساس بالنظام الاجتماعي، فلا يمكن استبعاد كل وسيلة لمجرد مناقشتها للقواعد العامة دون دراسة أو تعمق لآثارها في المجتمع [2].

ج- قيمة الدليل غير المشروع

- في النظام اللاتيني:

انطلاقا من قاعدة أن الأصل في الإنسان البراءة فإن المتهم يجب أن يعامل على أساس انه بريء في مختلف مراحل الدعوى إلى أن يصدر بحقه حكم نهائي، باب وهذا يقتضي أن تكون الأدلة التي يؤسس عليها حكم الإدانة مشروعة سواء كانت تقليدية أو ناتجة على الوسائل الالكترونية، وانطلاقا من ذلك الدليل الالكتروني، وهي القاعدة متبعة في قانون الإجراءات الجزائية الجزائري [3] ونفس النهج سار عليه المشرع المصري من خلال ما جاءت به المادة 336 من قانون الإجراءات الجنائية المصري والتي جاء فيها.

إذا تقرر بطلان إجراء، فإنه يتناول جميع الآثار التي تترتب عليه مباشرة ويلزم إعادته متى أمكن ذلك.

أما بالنسبة لدليل البراءة فهناك اختلاف فقهي حول مدى اشتراط المشروعية بوجه عام في دليل البراءة.

[1]- أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دراسة مقارنة، ط2 دار النهضة العربية، القاهرة 1198، ص93.

[2]- سعيد السيد قنديل، مرجع سابق ص206.

[3]- تنص المادة 1/157 من قانون إجراءات جزائية الجزائري، تراعي الأحكام المقررة في المادة المتعلقة باستجواب المتهمين والمادة (105) المتعلقة سماع المدعى المذنب وإلا ترتب على مخالفتها بطلان الإجراء نفسه وما يتلوه من إجراءات.

الاتجاه الأول: يرى أن المشروعية لازمة في كل دليل سواء أكانإدانة أو براءة وذلك تأسيسا على نص المادة 336 من قانون الإجراءات الجنائية المصري التي تقرر بطلات جميع الآثار المترتبة من الإجراء الباطل دون تفرقة بين دليل إدانة ودليل براءة [1].

الاتجاه الثاني: يرى أن المشروعية لازمة في دليل الإدانة دون البراءة تأسيسا على أن المحكمة لا تحتاج إلى اليقين في إثبات البراءة بل يكفي في ذلك الشك وهو ما يمكن الوصول إليه من خلال أي دليل ولو كان غير مشروع، وتعتنق محكمة النقض هذا الاتجاه [2]

الاتجاه الثالث :يرى ضرورة التفرقة بين ما إذا كان دليل براءة قد تم الحصول عليه نتيجة سلوك يعد جريمة جنائية وما إذا كان قد تم الحصول عليه نتيجة سلوك بشكل مخالفة لقاعدة إجرائية، فإذا كان الأول وجب إهدار الدليل وعدم الاعتداد به، لأن القول بغير ذلك مفاده استثناء بعض الجرائم من العقاب والدعوى إلى ارتكابها وهو مالا يجوز وتأباه الشرائع القومية [3].

- قيمة الدليل الغير المشروع في النظام الانجلو امريكي

و عليه سوف نتناول من خلال التالي نموذجين من القوانين وهما كآتي.

- **بالنسبة لقانون الإنجليزي**:القاعدة الأساسية في نظام القانون العام انه متى كان الدليل منتجا في الإثبات فهو مقبول أيا كانت الطريقة التي تم الحصول عليه من خلالها، أي حتى لو كان ذلك بطريق غير مشروع [4] وطبقا لذلك نصت المادة 76 منه منظمة لقواعد استبعاد الاعتراف الذي يتم إما باستعمال وسيلة سرية ضد المتهم، أو أنه غير حقيقي، أو لا يعتمد عليه أي قبل أو حصل من أي شخص غير المتهم أما المادة 87 نظمت السلطة التقديرية للقضاء في استبعاد الدليل حيث يجوز للمحكمة أن ترفض السماح بقبول الأدلة التي قدمها الادعاء، إذ ظهر للمحكمة من خلال تقدير كافة الظروف بما فيها الظروف التي تم فيها تحصل الدليل وتطبيقا لذلك ورفض القاضي في إحدى القضايا قبول تسجيلات على أساس أنها تمت من خلال تقدير كافة الظروف بما فيها الظروف التي تم فيها تحصل الدليل وتطبيقا لذلك ورفض القاضي في إحدى القضايا قبول تسجيلات على أساس أنها تمت من خلال شرك خداعي حيث قام البوليس بتركيب جهاز

[1]- محمود نجيب حسن، مرجع سابق، ص438.

[2]- وقد عبرت عنه محكمة النقض يقولها إن كان يشترط في دليل الإدانة أن يكون مشروعا إذ لا يجوز أن يكون مشروعا إذ لا يجوز أن تبنى إدانة صحيحة على دليل باطل في القانون، إلاأن المشروعية ليست بشرط واجب في دليل البراءة، ذلك انه من المبادئ الأساسية في الإجراءات الجنائية أن كل متهم يتمتع بقرينه البراءة حتى يحكم بإدانته نهائيا.

[3]- سعيد السيد قنديل، مرجع سابق.ص211.

[4]- أحمد عوض بلال، مرجع سابق.ص 41.

التنصت على خط تيليفون إحدى الشاكيات بناء على موافقتها، وقد افتعلت الشاكية عدة مكالمات تليفونية مع الشخص محل الاشتباه، وقد تم تسجيل هذه المكالمة التي تضمنت موضوعات تدين المتهم [1].

- **بالنسبة لقانون الأمريكي**: كان القضاء الأمريكي في البداية تبنى القاعدة الإنجليزية التي سادت في نظام القانون العام، أي عدم استبعاد الأدلة المتحصلة بطرق غير مشروعة، إلىأن لاحظت المحكمة الفدرالية العليا بطريقة عارضة عام 1886.

إلا انه يرد على ذلك بعض الاستثناءات فالمحكمة العليا التي نشأت قاعدة الاستعباد حددت، ربع حالات لا يتم فيها الاستبعاد وهي توافر حسن النية لدى رجال الشرطة الذي يقوم بالعمل الإجرائي ويستند في ذلك على أساس قانوني صحيح، وثاني هذه الحالات عندما تكون الصلة بين العمل الإجرائي المخالف والدليل المتحصل من ذلك الإجراء ضعيفا وبسيط لدرجة عدم اكتشاف الخطأ أو المخالفة وثالث هذه الحالات عندما يتم الحصول على الأدلة بصورة مستقلة عن العمل الإجرائي المخالف ورابع هذه الحالات، إذا كانت الأدلة ذاتها لا يتم اكتشافها إلا بارتياد السبيل القانوني الصحيح

وتأكيد على ذلك، خصص المشرع الأمريكي مبحث خاصا وهو المبحث الخامس في المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الالكتروني، يتعلق بعلاج انتهاكات الباب الثالث وقانون التسجيل والقصي، ويقصد به علاج بطلان الإجراءات غير المشروعة غير المشروعة في الحصول على الدليل الالكتروني حيث نص في ذلك على انه يجب على رجال الضبط القضائي والمدعيين العموميين سلوك مسك أوامر الباب الثالث وقانون التسجيل والتقصي، عند التخطيطات للمراقبة الالكترونية للمراقبة الالكترونية، إذ يمكن أن تسفر الانتهاكات عن غرامات وجزاءات مدنية وإجراءات جنائية ويصلان الدليل الذي تم الحصول عليه [2]

- القيود المستمدة من نصوص قانونية خاصة

إنالإثبات المسائل غير جنائية التي تطرح على المحكمة الجنائية، يخضع للقانون الخاص وهو ما نصت عليه نص المادة 225 من قانون الإجراءات الجنائية المصري "تتبع المحاكم المقررة في القانون الخاص بتلك المسائل. غير أن تقييد القاضي الجنائي بوسائل الإثبات عنصر مفترض في الجريمة سابقا في وجودها على

[1]- سعيد السيد قنديل، مرجع سابق.ص213.

[2]- سعيد السيد قنديل،مرجع سابق، ص 400

ارتكاب العقل الإجرامي بمعنى إلا تكون هذه المسالة هي ذاتها الفعل الإجراميالانجازإثباتها بكافة طرق الإثبات بما فيها الدليل الالكتروني باعتبارها مسالة جنائية [1]

وتجدر الإشارةإلىأن تقييد القاضي الجنائي عند تقديره لدليل الالكتروني بضوابط معينة سواء كانت متعلقة بهذا الدليل ذاته أو متعلقة بهذا الدليل ذاته أو متعلقة بالاقتناع، غير كافية لضمانة منع الاستبداد والتحكم، بل لابد من ضمانة أخرى اشد من سابقيها، لتجعل سلطة القاضي الجنائي، التقديرية تدور في إطار معتدل بهدف الوصول إلى الحقيقة الواقعية باعتبارها غرض الدعوى الجنائية.

[1]-محمد محمود مصطفى، مرجع سابق ، ص428

الفصل الثاني

التعاون الدولي لمكافحة جرائم الاعتداء على التوقيع الالكتروني

تعد جرائم التوقيع الالكتروني إحدىأهم صور الجرائم ذات البعد الدولي العابر للحدود فلم تعد الحدود القائمة بين الدول تشكل حاجز أمام مرتكبي هذه الجرائم كما أن نشاطهم الإجرامي لم يعد قاصرا على إقليم معين بل امتد إلىأكثر من إقليم بات المجرم يشرع في التحضير لارتكاب جريمته في بلد معين ويقبل علىالتنفيذفي بلد آخر ويهرب إلى بلد ثالث للابتعاد عن أيدي أجهزة العدالة فجريمة أصبح لها طابع دولي والمجرم ذاته أصبح مجرما وليا لذا ظهرت أهمية التعاون الدولي لمكافحة جرائم الاعتداء جمع الاستدلالات لتتبع الجاني وكذا تعزيز التعاون الأمني بين السلطات البوليس دوليا وعقد اتفاقيات دولية وإنشاء قنوات جديدة للاتصال بين تلك الجهات وتدعيم التعاون بين البوليس الإقليمي اليورو يول وتطوير أجهزة الشرطة الوطنية في الدول المنظمة لملاحقة وتسليم المجرمين ومنعهم من الإفلات من العقاب فمكافحة مرتكبي تلك الجرائم إذا لا يتحقق إلاإذا كان هناك تعاون على المستوى الإجرائي الجنائي بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة وذلك عن طريق إنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالانترنت.

وعلى ذلك فسوف نتناول ها الفصل في مبحثين نتناول في

المبحث الأول: التدابير الدولية لمكافحة جرائم الاعتداء على التوقيع الالكتروني

المبحث الثاني: التعاون القضائي الدولي لمكافحة جرائم الاعتداء على التوقيع الالكتروني.

المبحث الأول: التدابيرالدولية لمكافحة جرائم الاعتداء على التوقيع الالكتروني

تتسم جرائم التوقيع الالكتروني بالنظر إلى طبيعتها، بطابع دولي لذا لا تستطيع الدول بجهودها المنفردة القضاء على هذه الجريمة لذا من الضروري أن تساعد الدول بعضها البعض في تقديم الأدلة وان يكون المحققون والنواب العامون على دراية بآليات المتبعة للحصول على هذه المعلومات ويتحقق هذا التعاون عقد اتفاقيات دولية وتدعيم التعاون مع البوليس الدولي أما على المستوى الوطني لابد من خلق أجهزة اتصال متطورة تتماشى وطبيعة الجرائم المرتكبة وتطوير الجانب البشري من ضبطية قضائية إلى قضاة ونيابة العامة لتعامل مع هذه الجرائم والقبض على مجرمين إضافة إلى تنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وتقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في دول الأعضاء وتتمثل الإجراءات الجنائية في إجراءات ضبط مرتكبيها من قبض وتفتيش وتسليم لتصبح منطقة قضائية واحدة بالنسبة لهذه الجرائم ومن ثم فان تسليم المجرمين الذين تثبت إدانتهم في جرائم الاعتداء على التوقيع الالكتروني أصبح ضرورة ملحة طالما أننا اعترفنا بضرورة التعاون الدولي لمكافحتها.

المطلب الأول: التدابير الدولية الإجرائية الواجب مباشرتها على مستوى جهات المكافحة

في ضوء التزايد المستمر والمطرد لجرائم المعلومات بوجه عام والتوقيع الالكتروني خاصة قامت العديد من الدول بإنشاء جهات مختصة لتعامل مع هذا النوع من الجرائم ودعمت تلك الدول هذه الجهات بالفنيين المتخصصين ورجال البحث الجنائي الدربين تدريبا خاصة لمكافحة هذا النوع من الجرائم ونظرا للطبيعة الدولية لهذه الجرائم وكونها متعدية للحدود، أبرمت العديد من الاتفاقيات وانعقدت المؤتمرات الدولية والإقليمية وطنية وعلى هذا الأساس سنقسم دراستنا لهذا المطلب في الفروع التالية:

الفرع الأول: جهات مكافحة جرائم التوقيع الالكتروني على المستوى الدولي

لما كانت جرائم المعلومات والتوقيع الالكتروني ليس لها حدود جغرافية فان ملاحقة مرتكبيها وضبطهم ومحاكمتهم وعقابهم على ما ارتكبوه من جرائم يتطلب وجود آليات ومعايير دولية يتم الالتزام بها دوليا لضبط المتهمين أو جمع الأدلة أو مناقشة الشهود، أو اللجوء إلى الإنابة القضائية أو تبادل المعلومات وفي ضوء ذلك سوف نقسم هذا الفرع إلى النحو التالي

أولا: التدابير الإجرائية الصادرة من المجلس الأوروبي

اصدر المجلس الأوروبي التوجيه رقم 95 في عام 1990 وضح فيه بعض التدابير الإجرائية لتعزيز التعاون الدولي في مجال الإجرائي لمكافحة جرائم الاعتداء على التوقيع الالكتروني حيث حث الدول الأعضاء في المجلس لتحديث قوانين الإجراءات الجنائية الوطنية بما يلاءم هذا التطور[1] واهم ما ورد في هذه التوصيات هو

- إن تحول النصوص الإجرائية للسلطة القائمة بالتفتيش ضبط برامج الكمبيوتر وقواعد البيانات الموجودة بالأجهزة وفقا لذات إجراءات التفتيش التقليدية.
- النص على مد الإجراءات إلى أنظمة كمبيوتر أخرى قد تكون موجودة خارج الدولة، ويقتضي الأمر التدخل السريع، وحتى لا يمثل هذا الأمر اعتداء على سيادة الدولة أو القانون الدولي، وجب وضع قاعدة قانونية صريحة ستسمح بسهولة تطبيق هذا الإجراء[2]
- تعديل القوانين الإجرائية بما يمكن سلطات التحقيق أمر للغير بان يقدم المستندات الالكترونية المخزنة في الجلسة متى كانت تفيد في كشف الحقيقة في جريمةضرورية من أجل تخويل سلطانة المختصة سلطة التفتيش أو الولوج بطريقة مشابهة لنظام معلوماتي أو جزء منه وكذلك لبيانات المعلوماتية المخزنة فيه وعلى أزمنة ولدعامة تخزين معلوماتية تسمح بتخزين بيانات معلوماتية.

ثانيا: المنظمة الدولية لشرطة الجنائية "انتربول" لمكافحة جرائم التوقيع الالكتروني.

تعد المنظمة الدولية للشرطة الجنائية "انتربول""OPIC"[3] من أهم الأجهزة الدولية في مجال مكافحة جرائم الاعتداء على التوقيع الالكتروني، وتتخذ من باريس مقرا لها وتعمل هذه المنظمة على تشجيع التعاون المتبادل بين أجهزة الشرطة في الدول بما يحقق مكافحة فعالة للجريمة، كما أنها ستهم في إقامة النظم التي تساعد على منع ومكافحة جرائم القانون العام وتقوم منظمة الانتربول بذلك من خلال وظيفتين:

1-جمع البيانات والمعلومات المتعلقة بالجريمة والمجرم بواسطة المكاتب المركزية الوطنية، لها والمتواجدة في أقاليم دون الأعضاء.

[1]- مدحت عبد الحليم رمضان، مرجع سابق، ص 76.

[2] -Alain Bensoussan, internet aspect juridique, HERMES, paris, France, 2eme édition, 1998, p.20

[3]- فهد عبد الله العبيد العازمي، مرجع سابق، ص 650.

2-التعاون في ضبط وملاحقة المجرمين الهاربين وتسليمهم إلى الدول طالبة التسليم:

وهي تختصفي هذا بالجرائم ذات الطابع الدولي وخاصة المتعلقة بالعنف ضد الأطفال وجرائم الأموال[1]، كما تختص بالجرائم العابرة للحدود وخاصة جرائم التوقيع الالكتروني ويدل على ذلك قيام المنظمة في مؤتمر جرائم الانترنت المنعقد في لندن في 2005/10/9 بالدعوى إلى إيجاد تعاون دولي فعال لمكافحة هذا النوع من الجريمة، كما دعى إلى ذلك أيضا المدير التنفيذي للخدمات الشرطية السيد لوبوتان في المؤتمر الدولي السادس بشأن الجرائم المعلوماتية المنعقد في القاهرة في الفترة 2005/4/15 وهو أيضا ما أكدته المنظمة في المؤتمر الدولي الذي انعقد في كوريا الجنوبية.

و تقوم منظمة الانتربول الآن بدور رئيسي في مجال تبادل المعلومات وتعميم التحذيرات والتنبيهات المتضمنة المعلومات الاستخبارية والإحاطات والمستورة التحليلية والفنية عن الأخطار الإجرامية المحتملة، والتقصي في قواعد البيانات، وتقديم الخبرات والدورات التدريبية في مجال مكافحة جرائم التوقيع الالكتروني وتسيير تبادل وتحليل وتخزين البيانات الجنائية كما أنشأت منظمة الانتربول وحدات لمكافحة جرائم التكنولوجيا، ما قامت بوضع استراتيجيات محكمة لمواجهة هذا النوع من الجرائم بالتعاون مع مجموعة الثماني من خلال الآليات الآتية [2].

-إنشاء مركز الاتصالات أمني عبر شبكة الانترنت يعمل على مدى اليوم الكامل طوال الأسبوع في كل إدارات الشرطة في الدول الأعضاء في المنظمة.

-استخدام وسائل حديثة في تلك المكافحة كقواعد البيانات المركزية، كما تقوم المنظمة بتزويد أجهزة الشرطة في دول الأطراف بكتيبات إرشادية حول جرائم المعلومات والتوقيع الإلكتروني، وكيفية التدريب على مكافحتها والتحقيق فيها، ومثال ذلك ما قدمته للشرطة الأوروبية والمسمى دليل جرائم الحاسب الآلي.

-يتولى الانتربول إقامة العلاقات بين الدول المنظمة وتبادل المعلومات بين سلطات التحقيق بشأن الجرائم الحادثة في نطاق عدة دول كجرائم التوقيع الالكتروني والانترنت بصفة عامة.

ثالثا: الاتحاد الدولي للاتصالات

لقد استحدث الاتحاد الدولي للاتصالات دليلا الكترونيا لتتبع المعايير الأمنية الخاصة بتكنولوجيا المعلومات والاتصالات لمكافحة الجريمة عبر الانترنت وذلك بالتعاون المشترك مع الوكالة الأوروبية

[1]- حسام محمد نبيل الشنراقي، مرجع سابق، ص738.

[2]- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى ، 2006 ، ص155.

المختصة بأمن الشبكات والمعلومات وأطراف دولية أخرى للاهتمام بشؤون الأمن المعلوماتي على شبكة الانترنت تعتمد على مفهوم أن تنهض جهة واحدة بذلك التتبع، ما يمكن المعنيين من الرجوع إليها ومتابعتها [1] لتوحيد المرجعية لعدم تشتيت الجهود والمهام ووصف الدليل بأنه "خريطة طريق" فيما يتعلق بمعايير الأمن الخاصة بتكنولوجيا المعلومات والاتصالات حيث يستطيع أن يلاحق المعلومات بأحدث المعايير الأمنية المتجددة باستمرار، ثم يصبها في قاعدة بيانات نفتح أمام المعنيين بما يسهل مهمة البحث عن المعلومات المطلوبة، ويعرض الدليل أسماء المنظمات المعنية بتطوير المعايير وما تنشره من صيغ خاصة بأمن الانترنت مما يجنب تكرار الجهود كما يسهل مهمة مهندسي أمن الشبكة الالكترونية في كشف الثغرات التي تهدد أمنها ويضم الدليل خمسة أقسام تحدث بصفة مستمرة وتتناول منظمات تطوير المعايير الخاصة بتكنولوجيا المعلومات والاتصالات وإعمالها والصيغ المعتمدة لتلك المعايير وطرق إقرار الاتفاق عليها.

و إلى جانب الاتحاد الدولي للاتصالات يوجد مؤسسات دولية أخرى كمؤسسة الانترنت للأسماء والأرقام المخصصة ICANW ومنتدى إدارة الانترنت IFG ومنظمة التعاون الاقتصادي والتنمية OECDومجموعة الثمانية الاقتصادية G8.....الخ هذه المؤسسات الدولية التي تسعى لمواجهة الجريمة المعلوماتية الرقمية عبر الانترنت.[2]

رابعا: التدابير الإجرائية لمكافحة جرائم التوقيع الالكتروني الصادرة عن الجمعية الدولية لقانون العقوبات.

و قد تبنى المؤتمر الدولي الخامس عشر للجمعية العامة لقانون العقوبات للعديد من التوصيات التي تتعلق بالتدابير الإجرائية والتي تنطبق على جرائم الاعتداء على التوقيع الالكتروني ومنها [3].

-آن تمكن سلطات التحقيق والتحري سلطات قسرية كافية تتعادل مع الحماية الكامنة لحقوق الكانسان وحرمة الحياة الخاصة.

-أن يتم تحديدالسلطات التي تقوم بإجراء التفتيش والضبط عند التفتيش شبكات الحاسب.

[1]- وهذا ما اقره المجلس الأوروبي على مستوى الدول الأوروبية عندما اعتبر اتفاقية المجلس الأوروبي بمثابة النظام العام الأوروبي في مجال حماية شبكات الاتصالات عبر الانترنت ومكافحة الجريمة المعلوماتية الرقمية.

[2]- فهد عبد الله العبيد العازمي، مرجع سابق، ص665.

[3]- ايمن رمضان محمد أحمد، مرجع سابق، ص 398.

-السماح للسلطات المختصة باعتراض الاتصالات داخل نظام الحاسب ذاته أو بينه وبين نظم الحاسب الأخرى مع استخدام الأدلة التي يتم الحصول عليها في الإجراءات أمام المحاكم.

-يجب عند البدء في التحريات أن يوضع في الاعتبار، بإضافة إلى القيم المادية التقليدية كل القيم المرتبطة ببيئة تكنولوجيا المعلومات يجب أن تحدد بوضوح:

-السلطات التي تقوم بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات وخاصة ضبط الأشياء غير المحسوسة، تفتيش شبكات الحاسب.

-واجبات التعاون الفعال من جانب المجني عليهم "Victimes" والشهود Temoins وغيرهم من مستخدمي في تكنولوجيا المعلومات.

-السماح لسلطات العامة باعتراض الاتصالات داخل الحاسب ذاته مع استخدام الأدلة التي يتم الحصول عليها في الإجراءات أمام المحاكم [1].

خامسا: التدابير الإجرائية لمكافحة جرائم التوقيع الالكتروني وفقا لمؤتمر هافانا 1990.

أصدر مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء هفانا 1990 قرار بشأن الجرائم ذات الصلة بالكمبيوتر ومنها جرائم الاعتداء على التوقيع الالكتروني، الذي حث دول الأعضاء في مجال الجرائم ذات الصلة بالكمبيوتر أن تكثف جهودها كي تكافح عمليات إساءة استعمال الكمبيوتر التي تستدعي تطبيق جزاءات جنائية على الصعيد الدولي بالتدابير التالية [2].

-تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير المتخذة من أجل أمان أن تطبق الجزاءات والقوانين الراهنة، بشأن سلطات التحقيق وقبول الأدلة في الإجراءات القضائية على نحو ملائم وإدخال تغييرات مناسبة إذا دعت الضرورة إلى ذلك.

-تحسين تدابير الأمن والوقاية المتعلقة بالحاسوب مع مراعاة حماية الخصوصية واحترام حقوق الإنسان وحرياته الأساسية.

-اعتماد تدابير مناسبة لتدريب القضاة والمسؤولين والأجهزة المسؤولة عن منع الجرائم الاقتصادية والجرائم ذات الصلة بأجهزة الحاسوب والتحقيق فيها ومحاكمة مرتكبيها وإصدارالأحكام المتعلقة بها.

[1]- حنان محمد حسن، مرجع سابق، ص222.

[2]- ايمن رمضان محمد أحمد، مرجع سابق ، 402.

-التعاون مع المنظمات المهتمة بهذا الموضوع في وضع قواعد للأداب المتبعة في استخدام أجهزة الحاسوب وتدريس هذه الآداب ضمن المناهج الدراسية.

-اعتماد سياسات بشان خبايا الجرائم المتعلقة بالكمبيوتر تنسجم مع إعلان الأمم المتحدة بشأن مبادئ العدل المتعلقة بضحايا الإجرام والتعسف في استعمال السلطة وتتضمن إعادة الممتلكات التي يتم الحصول عليها بطرق غير مشروعة وتدابير لتشجيع الضحايا على إبلاغ السلطات المختصة بهذه الجرائم.

الفرع الثاني: جهات مكافحة جرائم التوقيع الالكتروني على المستوى الإقليمي.

لمكافحة جرائم التوقيع الالكتروني على الصعيد الإقليمي لا بد من تظافر جهود الدول ووجود آليات لضبط المتهمين وتقديمهم للمحاكمة وهذا ما سندرجه على النحو التالي

أولا:على المستوى الأوروبي.

اتفاق شحن "Schengen"، تم التوقيع على اتفاق Schengen عام 1985 ويهدف هذا الاتفاق إلىإلغاء الحدود بتوحيد مجالات التعاون بين أجهزة الشرطة لدول الأعضاء باستثناء فضاء جماعي من غير حدود سمي ب system information Schengenمن خلال التوقيع على شنجن في 1985/6/14 وقد استحدثت هذه الاتفاقية وسيلتين جديدتين لتعزيز التعاون الشرطي الأوروبي لمواجهة التحديات الأمنية التي فرضتها الظروف الجديدة ومنها جرائم الانترنت والتوقيع الإلكتروني وهاتان الوسيلتين هما [1]

1-**حق المراقبة غير المحدود:** حيث وإنه وفقا للمادة 40 من الاتفاقية يجب على رجل الشرطة في إحدى دول الاتفاقية أن يستمر في مراقبة شخص مشتبه فيه موجود في إقليم دولة أخرى طرف في الاتفاقية في إطار أعمال، جمع الاستدلالات التي بدأها لكشف غموض تلك الجريمة، ويخضع هذا الحق لعدة شروط لعدة شروط تختلف تبعا لما إذا كانت المراقبة تتم في الأحوال العادية أم أن هناك حالة ضرورة ففي الحالة الأولى يجب الحصول على إذن مسبق من الدولة المطلوب منها السماح باستمرار مراقبة المشتبه فيه من الجرائم التي يجوز فيها تسليم المجرمين.

أما في الحالة الثانية فيجوز لرجل الشرطة أن يتجاوز الحدود الإقليمية لدولة إلى إقليم دولة أخرى دون إذنها، وذلك في جرائم حددتها المادة 7 من المعاهدة.

[1]- حسام محمد نبيل الشنراقي، مرجع سابق، ص741.

2-الحق في ملاحقة المجرمين خارج الحدود.

نصت المادة 41 من الاتفاقية على حق رجل الشرطة التابع لدولة في ملاحقة أحد المجرمين على إقليم دولة طرف في حالتين: إذا كان المجرم قد ضبط في حالة تلبس بارتكاب إحدى الجرائم الجسيمة المحددة في هذه المادة على سبيل الحصر، وفي حالة هرب محبوس فتجيز الاتفاقية لرجل الشرطة أن يتجاوز حدود دولية لملاحقة المجرم على إقليم دولة أخرى طرف في الاتفاقية دون إذن منها ومن ناحية أخرى فقد نصت الاتفاقية على نظام تسجيل المعلومات يسمى "نظام معلومات شنجن" وهو يمثل قاعدة معلومات متعلقة بالأشخاص المطلوبين والأموال والأسلحة التي يتم البحث عنها، كما يساعد ذلك النظام في ملاحقة مرتكبي الجرائم عبر الانترنت ومنها جرائم التوقيع الالكتروني وقد تم إبرام اتفاقية تعاون بين الشرطة القضائية والجمارك في فرنسا وسويسرا في مارس 1998 لتسهيل مهام هذا النظام.

ب- الأوروجسيت:

كما يوجد على المستوى الأوروجيست كجهاز يساعد على التعاون القضائي والشرطي في مواجهة ومكافحة الجرائم الالكترونية ويهمنا في دراستنا جرائم التوقيع الالكتروني والذي تم إنشاؤه في 2002/2/28 من قبل مجلس أوروبا وينعقد له الاختصاص عندما تمس الجريمة دولتين على الأقل من أعضاء الاتحاد الأوروبي أو دولة عضو مع أخرى في العالم الثالث أو دولة عضو مع الرابطة الأوروبية، وتشمل في غير تلك الحالات المؤسسات، وتعد الاوروجيست دعامة فعالة في التحقيقات ومطاردة المتهمين بالتحليلات اللازمة لاستكمال التحقيقات في الجرائم ويتكون من نواب عموم ومستشارين القائمين بالضبط القضائي للدول أعضاء الاتحاد الأوروبي ذوي الاختصاص والمنتدبين، من كل دولة عضو في الاتحاد وفقا لنظامها القانوني، ويقوم بتحسين التنسيق والتعاون بين السلطات القضائية المختصة للدول الأطراف وتبادل المعطيات بين دول الاتحاد الأوروبي وكذا التحفظ عليها كما يمكنه أن يطلب من الوكلاء العامين ذوي الاختصاص الوطني إجراء التحقيقات أو الملاحقات أو التبليغ عن الجرائم السلطات.[1]

[1] - نبيلة هبة هروال، مرجع سابق، ص 159، 160.

ثالثا:على مستوى العربي

أ- القانون الجزائي العربي الموحد الاسترشادي:

اعتمد مجلس وزراء العدل العربي بتاريخ 19 نوفمبر 1996 القانون الجزائي العربي الموحد كقانون نموذجي وذلك بالقرار 12 -229[1]وقد حرم هذا القانون الاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية حيث جرمت المواد من 461-463 جمع المعلومات الاسمية أو معالجتها آليا، أو استعمالها بالمخالفة لأحكام القانون أو المساس بسرية معلومات الأشخاص وبمطالعة المادتين 462-463 نلاحظ أنهما تناولت صورتين من صور الجرائم الماسة بسرية المعلومات الالكترونية حيث تناولت المادة 462 جريمة الاعتراض غير القانوني للبيانات والمعلومات الشخصية لأفراد الطبيعيين فقط، حيث تنص تلك المادة على انه يعاقب بالحسب مدة تزيد على سنة وبالغرامة كل من حصل على معلومات السمية خاصة بالغير، أثناء تسجيلها أو ترتيها أوإرسالها بآلية وسيلة من وسائل المعالجة التي من شأنها إفشائها المس يسمعه المعنى بالأمر أو بحياته الشخصية، مما يمكن اطلاع على تلك المعلومات دون إذن المعنى بالأمر.

في حين تناولت الفقرة الأولى من المادة 463 جريمة الدخول غير الصريح أو البقاء داخل نظام المعالجة الآلية حيث تنص على " يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين، كل من دخل بطريق الغش إلى كامل أو جزء من نظام المعالجة الآلية للمعلومات أو بقى فيه وتضاعف العقوبات إذا تنتج في ذلك أما محو المعلومات التي تحتوي عليها النظام أو تعديلها، وهو ما يقابل نص المادة 2/462 من القانون الفرنسي الصادر 1988 بشأن جرائم الغش المعلوماتي والتي يقابلها المادة 1/323 من قانون الخاصة بجريمة الدخول غير القانوني أو البقاء داخل النظام المعلوماتي في هذا البحث [2]

ب- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010

أبرمت هذه الاتفاقية في 2010/12/21 ووقع عليها سبع عشرة دولة عربية [3] وقد عبرت المادة الأولى منها عن الهدف الذي تنشده وهو تعزيز التعاون فينما بين الدول العربية لمكافحة جرائم تقنية المعلومات

[1]- هذا القانون منشور على الموقع الالكتروني لجامعة الدول العربية

http://www.arableagueonline.org 6 جوان 2020 على الساعة 14:35

[2]- محمد كمال محمود الدوسقي، مرجع سابق، ص 200

[3]- نص هذه الاتفاقية منشورة على الموقع الالكتروني لجامعة الدول العربية

http://www.arableagueonline.org 05 جويلية 2020 على الساعة 10:00

التي تهدد أمنها ومصالحها، وسلامة مجتمعاتها، وذلك يتبنى سياسة جنائية مشتركة تهدف إلى حماية امن المجتمع العربي وأفراده ومصالحهم ضد تهديدات جرائم تقنية المعلومات، وقد جاءت هذه الاتفاقية بهد مطالبات عدة من قبل المختصين في أكثر من مناسبة بإصدار مثل هذه الاتفاقية حيث تصمن " إعلانالقاهرة لمكافحة الجريمة الالكترونية 2008 الصادر عن المؤتمر الإقليمي الأول دول الجريمة الالكترونية المنعقد في القاهرة نوفمبر 2007 دعوى الدول العربية إلىإسراع في إقرار تشريعات لمكافحة الجرائم الالكترونية، وتشجيع الدول المنطقة العربية للاسترشاد باتفاقية بودابيست بشان الجرائم المعلوماتية 2001 عند إعداد القوانين الموضوعية والإجرائية الخاصة بمكافحة الجرائم المعلوماتية، وبنظرة عامة على اتفاقية العربية لمكافحة جرائم تقنية المعلومات، يلاحظ أنهاشملت كافة المسائل اللازمة لمكافحة الجرائم المعلوماتية بشكل عام، من حيث الصور الإجرامية ومجالات التعاون القانوني والقضائي التي تتناسب وطبيعةالجرائم المعلوماتية من سرعة في جميع الأدلة وملاحقة المجرمين، وهو ما يكسبها قيمة وفاعلة في مجال مكافحة تلك الجرائم من جرائم الاعتداء على التوقيع الالكتروني:

- السماح أثناء عملية تنفيذ التفتيش للجهات القائمة بالتنفيذ بمد التفتيش إلى أنظمة الكمبيوتر الأخرى والتي تكون متصلة بالنظام محل التفتيش أو ضبط ما به من برامج ومعلومات بشرط أن يكون هذا الإجراء ضروري.

- يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال أجنبية لجمع أدلة معينة ويتعين عندئذ أنيسمح الأخيرة بالضبط والتفتيش وبالأخص عندما تكون هناك أسباب تدعو للاعتقاد بان هذه البيانات على وجه الخصوص معرضو للفقد أو التغيير

- تطوير وتوحيد أنظمة التعامل مع الأدلة الالكترونية والاعتراف بها بين الدول المختلفة كما يتعين تطبيق النصوص الخاصة بالأدلة التقليدية على الأدلة الالكترونية

- ضرورة النص على إلزام حارس البيانات أو أي شخص يقع عبئ التحفظ عليها أن يحافظ على السرية بالنسبة لهذه الإجراءات

- ضرورة النص على تحويل سلطات المختصة سلطة ضبط أو الحصول بطريقة متشابهة على البيانات المعلوماتية

- يجب على كل طرف أن يتبنى الإجراءات الأخرى التي يرى أنها ضرورية من اجل تأهيل سلطانة المختصة أنتآمر كل شخص ما على أرضه بإرسال بيانات معلوماتية معينة في حوزته أو تحت سيطرة هذا الشخص والمخزنة في نظام معلوماتي أو في دعامة تخزين معلوماتية

- مقدم الخدمة الذي يقدم خدماته علىأرض ذلك الطرف من اجل إرسال البيانات التي في حوزته أو تحت سيطرته والمتعلقة بالمشتركين بتلك الخدمات
- يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات يرى أنها

الفرع الثالث: جهات مكافحة جرائم التوقيع الالكتروني على مستوى الوطني

في ظل تزايد الجرائم التي تستهدف التوقيع الالكتروني في صورة المتعددة كجرائم الاحتيال والسرقة وللإتلاف والدخول غير المصرح به النظام معلومات التوقيع الالكتروني، وما يترتب عليه من خسائر مادية فادحة قررت الدول وضع حد لهذا النوع من الإجرامإنشاء أجهزة لمكافحته على المستوى الوطني فقد اتخذت تدابير تشريعية لمواجهة المخاطر التهديدات المتزايدة النامية عن إساءة استعمال تكنولوجيا المعلومات وذلك بين تشريعات خاصة أوأجراء تعديلات على قوانين العقوبات القائمة لديها على النحو الذي يكفل لمجتمعاتها الحماية اللازمة من هذه الإخطار وفي ضوء ما سبق سنتناول في هذا الفرع ابرز الجهود التشريعية على المستوى الوطني لحماية التوقيع الالكتروني وذلك على النحو الآتي:

أولا:على مستوى المجموعة اللاتينية:

ومن أبرز تطبيقاتها نجد

أ- فرنسا: من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية لمكافحة الجرائم المعلوماتية الرقمية عبر الانترنت على المستوى الوطني والدولي والأوروبي، حيث أصدرت القانون رقم 660 لعام 1980 برمجيات وقانون حماية وطبوغرافية منتجات الموصلات كما أصدرت في عام 1988 القانون رقم 19-88 وهو الخاص بالغش المعلوماتي 1980 والذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها، والقانون الفرنسي الصادر في 1991 أجاز اعتراض الاتصالات البعدية بما في ذلك شبكات تبادل المعلومات وخلف وسائل خاصة للتحقيق لاكتشاف الجرائم الخطيرة فمثلا يمكن للمحققين أن يشاركوا تحت اسم مستعار في المحادثات الالكترونية بدون أن يكونوا مسؤولين جنائيا [1]

ولتوسع دائرة ملاحقة مرتكبي جرائم الانترنت نجد أن المشرع الفرنسي اعتمد على العناصر التالية

- دعم قوات الشرطة المتخصصة في هذا المجال بزيادة عندهم بالإضافة إلى تحسين أسلوبهم وتقوية معارفهم القانونية

[1]- فهد عبد الله العبيد العازمي، مرجع سابق ، ص627.

- تنظيم منهج عالي المستوى من جانب المكتب المركزي لمكافحة الإجرام المرتب بتكنولوجيا المعلومات والاتصالات "OCLCTIC" والشرطة القضائية "CNFPG" ومعهد البحوث الجنائية التابع الدرك الوطني "IRCGN" يتم فيها مناقشة مواضيع ذات أهمية مثل مشاكس كل الاتصال اللاسلكي والتعريفات القانونية للاتصالات الالكترونية وغيرها بإضافة إلىإمداد رجال الضبط القضائي بوسائل تساعدهم على إجراء التحقيقات في تلك الجرائم وتختص بعمليات المكافحة في فرنسا العديد من الوحدات والمراكز المتخصصة وغير المتخصصة ضمن عناصر الشرطة والدرك الوطني ومن أهم هذه الوحدات:

- **القسم الوطني يقع جرائم المساس بأموال والأشخاص DNRAPB**

- وقد بدأ هذا القسم مهامه عام 1997 ويقوم بالتحقيق مجموعة من رجال البحث والتحري والمحققين المختصين في الجريمة المعلوماتية الرقمية عبر الانترنت، حيث تقوم السلطات مع قنوات التعاون القضائي الدولي بالحجز على عناوين ASRESS IP وأرقام بطاقات الائتمان التي تصل إلى قسم D.N.R.A.P.B.[1]

- **المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات**

ولقد تم إنشاؤه بموجب مرسوم وزاري رقم 2000 /405 في 15 /5/ 2000 على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية ويعد هذا المكتب الأساس في مكافحة جرائم الانترنت في فرنسا إلى جانب الوحدات ويساعده في نشاطاته كل من وزارة الدفاع المديرية العامة للشرطة الوطنية وزارة الاقتصاد والمالية والصناعة مديرية العامة للجمارك والحقوق غير المباشرة والمديرية العامة للمنافسة والاستهلاك وقمع الاحتيال [2] ويتحدد نطاقه في الجرائم الخاصة والمرتبطة بتكنولوجيا المعلومات والاتصالات سواء كانت تلك التكنولوجيا محلا للاعتداء أو وسيلة لارتكاب وتسهيل ارتكاب ذلك الاعتداء وهذا المكتب مكلفا وفقا للفقرة الثالثة من المرسوم كآتي –تنشيط وتنسيق عمليات الملاحقة لمرتكبي الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات سواء كانوا فاعلين أصليينأو شركاء

- مشاركة مصالح التحقيق التابعة لشرطة القضائية في إجراءات التحقيق في تلك الجرائم

- تقديم المساعدة لمصالح الشرطة الوطنية والدرك الوطني ومديرته العامة لجمارك والحقوق غير المباشرة، والمديرية العامة للمنافسة والاستهلاك وقمع الاحتيال.

[1]- فهد عبد الله العبيد العازمي، مرجع سابق ، ص 626.

[2]- نبيلة هبة هروال، مرجع سابق، ص 123.

- تحليل الشكاوى والبلاغات المقدمة من قبل مستخدمي الانترنت [1]

ويستعين المكتب المركزي لمكافحة جرائم التوقيع الالكتروني بثلاث جهات [2]

- الأولى: وحدة التحليل والتوثيق العملي: وتختص بتحليل ومعالجة المعلومات الواردة من السلطات القضائية المختصة بمكافحة الجرائم المرتبطة بتكنولوجيا والاتصالات سواء على مستوى الوطني او الدولي

- الثانية: وحدة المساعدات التقنية: وهي مدعمة بتقنيات أو برامج ذات مستوى تكنولوجي على التامين المساعدة في التحري والبحث وجمع الدليل الالكتروني وتضم عدد من المحققين المختصين في التحقيق في الإجرام المعلوماتي

- الثالثة: وحدة العمليات: وتتشكل من أربع فرق تختص إحداها بجرائم الاحتيال الواقعة على وسائل الدفع، أما البقية فتختص بالجرائم الواقعة على شبكات الاتصال

- **القسم المعلوماتي الالكتروني في التابع البحوث الجنائية لشرطة الوطنية IRCGN**

إنشاء هذا القسم سنة 1996 مهامه الأساسية تقديم المساعدة التقنية من خبرة ورقابة واعتراض وتحليل ومعالجة للبيانات المدمجة في الحواسيب الآلية في أيطارالأعمال الاقتصادية والمالية والمتعلقة بالتحقيقات القضائية خاصة تلك المرتبطة بأرصدة المؤسسات وكذا أعمال قرصنة البرامج أي النسخ غير المشروع والتوقيع الالكتروني ويقدم المساعدة لمصالح الدرك .

- **وحدات أقسام الاستعمالات والتحقيقات القضائية B D R I J**

وهي تختص بتجمع ومعالجة المعلومات لتخصصها وخبراتها في المواقع والاتصالات الالكترونية بالشبكات الدولية، عن الجرائم الواقعة عبر الشبكة الانترنت، وتقوم تلك الأقسام بتبادل الخبرات التقنية وكذلك الاختصاصات بين رجال الشرطة الوطنية

خلية استقبال وتحليل الانترنت

تختص هذه الخلية بتحليل المخاطر الناتجة عن استخدام شبكة الانترنت وتامين الرقابة على الشبكة لتامين وحماية الأعمال التجارية الالكترونية ولمواجهة الجرائم الالكترونية على الشبكة المعلوماتية

[1] - حسام محمد نبيل الشنراقي، مرجع سابق، ص 754.

[2] - ايمن رمضان محمد أحمد، مرجع سابق، ص 430.

- **المديرية العامة للمنافسة والاستهلاك وقمع الاحتيال:**

وهي تختص بحماية المستهلكين من المواقع المخالفة للخدمة الوطنية والأوروبية وكذلك قمع ومكافحة الاحتيال عبر المواقع التجارة الالكترونية [1]

ب- **بلجيكا**: أصدرت مجموعة من القوانين بشأن حماية البيانات الشخصية المعالجة آليا كقانون تنظم استخدام أجهزة الحاسوب في المعالجة الالكترونية لبيانات الشخصية 1989 وقانون حماية الحياة الخاصة فيما يتعلق بالتعامل مع المعطيات الشخصية 1992 وفي عام 2000 أجرى البرلمان البلجيكي تعديلا على قانون العقوبات وتحديدا تعديل المادة 550/ب تشتمل جرائم الكومبيوتر مثل الاختراق وإتلاف الكمبيوتر [2]

ج- **المانيا:** تم تعديل قانون العقوبات بإضافة قسمين الأول بشأن التجسس على البيانات والآخر إتلاف الكمبيوتر، بإضافة إلى قانون خاص بحماية المعطيات 1977 عدل جذريا بتاريخ 1990 كما تم تعديله 1994 [3]

ثانيا: دول المجموعة الانجلو أمريكية:

يرجع النظام الانجلو أمريكي أساس إلى القانون الإنجليزي القديم، حيث قام الانجليز بثقله إلى أمريكا الشمالية ويقوم هذا النظام على السوابق القضائيةفي مجال التجريم والعقاب ومن الدول التي تبنت هذا النظام انجلترا والولايات المتحدة الأمريكية وأستراليا وايسلندا وقد اصدر عدد كبير من دول هذه المجموعة تشريعات خاصة بحماية المعلومات والبيانات الالكترونية وفيما يلي تستعرض أهم جهود تلك الدول.

كما وقد خصصت بريطانيا وحدات متخصصة في مجال البحث والتنقيب عن جرائم المرتبطة بالانترنت وتضم هذه الوحدة 80 مفتشا من رجال الشرطة، الجمارك، أفراد من معالج استعمالات متمركزون في لندن وفي جميع المفتشيات الإقليمية التقليدية المتواجدة في إنجلترا وتتخلص مهام هذه الوحدة المتخصصة في مكافحة هذا النوع المستحدث من الإجرام والتي بدأت إعمالها عام 2001 في مجال

[1] - فهد عبد الله العبيد العازمي، مرجع سابق، ص 235.

[2] - يونس عرب ، مرجع سابق، ص 56.

[3] - أحمد خليفة المطلط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، 2000، ص 145.

متابعة مرتكبي الجرائم المعلوماتية ونشر الفيروسات والقرصنة المعلوماتية، كما تم إنشاء وحدة الجريمة الالكترونية في الشرطة المركزية "PCEU" وتختص بما يلي [1]

- تحليل وتطوير المعلومات الاستخباراتية حول الجريمة الالكترونية لإنتاج منتجات معلوماتية استخبارية.

- تطوير وصيانة تعاونية من الحكومة والشرطة والشركاء في الصناعة على الجريمة الالكترونية

- تبادل المعلومات والاستخبارات المعلقة بالجريمةالالكترونية مع أصحاب المصلحة الرئيسين بما في ذلك الدوائر الحكومية والشركاء في الصناعة والأوساطالأكاديمية

- توفير التعليم وتقديم المشورة للوقاية من التعرض للجريمة الالكترونية

- تعزيز معايير الإجراءات والتدريب والتصدي للجريمة الالكترونية

أماانجليترا أصدرت في عام 1990 قانون إساءة الكمبيوتر [2] الذي يتناول بالتجريم جريمة الدخول غير القانوني، بالإضافة إلى قانون حماية البيانات الصادر عام 1984وخصصت فريقين هما:

- **فريق منع الجريمة:** دوره هو تطوير وتقديم المشورة العامة لمنع الجريمة الالكترونية والتنسيق لمنع الجريمة وتوفير المشورة الالكترونية مع الحصول على استخدام امن الانترنت ونشر الأهداف المحددة وتقديم المشورة والوقاية من الأفعال التي تؤدي لتعطيل النشاط والسلوك

- **فريق الاتصالات والتنسيق**: وفريق الاتصالات والتنسيق هو التواصل الالكتروني وتنسيق البحوث ب\أن التهديدات ومواطن الضعف الناشئة عن الجريمة الالكترونية والتكنولوجيات وتوفير التدريب الالكتروني لدائرة الشرطة [3]

ب- الولايات المتحدة الأمريكية:

تعد الولاياتالأمريكية من الدول المتقدمة تكنولوجيا والمتطورة نفسيا في مجال مكافحة الجرائم المعلوماتية وجرائم الشبكات فقد وضعت عدة أقسامأو وحدات للشرطة لمواجهة هذا الإجرام والحد من خسائره ومنها

[1]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 747-748.

[2]- محمد كمال محمود الدسوقي.مرجع سابق، ص 209.

[3]- حسام محمد نبيل الشنراقي، مرجع سابق ، ص 749.

1- **قسم جرائم الحاسب وجرائم حقوق الملكية الفكرية والذي انشأ عام1991**والمختص بالكشف عن جرائم الحاسب الآلي وحقوق الملكية الفكرية وملاحقة مرتكبيها

2- **وحدة جرائم الانترنت** وهي وحدة تختص بالتحقيق في جرائم حقوق الملكية الفكرية وفي الجرائم المرتبطة بالتقنية العالية، ويرأسها مدير مساعد لمكتب التحقيقات الفيديرالي ولها نفس مرتبة وحدة التفتيش الجنائي

3- **مكتب رئيس التكنولوجيا**: وهو مكتب مفوض مباشرة من مكتب مدير التحقيقات الفيدرالية الأمريكي لتسيير مختلف المشروعات التكنولوجيات وملاحقة مرتكبي الجرائم الواقعة في المجال كملاحقة الشهيرة المسماة كارنيفور والأخرى المسماة المصباح العجيب

4- **المركز الوطني لحماية البنية التحتية**: التابع للمباحث الفيدرالية الأمريكية والذي يتقاسم مهامه مع الوزارة الدفاع وتجدر الإشارةإلىأن نشأة هذا الفريق تعود إلى تقرير جمعية العمل حول الانترنت والذي حددت من خلاله البنية التحتية التي تعتبر هدفا للهجوم والاعتداء عبر الانترنت .

5- تم تأسيس مركز تلقي شكاوى الاحتيال عبر الانترنت من طرف مكتب التحقيقات الفيدرالي بالاشتراك مع المكتب الوطني لجرائم ذوي الياقات البيضاء NW3C[1]

6- تم إنشاء وحدة متخصصة تابعة لقسم العدالة الأمريكي تختص بمكافحة الإجرام المعلوماتية تتكون من خبراء في تقنيات الحوسبة والانترنت ومن كمستشارين قانونين [2]

بإضافة إلى سنها تشريعات مستقلة بشأن جرائم الكمبيوتر وتتميز بامتلاكها ترسانة من التشريعات تغطي الجوانب تغطي الجوانب المختلفة للجرائم المعلوماتية ومن تلك التشريعات قانون الاحتيال وإساءة استخدام الحاسوب 1984 نقد جرمت المادة 1030 التوصل غير المفرح به الدخول إلى احد أنظمة الكمبيوتر الحكومية وكشف المعلومات السرية ومن ثم ارتكاب احتيال، إلحاق أضرار جراء الدخول غير المفرح به سواء للنظام أو البرامج أو المعلومات المخزنة فيه [3] ومن جهة أخرى نجد أن الولايات المتحدة الأمريكية توفر أيضا تدريبا لنظرياتها من الأجهزة في البلدان الأخرى داخل الولايات المتحدة الأمريكيةأو خارجها عن طريق إنشاء معاهد خاصة بتدريب باطلاع المتدربين على أساليب مبتكرة للتحقيق ويشجعون على تبادل الآراء مع نظرائهم في مختلف أنحاء العالم

[1]- عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الانترنت، الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، 2004، ص 812-814.

[2]- نبيلة هبة هروال، المرجع السابق، ص 110.

[3]- محمد كمال محمود الدوسقي، مرجع سابق ، ص210.

ج- **كندا:** وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت حيث عدلت من قانونها الجنائي ويشمل قوانين خاصة بجرائم الالكترونية كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية وجرائم التدمير أو الدخول غير المشروع لأنظمة الحاسب الآلي وقد نظمت النصوصالتشريعية تفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسات المالية ويستوي أن تكون السجلات مكتوبة أم في شكل الكتروني مادة 7/29 من قانون الإثبات الكندي

ويعمل مركز الشكاوى الخاص بجرائم الانترنت IG3 مع المنظمة الكندية المسماة الإبلاغ عن الجرائم الاقتصادية على خط الانترنت RECOI ويدير هذه المنظمة المركز القومي للجرائم المكتبة في كندا وتنطوي منظمة الإبلاغ عن جرائمالانترنت على شراكة متكاملة بين وكالات تطبيق القوانين الدولية والفدرالية والإقليمية من جهة وبين المسئولين عن وضع وتطبيق أنظمة العمل والمنظمات التجارية الخاصة التي لها مصلحة تحقيقية مشروعة في تلقى شكاوى الجرائم الاقتصادية، من جهة أخرى.[1]

ثالثا: جهات المكافحة على مستوى التشريعات العربية

بمطالعة الوضع العام في المنطقة العربية نلاحظ أن هناك حراك تشريعي في عدد من الدول العربية نحو استكمال بنيتها التشريعية وسد ما بها من نقص لمكافحة الجرائم المعلوماتية وحماية البيانات الالكترونية بصفة عامة والتوقيع الالكتروني بنية خاصة، ومن ابرز تلكالجهودنجد.

أ- الأجهزة المختصة بمواجهة الجرائم التوقيع الالكتروني في مصر

لمكافحة الجرائم التوقيع الالكتروني اتخذت وزارة الداخلية المصرية عدة تدابير وخطط جديدة وشكلت دوريات أمنية من خلال فرض رقابة صارمة على استخدام الانترنت وهناك تنسيق دائم بين كل الإدارات بالوزارة العدل الاتصالات والهيئات التشريعية والأجهزة الفنية بالدولة ومن تلك الجهات والإدارات المتخصصة في مواجهة جرائم التوقيع الالكتروني [2] ما يلي:

- الإدارة العامة للمعلومات والتوثيق: تعتبر الإدارة العامة للمعلومات والتوثيق هي المختص بشكل رئيسي بالتعامل مع جرائم المعلومات بوجع عام، ومنها الجرائم التي تقع على التوقيع الالكتروني ويبدأ اعملها من خلال المتابعة الفنية والتحري عن الجرائم التي يتم التبليغ بها للإدارة من الإدارات الأخرى باستخدام شبكة الانترنت وتحديد بشخص المتهم هذا من جهة ومن جهة أخرى فهي تقوم بتحديد المتهم من خلال عمليات التتبع ويعتمد أسلوب عمل هذه الإدارة في معرفة شخص مرتكب

[1]- فهد عبد الله العبيد العازمي، مرجع سابق ، ص 226.

[2]- سليمان أحمد فاظل، مرجع سابق ، ص393

الجريمة على استخدام البرامج الحديثةوذلكعن طريق الاعتماد على بروتوكول IP الذي يتعامل من خلاله الشخص مع شبكة الانترنت [1]

فقد تم إنشاء الإدارة العامة لمكافحة جرائم الحاسب الآلي وشبكة المعلومات بمقتضى القرار 13507 لسنة 2002 وهي تخضع فنيا لإشراف مصلحة الأمن وتنقسم إلى عدة أقسام[2]

- **قسم العمليات**: وهو قسم يختص بمكافحة الجرائم التي يكون الحاسب الآلي أداة لارتكابها في مجالات نظم المعلومات بالاشتراك مع الأجهزة المتخصصة سواء داخل الوزارة أو خارجها كما يقوم بالتنسيق مع الأجهزة النوعية المختصة بأعمال المكافحة لإجراء وإعمالالضبط في تلك الجرائم وفقا التعليمات المنظمة لذلك، كما تقوم بإعداد قاعدة بيانات تضم جرائم المعلومات والأحكام الصادرة فيها ومرتكبيها التي تدخل في نطاق اختصاص الإدارة فضلا عن إنشاء الملفات والسجلات والبطاقات اللازمة لذلك.

- **قسم التامين:** يختص قسم التامين بتامين المعلومات والشبكات الخاصة بأجهزة الوزارة يوضع الخطط والأساليب التي تستخدم لذلك، وذلك بالتنسيق مع الأجهزة بذلك من داخل الوزارة او خارجها وفقا للقوانين واللوائح والتعليمات المنظمة لذلك، كما يقوم بمتابعة التراخيص التي تصدر للشركات الخاصة في مجال نظم وأجهزة وشبكات المعلومات.

- **قسم البحوث والمساعدات الفنية**: يقوم هذا القسم بإعداد البحوث الفنية والقانونية في مجال تامين نظم شبكات المعلومات والحاسبات الآلية ودراسة الظواهر الإجرامية المتعلقة بجرائم الحاسبات والانترنت واستنباط النتائج للاستفادة منها في أساليب المكافحة وهذا بالتنسيق مع الأجهزة المختصة، كما يقوم يبحث في مدى ملائمة التشريعات الجنائية لمواجهة مثل هذه الجرائم، فضلا عن تقديم الدعم الفني وتوفير المساعدات الفنية وإبداءالرأي والمنشورة في كافة القضايا وبالوقائع المرتبطة بهذا النوع المستحدث من الجرائم للجهات المختصة.

- **الإدارة العامة لمباحث الأموال العامة:**

وتختص الإدارة العامة لمباحث الأموال العامة بمكافحة الجرائم الاقتصادية التقليدية بصفة عامة والمستحدث بصفة خاصة باعتبارها إحدى الروافد الرئيسية لقطاع الأمن الاقتصادي، وتعتبر جرائم لتزوير العملات الورقية التزوير باستخدام الماسحات الضوئية والطابعات من أكثر الجرائم التي تصطلح

[1]- ايمن رمضان محمد أحمد، مرجع سابق ، ص 430.

[2]- ايمن عبد الحفيظ، مرجع سابق، ص 457.

الإدارة العامة لمباحث الأموال العامة بمكافحتها والتي يكون الحاسب الآلي أداة الأساسية لارتكابها [1] كما وتقوم الإدارة بإتباع خطوات لمكافحة جرائم تزوير التوقيع الالكتروني وكذا سرقة وتزوير بطاقات الائتمان.

ب -جمهورية السودان: شهدت السودان عام 2007 حركة تطوير للبنية التشريعية للتصدي للجرائم المتولدة عن إساءة استعمال تقنية المعلومات ومن ابرز تلك التشريعات نجد قانون الجرائم المعلوماتية عام 2007 وقانون المعاملات الالكترونية لسنة 2007 الذي يضفي حماية لبيانات الإلكترونية وكذا التوقيع الالكتروني ويعاقب على من يقوم بكشف مفاتيح التشفير وكشف عن معلومات مشفرة ومخزنة في غير الأحوال المصرح بها وكذا الاطلاع على المعلومات وبيانات الالكترونية دون ترخيص أوإفشائها وذلك حسب نص مادة 27 من قانون المعاملات الكترونية سنة 2007.[2]

ج- الأجهزة المختصة بدول الخليج لمكافحة جرائم التوقيع الالكتروني:

طبقت دول الخليج قوانين حقوق الكلية الملكية الفكرية على الجرائم المعلوماتية بحيث تمتد حمايته هذه القوانين لتشمل برامج الحاسب الآلي وتطبيقاته، قبل أن تتوجه بعض الدول الخليج إلىإصدار نظم وقوانين خاصة بالجرائم المعلوماتية

- **سلطة عمان:** تعد عمان أولى دول الخليج في لبني قواعد نونية تجرم الأفعال الإجرامية الناجمة عن إساءة استعمال تقنية المعلومات من خلال التعديل الذي ادخل على قانون الجزاء العماني رقم 7 الصادر عام 1984 بموجب المرسوم السلطاني رقم 2001/72 وقد تضمنت هذه التعديلات إضافة الفصل الثاني مكرر إلى الباب السابع تحت عنوان جرائم الحاسب الآلي ويعد هذا القانون أول القوانين العربية في مجال مواجهة الجرائم المعلوماتية من خلال تعديل قانون العقوبات [3]

كما يوجد بعمان قسم خاص يعني بجرائم الحاسب الآلي والانترنت ويوجد به أشخاص مؤهلين ومختصين بتلك النوعية من الجرائم، ويتبع هذا القسم الإدارة العامة للتحريات والتحقيقات الجنائية بشرطة عمان السلطانية، كما توجد جهات خاصة معنية بالجرائم المعلوماتية الرقمية وتمارس عليها بالتنسيق والتعاون مه الأجهزة الأمنية المختلفة بدولة [4]وكذا إصدار المرسوم السلطاني رقم 2008/69

[1]- فهد عبد الله العبيد العازمي، مرجع سابق ، ص241.

[2]- عادل رمضان الابيوكي: التوقيع إلكتروني في التشريعات الخليجية، المكتب الجامعي الحديث، القاهرة، 2009. ص 46.

[3]- محمد كمال محمود الدسوقي، مرجع سابق ، ص 242.

[4]- هلال بن محمد بن حارب البوسعيدي، الحماية القانونية الفنية لقواعد المعلومات المحسوبة، دراسة قانونية وفنية مقارنة، دار النهضة العربية، القاهرة، مصر، 2009، ص 279

بإصدار قانون المعاملات الالكترونية يتضمن هذا القانون مجموعة الضمانات للبيانات الشخصية الخاصة بموجب الفصل السابع المعنوي بحماية البيانات الخاصة بمواد 43.49 من ابرز تلك الضمانات

- عدم جواز جمع بيانات مباشرة من الشخص الذي تجمع البيانات من غيره دون موافقة صيحة من الشخص صاحب البيانات وسواء كانت الجهة حكومية أو مقدم خدمات تصديق، وهو وفقا للتعريف الوارد بهذا القانون أي شخص أو جهة معتمدة أو مرخص لها بقيام بإصدار شهادات تصديق الكترونية أوأية خدمات أخرى متعلقة بها وبالتوقيعات الالكترونية

- وكذا إلزام مقدمو خدمات التصديق بإتباع الإجراءات المناسبة لضمان سرية البيانات الشخصية وعدم إفشاءأو تحويل أوإعلانأو نشر تلك البيانات كما تضمن الفصل التاسع من هذا القانون المواد 52-53 نصوص عقابية واليت تناولت إتلاف النظم المعلوماتية واختراقها والعبث بالتوقيعات الالكترونية والاستخدام غير المشروع لها والتزوير المعلوماتي وفك التشفي وغير منا الجرائم[1]

- **دولة الإمارات العربية المتحدة:** أصدرت دولة الإمارات قانون الاتحادي رقم 40 لسنة 1992 في شأن المصنفات الفكرية وحقوق المؤلف، وقد تشمل هذا القانون برامج الحاسب الآلي بالحماية علاوة أن المشرع الإماراتي في هذا القانون وقد اعتبر مخالفة نصوص الحماية الفكرية لبرامج الحاسب الآلي جرائم يعاقب عليها بالقانون بعقوبة جنائية، كما أصدرت عام 2002 قانون التوقيع الالكتروني والتجارة وقد مضى هذا القانون بمنع مزود خدمات الانترنت من كشف أية معلومات يحصلون عليها أثناء تزويد الخدمة، كما صدر القانون الاتحادي رقم 2 لسنة 2006 لمكافحة جرائم تقنية المعلومات، وقد حدد المشرع الإماراتي الأفعال التي يعد ارتكابها جريمة من جرائم المعلومات، كما حدد العقوبات الملائمة لها تبعا لخطورتها وضررها المتوقع، وقد تشمل القانون اغلب الجرائم المعلوماتية ومنها التعدي على البيانات أو المعلومات أو حذفها أو تدميرها أوإفشاؤهاأوإتلافها، أو تغييرها أو إعادة نشرها [2]

- **دولة المملكة العربية السعودية:** تعد المملكة العربية السعودية الدولة العربية الثالثة التي أصدرت نظاما لمكافحة الجرائم المعلوماتية فقد صدر نظام مكافحة الجرائم المعلوماتية بالمرسوم الملكي رقم 17 الذي يهدف إلى مواجهة جرائم الحاسب الآلي والانترنت، من خلال وضع آلية نظامية للحد من وقوع هذا النوع من الجرائم، وذلك بتحديد الجرائم المستهدفة بالنظام والعقوبات المقدرة لكل جريمة، وقد حدد النظام السعودي اغلب الجرائم المعلوماتية والأفعال التي تشكل خطرا على المعلومات كما قامت وزارة

[1]- محمد كمال محمود الدسوقي، مرجع سابق ، ص 214.

[2]- جميل عبد الباقي الصغير، مرجع سابق ، ص87.

التعليم العالي بسعودية بإنشاء مركز التميز لأمن المعلومات [1]وإنشاء وحدة خاصة لمتابعة والتحقيق في المخالفات المتعلقة بأمن المعلومات تكوين لجان الدائمة برئاسة وزارة الداخلية وعضوية وزارات الدفاع، المالية، الثقافة وإعلام، اتصالات وتقنية المعلومات، تجارة شؤون إسلامية، تربية وتعليم، رئاسة استخبارات وذلك لمناقشة ما يتعلق بمجال ضبط واستخدام انترنت [2]

-اليات المكافحة في التشريع الجزائري :

ان الجزائر و كغيرها من دول العالم سارعت هي الاخرى الى توفبر كوادر و أجهزة متخصصة تعنى بعملية البحث و التحري عن جرائم التوقيع الإلكتروني سواء على مستوى جهاز الشرطة أو الدرك الوطني،فعلى مستوى الشرطة فقد أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بالجزائر العاصمة و مخبرين جهويين بكل من ولاية و هران و قسنطينة تحتوي هذه المخابر على فروع تقنية من بينها خلية الإعلام الألي بالإضافة إلى أنه يوجد على مستوى مراكز الأمن الولائي فرق متخصصة مهمتها التحقيق في الجريمة المعلوماتية تعمل بالتنسيق مع هذه المخابر ،أما على مستوى الدرك الوطني فإنه يوجد المعهد الوطني للأدلة الجنائية و علم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام الإلكتروني ، و الذي يختص بالتحقيق في الجرائم المعلوماتية ومكافحتها ببئر مراد رايس و التابع لمديرية الأمن العمومي للدرك الوطني [3]، ومن بين الأجهزة المتخصصة في البحث و التحري عن جرائم الانترنت نجد ،مركز الوقاية من جرائم الإعلام الألي و الجرائم المعلوماتية للدرك الوطني CPLCIC/GN اضافة الى المعهد الوطني للادلة الجنائية و علم الإجرام للدرك الوطني INCC/GN،و المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الامن الوطني ،و الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها التي تم تحديد تشكيلتها و تنظيمها و سيرها بواسطة المرسوم الرئاسي 261/15 المؤرخ في 2015/10/08

[1]- مركز التميز لأمن المعلومات: تتركز أهداف المركز في بيئة من المعلومات التي ضم المراكز البحثية والكليات لنقل الخبرى وتوجه الأبحاث في هذا المجال، ونشر الوعي بأمن المعلومات وتطوير الأمن الوطني

[2]- فهد عبد الله العبيد العازمي، مرجع سابق ، ص249.

[3]حايت امال ،ورقة مقدمة في محاضرة حول الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في قانون الجزائري ،جامعة مولود معمري ،تيزي وزو ،ص21.

المطلب الثاني: التدابير الدولية الإجرائية المتعمدة في مجال تسليم المجرمين

إن الاعتداء على التوقيع الالكتروني من خلال وسائل فنية تتيح للمتهم ارتكاب الجريمة حال وجوده في دولة أجنبية أدى إلى ابتعاد المجرمين عن سلطات الدولة المتضررة من الجريمة وإفلاتهم من العقاب في كثير الأحيان، وهو ما يعكس ضرورة التعاون الدولي لمكافحة الجرائم التي يكون بالتوقيع الالكتروني محلاها، وضمان توقيع العقاب على مرتكبي هذه الجرائم [1]وهذا التعاون يتخذ صورة متعددة منها تسليم المجرمين الذي عمدته مختلف التشريعات مقارنة

ومن خلال هذه الدراسة سنقوم بتقسيم هذا المطلب إلى الفروع الآتية

الفرع الأول: مفهوم نظام التسليم المجرمين في مجال مكافحة جرائم الاعتداء على التوقيع الالكتروني

يعد مصطلح تسليم المجرمين الترجمة العربية لكلمة "Extradition" وهي كلمة فرنسية استعملت لأول مرة في مرسوم 19 فيفري 1891 في فرنسا ولكلمة " Extradition" الإنجليزية التي اشتقت من الفرنسية واستعملت لأول مرة في بريطانيا في القانون التسليم سنة 1970[2] والتسليم بصفة عامة هو " إجراء تتخلى الدولة بموجب على فرد موجود لديها سلطات دولة أخرى تطالب بتسليمه إليها – بغرض محاكمته عن جريمة ارتكبها أو لتنفيذ حكم صادر هذه بعقوبة جنائية [3] كما يعرف بأنه مجموعة من الإجراءات القانونية التي تهدف إلى قيام دولة بتسليم شخص متهم أو محكوم عليه إلى دولة أخرى لكي يحاكم بها، أو ينفذ فيه الحكم الصادر عليه من محاكمها [4]وذلك استنادا إلى اتفاقية أو وفقا لمبدأ المعاملة بالمثل أو المجملة الدولة

كما عرفته المحكمة العليا الأمريكية " بأنه الأجراء القانوني المؤسس على معاهدة أو معاملة بالمثل أو قانون وطني، حيث تتسلم دولة ما من دولة أخرى شخص متهم أو مرتكب مخالفة جنائية ضد القوانين الخاصة بالدولة الطالبة، أو مخالفة للقانون الجنائي الدولي، حيث يعاقب على ذلك في الدولة الطالبة [5]

[1]- ايمن رمضان محمد أحمد، مرجع سابق ، ص404.

[2]- بالفرد لطفي لمين، التعاون الدولي في مجال تسليم المجرمين، مجلة الشرطة الجزائرية العدد 92 أكتوبر 2009 ص13.

[3]- جميل الباقي الصغير الحماية الإجرائية المتعلقة بأنترنت، دار النهضة العربية، القاهرة، 2018 ، ص109.

[4]- فهد عبد الله العبيد العازمي، مرجع سابق ، ص 519.

[5]- رقية عواشرية، نظام تسليم المجرمين ودوره في تحقيق التعاون الدولي لمكافحة الجريمة المنظمة، محلية المفكر، جامعة محمد خيثر، الجزائر، بسكرة العدد الرابع 2008 ، ص19.

ويعرفه البعض بأنه"قيام إحدى الدول ويطلق عليها الدولة المطلوب منها التسليم بتسليم شخصا موجودا على اقلميها إلىأدلة أخرى يطلق عليها الدولة طالبة التسليم أو الطالبة بناءا على طلبها بفرض محاكمته عن جريمة تسبب إليه ارتكابها أو تنفيذ حكم صادر ضده من محاكمتها"[1]

و ذلك استنادا إلى اتفاقية أو وفقا لمبدأ المعاملة بالمثل أو المجاملة الدولة.

كما عرفته المحكمة العليا الأمريكية:"بأنه الإجراء القانوني المؤسس على معاهدة أو معاملة بالمثل أو قانون وطني،حيث تتسلم دولة ما من دولة أخرى شخص متهم أو مرتكب مخالفة جنائية ضد القوانين الخاصة بالدولة الطالبة، أو مخالفة للقانون الجنائي الدولي، حيث يعاقب على ذلك في الدولة الطالبة.[2]

و يعرفه البعض بأنه قيام إحدى الدول ويطلق عليها الدولة المطلوب منها التسليم بتسليم شخصا موجودا على إقليمهاإلى دولة أخرى يطلق عليها الدولة مطالبة التسليم أو الطالبة بناءا على طلبها بفرض محاكمته عن جريمة نسب إليه ارتكابها أو لتنفيذ حكم صادر ضده من محاكمتها.[3] والواضح مما سبق أن فكرة نظام التسليم تقوم من جهة على وجود علاقة بين دولتين:الأولى تطالب بأن يسلم إليها مرتكب الجريمة لتتخذ بحقه الإجراءات اللازمة لإيقاع العقوبة اللازمة عليه والثانية يوجه إليها طلب التسليم لتقرر بعد ذلك إما الاستجابة له إذا كان متوافقا مع تشريع نافذ المفعول فيها أو معاهدة أو اتفاق يربط بينها وبين الدولة الطالبة، وأما الرفض لعدم ذلك التشريع أو تلك الاتفاقية، ومن جهة أخرى نجده يشمل طائفتين من الأشخاص، طائفة الأشخاص المتهمين الذين تستند إليهم ارتكاب جرائم إلا أنه لم يهدر بحقهم أحكام يعد وطائفة أشخاص محكوم عليهم الذين صدر بحقهم حكم بإدانة إلا أنه لم ينفذ بعد نتيجة لفرارهم إلى دولة أخرى [4]

و مؤدى التسليم المجرمين في جرائم الاعتداء على التوقيع الالكتروني بأن الدولة التي يتواجد على إقليمها المتهم بارتكاب إحدى الجرائم عابرة للحدود مثل جرائم الاعتداء على التوقيع الالكتروني، عليها أن تقوم بمحاكمته، إذا كان تشريعها يسمح بذلك، وإلا كان عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى متخصصة [5].

[1]- محمد كمال محمود الدوسقي، مرجع سابق، ص 168.

[2]- رقيةعواشرية، مرجع سابق، ص19.

[3]- محمد كمال محمود الدوسيقي، مرجع سابق، ص 168.

[4]- ياسر محمد الكومي أبو حطب، مرجع سابق، ص 355.

[5]- محمد زكي أبو عامر، مرجع سابق، 41.

ووفقا للمبادئ العامة المتعلقة بالتعاون الدولي وتسليم المتهمين الواردة في القسم 501 من الفصل 3 من اتفاقية مجلس أوروبا دول الجريمة الالكترونية يتعين على الدول الأطراف التعاون بشكل موسع وتذليل العقبات التي تعترض التدفق السريع للمعلومات والأدلة [1].

و يشمل التعاون كافة الجرائم المتعلقة بأجهزة الحاسوب ومنها جرائم الاعتداء على التوقيع الالكتروني بإضافة إلى جميع الأدلة حول هذه الجرائم بالشكل الالكتروني بما يعني أن الشروط المنصوص عليها في الفصل 3 تطبيق سواء تعلق الأمر بجريمة ارتكبت باستعمال جهاز الحاسوب، أم جريمة عادية ترتكب من خلاله جهاز الحاسب الآلي ولكنها خافت أدلة الكترونية [2].

ثانيا:مصادر نظام تسليم المجرمين في جرائم التوقيع الكتروني.

تتعدد مصادر تسليم المجرمين والتي أساسها تطلب إحدى الدول من دولة أخرى تسليم شخص مقيم على إقليمهاإليها لمحاكمته أو تنفيذ حكم قضائي صادر بحقه، وتنقسم هذه المصادر إلى نوعين مصادر أصلية والتي تستند إليها دول الأطراف في عملية التسليم لإتمام إجراءات التسليم ومصادر احتياطية والتي عادة ما تلجأ إليها الدول عندما يصعب الاعتماد على المصادر الأصلية أو في حالة غيابها وعليه سنتولى بيان تلك المصادر على النحو التالي

أ-المصادرالأصلية:

1- المعاهدات والاتفاقيات: تعرفا لمعاهدة الدولية بأنها "اتفاق مكتوب بين شخصين أو أكثر من أشخاص القانون الدولي العام، لأحداث آثار قانونية معينة، وفقا لأحكام القانون الدولي العام [3].

حيث تعد المعاهدات والاتفاقيات بين الدول من أهم مصادر نظام تسليم المجرمين ففي ظل غياب معاهدة دولية مغرمة بشأن تسليم المجرمين فإنه لا يمكن القول بوجود التزام دولي بتسليم المجرمين ولقد شهد العالم بعد الحرب العالمية الثانية زيادة في عدد المعاهدات الدولية، والثنائية ومتعددة الأطراف لتنظم إجراءات تسليم المجرمين.

و عليه تقسم المعاهدات والاتفاقية الدولية إلى:

اتفاقيات التسليم الثنائية: وهي التي تتم بين دولتين وفقا لشروط والضوابط الموضوعة من قبلهما[1].

[1] - ايهاب محمد يوسف، اتفاقيات تسليم المجرمين، سالة دكتورة، كلية الدراسات المحكمة العليا بأكادمية الشرطة، 2003، ص230.

[2] - ايمن رمضان محمد أحمد، مرجع سابق، ص 406.

[3] - محمد كمال محمود الدوسيقي، مرجع سابق ، ص173.

اتفاقية التسليم المتعدد الأطراف: وهي اتفاقيات يكون أطرافها عدة دول [2]

2- الاتفاقيات الدولية: وهي اتفاقيات دولية تتضمن إحكاما متصلة بتسليم المجرمين دون أن تكون بحد ذاتها اتفاقيات تسليم [3].

و نظرا لأهمية وفعالية نظام تسليم المجرمين في مكافحة الجرائم الالكترونية، فإنه ولضمان الاستفادة منه فقد نص المادة 24 فقرة 3 من اتفاقية بودابيست المتعلقة بالجريمة الالكترونية 2001 "على أن أي دولة طرف لا توافق على تسليم المجرمين سواء لأنه لا يوجد اتفاق مبرم مع الطرف طالب التسليم، أو لأن الاتفاق المبرم بينهما لا يشمل التسليم بالنسبة للجرائم المعلوماتية الواردة بالاتفاقية والتي من بينها الجرائم الماسة بسرية المعلومات الالكترونية وهي الدخول غير القانوني لنظام توقيع الالكتروني والاعتراض غير القانوني للبيانات، فإنه في هذه الحالة يمكن اعتبار اتفاقية بودابست كأساس قانوني لتسليم الشخص المطلوب تسليمه على الرغم من أن هذا الطرف غير ملزم بذلك [4].

و لقد نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 على ذات الحكم في الفقرة 3 من المادة 31 منها [5].

3- القانون الداخلي:

بإضافة إلى عقد العديد من الاتفاقيات الإقليمية والدولية والثنائية التي تعني بعملية التسليم فقد حرصت معظم الدول على تنظيم أحكام تسليم المجرمين إما من خلال تشريعاتها الجزائية مثل الولايات المتحدة الأمريكية حيث ينظم قانونها الفدرالي الأحكام العامة لإجراءات التسليم إلى جانب تشريع كل ولاية وقانون الإجراءات الجنائية الايطالي لسنة 1988 وقانون الإجراءات الجنائية البولندي لسنة 1969 ومن التشريعات العربية، قانون الإجراءات الجنائية العراقي والتونسي والجزائري والبحريني، وقد تقوم بعض الدول سبق تشريعات خاصة بتسليم المجرمين، مثل قانون تسليم المجرمين الإنجليزي لسنة 1989و

[1]- ومن هذه الاتفاقيات الخاصة بتسليم المجرمين نجد: اتفاقية بين مصر واليونان 1986، اتفاقية بين الجزائر وبلجيكا 1970، اتفاقية التعاون القضائي وتسليم المجرمين مع بولندا في 1993 اتفاقية بين المغرب واسبانيا 1999.

[2]- ومن أمثلة هذه الاتفاقيات: اتفاقية جامعة الدول العربية لتسليم المجرمين عام 1953 واتفاقية الدولية الأوروبية لتسليم المجرمين 1957.

[3]- ومن أمثلة هذا النوع من الاتفاقيات، الاتفاقية العربية لمكافحة الجريمة 1997.

[4]- هلالي عبد الله أحمد، مرجع سابق ، ص249.

[5]- تنص الفقرة 3 من المادة 31 من الاتفاقية العربية لمكافحة تقنية المعلومات 2010 على انه " إذا قامت دولة طرف ما يجعل تسليم المجرمين مشروطا بوجود معاهدة وقامت باستلام طلب تسليم المجرمين من دولة طرف أخرى ليس لديها معاهدة تسليم فيمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين "

قانون الفرنسي لعام 1927 ومن التشريعات العربية القانون العماني 2000 وقانون تسليم المجرمين الأردني 1927.[1]

4- العرف الدولي:

يعتبر العرف الدولي في مجال تنظم تسليم المجرمين مصدرا أساسيا إشتقت منها المعاهدات والتشريعات الوطنية أحكامها، ومن أبرز القواعد العرفية حالة عدم جواز تسليم رؤساء وملوك الدول الأجنبية لتمسكهم بحصانه ومبدأ الخصوصية واستثناء تسليم الرعايا، خطر تسليم اللاجئ، عدم جواز التسليم في الجرائم السياسية، ومن القوانين العربية التي اعتبر العرف الدولي من بين المصادر الأساسية لنظام تسليم المجرمين قانون الإجراءات البحريني لسنة 2002 .[2]

ب-المصادر الاحتياطية:

1- قواعد المجالات والأخلاق: يمكن الاستناد إلى قواعد المجاملات الدولية في مجال تسليم المجرمين في حال غياب اتفاقيات تسليم بين الدولة الطالبة والدول المطلوب منها التسليم، حيث تقوم دولة ما في سبيل توطيد علاقاتها بدولة أخرى أو تعزيزها، تنفيذ طلب التسليم المقدم إليها من دولة أخرى دون ربطها باتفاقية تبادل تسليم المجرمين ومن التطبيقات العملية على عمليات التسليم التي تمت على أساس قواعد المجاملة الدولية ما قامت به الولايات المتحدة الأمريكية عام 1962 بطلب تسليم أحد المتهمين في قضية مخدرات من جمهورية لبنان على الرغم من عدم ارتباطهما بمعاهدة تسليم حينها، وقد تأسس الطلب الأمريكي على قواعد المجاملة الدولية .[3]

- أما قواعد الأخلاق الدولية تعتبر مجموعة من المبادئ السامية التي تقيد بها تصرفات الدول وفقا لمعايير الأخلاق الفاضلة والشهامة والمروءة، ولكنها ليست ملزمة من الناحية القانونية ومن أمثلة ذلك الابتعاد عن الكذب والخداع في العلاقات الدولية وتقديم المعونة إلى الدول المنكوبة،و هذه القواعد هي الأخرى ذات إلزام أدبي .[4]

2- المعاملة بالمثل: تعد المعاملة بالمثل أحد أهم الأدوات في مجال العلاقات الدولية ومن التطبيقات العملية لهذا المبدأ في مجال تسليم المجرمين ما قامت به مصر العربية بإبرام مذكرة تفاهم لتسليم المجرمين على أساس المعاملة بالمثل مع الولايات المتحدة الأمريكية، تتعهد فيها الخبرة بإتباع سلوك مماثل

---

[1]- محمد كمال محمود الدسوقي، مرجع سابق، ص 177.

[2]- تنص المادة 412 من قانون إجراءات جنائية "البحريني على اللجوء الى قواعد القانون الدولي العام فيما لم يرد في شأنه نص خاص في المعاهدات ولاتفاقيات الدولية التي لها قوة القانون في مملكة البحرين أو قانون الإجراءات الجنائية.

[3]- محمد كمال محمود الدسوقي، مرجع سابق ، ص180.

[4]-محمد كمال محمود الدسوقي، مرجع سابق، ص 182.

مع مصر بعد موافقتها على تسليم أحد المجرمين والذي يحمل الجنسية الإسرائيلية إلى الولايات المتحدة الأمريكية كونه متهم في جريمة جلب مخدرات من الهند إلى الولايات المتحدة الأمريكية بإضافة إتهامه بقتل أحد ضباط جهاز لمكافحة المخدرات الأمريكي [1].

ثالثا: نظم تسليم المجرمين.

تتنوع أنظمة تسليم المجرمين وتختلف كل دولة في الطريقة التي تبحث بها طلب التسليم بحسب نوع النظام التي تأخذ به وهناك ثلاثة أنظمة متبعة في تسليم المجرمين هي:

أ-التسليم القضائي: يقوم هذا النظام على أساس احترام حقوق الأفراد وصيانة حرياتهم لذا تعتبر السلطة القضائية هي الجهة الوحيدة المختصة بإصدار قرار التسليم، ولا شأن بجهة الإدارة بهذا الخصوص والدولة التي تأخذ بهذا الاتجاه تنتهج أحد المنهجين: الأول أن تكون المحكمة هي الوحيدة المختصة بإصدار قرار التسليم للدولة طالبة التسليم ولا دخل لنيابة العامة في إصدار هذا القرار وإنما يقتصر دورها وعملها على تلقي طلب التسليم من الجهة المختصة، لتتولى الأخيرة عملية إصدار القرار النهائي حول هذا الطلب[2]، أما النهج الثاني يتمثل في إعطاء النائب العام في الدولة المطلوب منها التسليم سلطة الفصل في إصدار القرار النهائي من عدمه، فبالرغم من حملة الإيجابيات التي قد يوفرها هذا النظام القضائي من حيث أنه يبيح للشخص المطلوب تسليمه أن يتقدم بأوجه دفاعه كاملا مما يمكنه من الدفاع عن نفسه عما يمكن أن يكون وراء الأوراق والمستندات، بإضافة إلى أنه لا يوجد به ما يسمى بالمجاملات السلوكية الدولية إلا أنه لا يخلو من بعض السلبيات، منها أنه يتطلب القدرة على إحداث نوع من التوازن بين الخبرة القانونية الدولية والأبعاد السياسية الدولية والتي قد لا تتوافر لجميع القضاة والسلطة القضائية أضف إلى ذلك طول الفترة التي تستغرقها إجراءات المحاكمة من شأنها أن تدفع بالمحكمة إلىإصدار أمر بالإفراج المؤقت عن المطلوب تسليمه بحيث استكمال باقي الإجراءات [3]

ب-التسليم الإداري: تسليم المجرمين يعدو وفقا لهذا النظام عملا من أعمال السيادة أو التدابير من تدابير السلطة التنفيذية التي تملك الصلاحية المطلقة لتقرير التسليم من عدمه وفقا لاعتبارات سياسية أو إدارية أو غير ذلك من الاعتبارات ويتطلب هذا النوع من التسليم أن توجه أجهزة الانتربول

[1]- عبد الفتاح محمد سراج. النظرية العامة لتسليم المجرمين، دار النهضة العربية، القاهرة، 2013، ص47.

[2]- فهد عبد الله العبيد العازمي، مرجع سابق، ص527.

[3] - هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، دبي كلية الشرطة، العدد 2 1999، ص445.

بالدولة طالبة التسليم طلبها بشأن القبض على المتهم المطلوب إلى انتربول الدولة المطلوب منها التسليم والتي تحيل الطلب إلى السلطة الإدارية المختصة لدراسة والبحث ومن ثم إصدار القرار [1].

فهذا النظام له العديد من الإيجابيات كما له العديد من السلبيات فمن إيجابياته السرعة فالبث في طلب التسليم وكذا الابتعاد عن إجراءات الطويلة والمعقدة والتي قد تحتاج إلى نفقات عالية فيما إذا لجأت الدولة إلى النظام القضائي، بإضافة إلى أنه يساعد على تحسن العلاقات الدولية بين الدول وعلى الرغم من هذه الإيجابيات التي يمتاز بها هذا النظام إلا أنه ثمة سلبيات تؤخذ عليه، الجاهدان لحق الفرد في الدفاع عن نفسه باعتباره ضمانة للمتهم، بإضافة إلى المجاملات الدولية التي قد تحدث لصالح الدولة طالبة التسليم ويقع ضحيتها المتهم المطلوب تسليمه، إضافة إن على النوع من التسليم يتم في أيطار من والكتمان مما يعني بهذه عن الأجهزة الرقابة القضائية والشريعة [2]

ج –**التسليم المختلط:** النوع الثالث من التسليم يجمع بين الجانبين القضائي والإجرائي وهو الأكثر رواجا وانتشارا حيث يوازي بين المصلحتين المتعارضتين، مصلحة الدولة طالبة التسليم ومصلحة الشخص المطلوب تسليمه، فيكون للسلطة القضائية حق فحص الطلب ويمنح الشخص المطلوب تسليمه كل الضمانات القانونية للدفاع، بشرط أن لا تقحم الدولة المطلوب منها المتهم نفسها في فحص وقائع الدعوى وتكتفي بما يرد إليها من مستندات ووثائق من الدولة الطالبة[3] وهذا النهج هو نهج العديد من القوانين الوطنية ومنها على سبيل المثال القانون الإيطالي والقانون السويسري.

الفرع الثاني: شروط وإجراءات تسليم المجرمين لمكافحة جرائم التوقيع الالكتروني.

سنتناول من خلال هذا الفرع شروط تسليم المجرمين بعضها يتعلق بالشخص المطلوب تسليمه والبعض الآخر يتعلق بالجريمة محل التسليم إضافة إلى الإجراءات والخطوات المتبعة لقيام بهذا التسليم

أولا: شروط التسليم في جرائم الاعتداء على التوقيع الالكتروني

لقد وضعت الاتفاقيات الدولية عدة شروط لتسليم المجرمين وهي كآتي:

أ- عدم جواز تسليم الرعايا: من المبادئ السائدة والمستقر عليها في المجتمع الدولي والتي نصت عليها معظم التشريعات الوطنية والاتفاقيات الدولية مبدأ عدم جواز تسليم الرعايا أيا كان نوع الجريمة المرتكبة من قبلهم في أي إقليم خارج دولتهم.

[1]- ياسر محمد الكومي محمود أبو حطب، مرجع سابق ، ص357.

[2]- فهد عبد الله العبيد العازمي، مرجع سابق ، 531.

[3]- هشام فريد محمد رستم، مرجع سابق ، 439.

و غالبية المعاهدات المتعلقة بتسليم المجرمين والقوانين الداخلية تأخذ بهذا النظام فرنسا ومصر، بينما تأخذ الدول الانجلوساكسونية كالولايات المتحدة الأمريكية وبريطانيا بمبدأ تسليم الرعايا وطبقا لنص الدستور المصري المادة 51 لسنة 1971 "لا يجوز إبعاد مواطن عن البلاد أو منعه من العودة إليها" [1] وكذا هذه القاعدة نجدها في القانون السويسري 1829 وفي مشروع جمعية القانون الدولي 1938 والقانون الفرنسي 1937 والقانون الألماني 1929 وفي المعاهدات مثل معاهدة تسليم المجرمين بين العراق والمملكة العربية السعودية 1931 وكذا معاهدة بين سويسرا وأمريكا 1900 تقتضي بأن أية حكومة من الحكومتين غير ملزمة بتسليم رعاياها.

في حين نجد بعض التشريعات تفرضقيود على استعمال الدولة حقها في رفقة تسليم رعاياهم ففي القانون الفرنسي نص يبيح تسليم الشخص المطلوب الذي اكتسب الجنسية الفرنسية بعد ارتكاب الجريمة.م5 وفضلا عن ذلك فإن القانون الفرنسي لا يمنع من مرور شخص فرنسي يقتني بتسليمه عبر الأراضي الفرنسية م28[2].

ب-عدم جواز التسليم في الجرائم السياسية: فلا يجوز التسليم في الجرائم السياسية [3] حيث يكون الغرض منه اتخاذ إجراءات انتقامية ضد الشخص المطلوب تسليمه وهو عمل لا يليق بالدولة المطلوب منها التسليم أن تساهم في تنفيذه.

و لقد أكد البند العاشر من المادة 16 من اتفاقية باليرمو بشأن جرائم الكمبيوتر ومنها التوقيع الالكتروني على أنه في حالة رفض الدولة طلب التسليم وقع عليها التزام بمعاقبة المتهم " حيث نصت على أنه إذا لم تقدم الدولة الطرف التي يوجد الجاني في إقليمها بتسليم ذلك الشخص فيما يتعلق بالجرم تنطبق عليه هذه المادة لكونه أحد مواطنيها وجب عليها بناء على طلب الدولة الطرف التي تطلب التسليم، أن تحيل القضية دون إبطاء ولا مسوغ له سلطاتها المختصة بقصد الملاحقة ويتعين على تلك السلطات أن تتخذ قرارها وتصطلح بإجراءاتها وفقا لمبدأ المعاملة بالمثل ويتعين على الدول الأطراف المعنية أن تتعاون معا، خصوصا في الجوانب الإجرائية ضمانا لفاعلية تلك الملاحقة [4].

[1]- جميل عبد الباقي الصغير ، مرجع سابق ، ص89.

[2]- فهد عبد الله العبيد العازمي، مرجع سابق ، ص535.

[3]- تحضر المادة 53 من الدستور المصري تسليم اللاجئين السياسيين وكذا المادة الثالثة من البند الرابع من القانون العماني حيث نص على إذا كان المطلوب تسليمه قد منح حق اللجوء السياسي في السلطنة قبل طلب التنازل واستمر متمتعا بهذا الحق بعد ورود الطلب.

[4]- ايمن رمضان محمد أحمد، مرجع سابق ، ص408

كما نصت الاتفاقية العربية لمكافحة الجريمة في مادتها السادسة فقرة أ على أنه، لا يجوز التسليم إذا كانت الجريمة المطلوب من اجلها التسليم، معبرة بمقتضى القواعد القانونية النافذة لدى الدولة المتعاقدة المطلوب إليها التسليم، جريمة لها صبغة سياسية وكذلك المادة الثالثة من معاهدة الأمم المتحدة النموذجية بشأن تسليم المجرمين 1950 وأيضا المادة الرابعة من اتفاقية جامعة الدول العربية لتسليم المجرمين 1952 وأيضا المادة 20 من الاتفاقية الأمنية لدول مجلس التعاون الخليجي.

و استنادا إلى هذا الشرط ترفض الدول المنظمة إلى الاتفاقية الأوروبية للتعاون تسليم المجرمين بذريعة أن من شأن التسليم في جرائم معينة المساس بمصالحها الأساسية ومن أمثلة الجرائم المعلوماتية التي تشكل المساس بالمصالح الأساسية لدولة "جريمة الدخول بطريق غير مشروع عن طريق الشبكات الدولية أو الجامعية إلى قواعد البيانات الإستراتيجية أو العلمية أو الاقتصادية أو المالية [1].

ج-عدم جواز التسليم في الجرائم العسكرية: نصت المادة السادسة من الاتفاقية العربية لمكافحة الجريمة في فقرتها على أنه "لايجوز التسليم إذا كانت الجريمة المطلوب من أجلها السليم، تنحصر في الإخلال بواجبات عسكرية.

د-عدم جواز تسليم من تمت محاكمتهم عن ذات الجريمة المطلوب تسليمهم لأجلها: من كان الشخص المطلوب تسليمه قد سبقت محاكمته عن الجريمة المطلوب تسليمه لأجلها غير أو عوقب عنها فإنه لا يجوز تسليمه، ليس هذا فحسب بل انه لا يجوز التسليم متى ما كان فيد التحقيق والمحاكمة عن ارتكابه فعلا ما هو ذاته المطلوب تسليمه لأجله، ويعد هذا الشرط من الضمانات الأساسية عند محاكمة الشخص المطلوب تسليمه ويهدف إلى توفير أكبر قدر ممكن من الحماية القضائية لشخص المطلوب تسليمه في الدولة الطالبة وهذا حتى لا يتعرض هذا الشخص لعقوبة مزدوجة [2].

هـ-أن يكون قانون الدولة طالبة التسليم مختصا بمحاكمة الشخص المطلوب تسليمه: يجب أن ينعقد الاختصاص بنظر جرائم الاعتداء على التوقيع الالكتروني لقانون الدولة طالبة التسليم وبالمقابل يتعين إلا يكون قانون الدولة المطلوب إليها التسليم مختصا بمحاكمة الشخص المطلوب تسليمه عن ذات العقل المنسوب إليه، وقد تبنت اتفاقية بودابست بشأن جرائم الحاسب الآلي نهجا متميزا في جرائم الاعتداء على التوقيع الالكتروني عندما أكدت على مبدأ إما التسليم وأما المحاكمة في جرائم الحاسب الآلي.

[1]- فهد عبد الله العبيد العازمي. مرجع سابق ، ص537.

[2]- محمد كمال محمود الدوسيقي ، مرجع سابق ، ص185.

و من التطبيقات العملية للتسليم في جرائم الاعتداء على التوقيع الالكتروني في هذا المجال عملية اوديسيونodysseus في فيفري 2004 بمبادرة من يوروبول، حيث قامت الشرطة من خلالها بعمليات شملت 15 دولة، استراليا، بلجيكا، كندا، ألمانيا،هولندا، النرويج،..." وقد تم تسليم المتهمين إلى سلطات التحقيق في بريطانيا حيث قضي بإدانتهم [1].

و-أن يكون الاعتداء على التوقيع الالكتروني في المنسوب إلى المتهم بشكل جريمة في قانون الدولة طالبة التسليم:

يشترط لقيام الدولة بتسليم شخص ما إلى دولة أجنبية أن يكون الاعتداء على التوقيع الالكتروني المنسوب إلى المتهم مجرما في قانون الدولة طالبة التسليم وفي قانون الدولة المطلوب إليها معا وقد أكدت المادة 24 من اتفاقية بودابست بشأن جرائم الحاسب الآلي على أنه يجب تسليم المتهمين بين الأطراف فيما يتعلق بالجرائم المبينة في المواد 2-11 من الاتفاقية، شرط أن تكون تلك الجرائم معاقبا عليها بموجب القوانين في بلد كل الطرفين المعنيتين بحرمان من الحرية لفترة أقصاها سنة على الأقل أو بعقوبة أشد ما لم يوجد اتفاق أو معاهدة بخلاف ذلك [2].

و هذا ما تضمنته المادة 166 من قانون رقم 2004/302 حول التعاون القضائي الدولي في المسائل الجنائية أحكاما مماثلة، كما أكدته المادة 66 من قانون رومانيا حيث نصت على حق الدولة ذات الصلاحية في أن ترسل تلقائيا إلى السلطات الأجنبية ذات الصلاحية، المعلومات والبيانات الضرورية، التي تسمح لهذه الأخيرة باكتشاف الجرائم المرتكبة بواسطة جهاز الحاسوب، أو بحل القضية المتعلقة بتلك الجرائم [3].

م-عدم القضاء الدعوى العمومية أو العقوبة: يشترط بجواز التسليم إلا تكون الدعوى العمومية أو الحكم القاضي يفرض عقوبة قد انقضى بأحد أسباب الانقضاء المحددة في التشريعات الوطنية للدولة طالبة التسليم والمطلوب إليها التسليم أو الدولة التي ارتكبت الجريمة على أرضها[4]

[1]- إيهاب محمد يوسف، مرجع سابق، ص23.

[2]- هلالي عبد الإله أحمد، مرجع سابق ، ص250.

[3]- أيمن رمضان محمد أحمد، مرجع سابق، ص410.

[4]- ياسر محمد الكومي محمود أبو حطب، مرجع سابق ، 360.

ثانيا: إجراءات تسليم المجرمين في جرائم التوقيع الالكتروني.

يقصد بإجراءات التسليم ذلك القواعد ذات الطبيعة الإجرائية التي تتخذها الدول الأطراف في عملية التسليم وفقا لقوانينها الوطنية وتعهداتها لأجل إتمام عملية التسليم، بهدف التوفيق بين المحافظة على حقوق الإنسان وحريته وبين تامين صالح العام الناشئ عن ضرورات التعاون الدولي في مكافحة الجريمة بحيث لا يفلت أي مجرم من العقاب، وهذه الإجراءات تتقاسمها الدولتان الطالبة والمطالبة وكما أنها ليست مطلقة بل مقيدة ببعض الالتزامات الدولية والتعهدية وهذا ما نصت عليه اتفاقية الأمم المتحدة لمكافحة الفساد unلتعاون الدولي المادة 44 فتسليم المجرمين الفقرة 14 " تكفل لأي شخص تتخذ بشأنه إجراءات فيما يتعلق بأي من الجرائم التي تنطبق عليها هذه المادة معاملة منصفة في كل مراحل الإجراءات، بما في ذلك التمتع بجمع الحقوق والضمانات التي تنص عليها القانون الداخلي للدولة الطرف التي يوجد فيها ذلك الشخص في إقليمها.[1]

أ- طلب التسليم

- يعتبر طلب التسليم الأداة التي من خلاله تعتبر الدولة الطالبة صراحة عن رغبتها في استلام الشخص المطلوب، فبدونه لا يمكن أن ينشأ الحق في التسليم، والأصل أن يكون كتابة حيث أنه لا يجوز أن يقدم هذا الطلب شفاهة غير مكتوب كأن يرسل برقيا أو تلغرافيا أو عن طريق اتصال الكتروني، لا في حالات معينة تتميز بصفة الاستعجال وغلى سبيل الاستثناء[2].

1- مراحل طلب التسليم.

يمر طلب التسليم ب 3 مراحل وهي:

المرحلة الأولى: تتمثل في تلقي الطلب واتخاذ إجراءات التحري وجمع الاستدلالات والقبض على الشخص المطلوب وهي من اختصاص الشرطة.

المرحلة الثانية: تتمثل في استجواب المقبوض عليه وحبسه احتياطيا أو إطلاق سراحه بكفالة أو بدونها أو منعه من مغادرة الأراضي الإقليمية إلى أن يتم الفصل في الطلب الوارد بشأنه وهي من اختصاص الادعاء العام.

[1]- فهد عبد الله العبيد العازمي، مرجع سابق. ص 547.

[2]- ياسر محمد الكومي محمود أبو حطب، مرجع سابق. ص 326.

المرحلة الثالثة: وهي فحصه الطلب من قبل المحكمة المختصة، والبت فيه بالقبور أو الرفض والمحكمة وهي بصدد ذلك تتحقق متى توافرت الشروط الشكلية.[1]

2- الأوراق والمستندات التي تطلب المشرع إرفاقها بالطلب:

أمل حكم الإدانة أو أمر القبض أوليه أوراق أخرى لها القوة نفسها صادرة طبقا للأوضاع المقررة في قانون الدولة الطالبة أو صورة رسمية مما تقدم.

- بيان الأفعال المطلوب التسليم من أجلها يوضح فيه زمان ومكان ارتكابها وتكييفها القانوني مع الإشارة إلى المواد القانونية المطابقة عليها وصورة من هذه المواد.

- أوصاف الشخص المطلوب تسليمه بأكبر قدر ممكن من الدقة وأيه بيانات أخرى من شانها تحديد شخصية وجنسية السلطات القضائية في الدولة الطالبة.

- وأن تطلب من الدولة المطلوب منها التسليم بأي طريق من طرق الاتصال الكتابية حسب توفيق الشخص احتياطياإلى حين وصول طلب التسليم ويجوز في هذه الحالة للدولة المطلوب منها التسليم أن تحسب الشخص المطلوب احتياطيا2

3- الجهات المناط بها أعداد طلب التسليم: يعتبر إعداد طلبي التسليم من الأعمال التي تتصل بالنظام القضائي للدول، فمثلا في مصر نجد المادة 1712 من التعليمات العامة لنيابة تقتضي بأن تتولى النيابة العامة إعداد طلب التسليم من خلال مكتب المحامي العام الأول ويجب أن يقدم طلب التسليم في الجرائم المعلوماتية من حكومةالدولة الطالبة إلى الحكومة المصرية عن طريق وزارة الخارجية المصرية أي بطرق الدبلوماسية والتي تحيله بعد فحصه من الناحية السياسية إلى وزارة العدل للنظر فيه وتقرير مدى أحقيته [3].

أما في الولايات المتحدة الأمريكية فإن إجراءات التسليم تبدأ من إدارة العدل، مكتب الأعمال الخارجية، حيث يقدم الطلب بصفة أساسية من محاكم الولاية طالبة التسليم أو من المحامي العام لهذه الولاية أو النائب المحلي الخاص بها، وفي فرنسا يتم إعداد طلب التسليم من وكيل النائب العام الذي يرسله إلىالنائب العام فيتولى هذا الأخير إرساله إلى وزارة العدل حيث تقوم الأخيرة بإرسال ملف التسليم

[1]- سليمان أحمد فضل، مرجع سابق، ص 421.

[2]- فهد عبد الله العبيد العازمي. مرجع سابق ص 546.

[3]- جميل عبد الباقي ، المرجع سابق ، ص92.

كاملا إلى وزارة الخارجية التي تتولى عبر القنوات الدبلوماسية إرسال الملف إلى سفارتها في الدولة المطلوب منها التسليم [1].

ب: نقل الأشخاص المحكوم عليهم.

تنص اتفاقية الأهم المتحدة لمكافحة الفساد.un التعاون الدولي المادة 45بشأن نقل الأشخاص المحكوم عليهم، يجوز لدول الأطراف أن تنظر في إبرام اتفاقات أو ترتيبات ثنائية أو متعددة الأطراف بشأن نقل الأشخاص الذين يحكم عليهم بعقوبة الحبس أو بأشكال أخرى من الحرمان من الحرية، لارتكابهم أفعالا مجرمة وفقا لهذه الاتفاقيةإلىإقليمها لكي يكمل أولئك الأشخاص مدة عقوبتهم هناك، بإضافة إلى ذلك فإنه يجب عند تسليم الشخص محل التسليم أن تسلم معه كل ما كان في جوزته أثناء القبض عليه وكل ما يمكن أن يكون دليلا عن الجريمة ويجوز الاحتفاظ بها إذا رأت الدولة المطلوب إليها التسليم لزوما لذلك أو أن تحتفظ بحق استرجاعها مستقبلا [2].

و فيما يتعلق بنفقات التسليم يتم تحديدها وفقا لما جاء بنصوص المعاهدة المبرمة بين الدولتين المتعاقدتين أو بين الدول المتعاقدة في حالة المعاهدة الدولية متعددة الأطراف.

أما الأموال التي تدفع لنقل الشخص المطلوب تسليمه ومحصلات الجريمة وأحيانا لترجمة الوثائق والمستندات المطلوبة، فإنه وفقا لما هو مستقر عليه تكون على الدولة الطالبة التسليم ما لم يتم الاتفاق على غير ذلك.[3]

الفرع الثالث: مظاهر التعاون الدولي في مجال تسليم المجرمين.

نظرا لاختلاف وتنوع النقم القانونية الإجرائية ولضبط المجرمين وتحقيق قواعد العدالة وضمان عدم الإفلات من العقاب سارعت العديد من الدول إلىإبراماتفاقات ومعاهدات دولية لفتح مجال أمام التعاون الدولي في مجال تسليم المجرمين وتحقيق مبدأ عالمية العقاب ومن خلال هذا الفرع سنحاول دراسة النقاط الآتية:

أولا: عالمية حق العقاب في جرائم التوقيع الالكتروني: ويعبر عنه بمبدأ عالمية النص الجنائي أو النظام العقاب العالمي يهدف إلى التصدي لتنامي الظواهر الإجرامية ذات الأبعاد الدولية من خلال تجاوز القيود التي يفرضها مبدأ الإقليمية فينعقد الاختصاص القاضي الجنائي لأي دولة من دول العالم بغض

[1]- ياسر محمد الكومي محمود أبو حطب، مرجع سابق، ص323.

[2]- المادة 37 من الاتفاقية الأمنية الخليجية 1994، والمادة 12 من اتفاقية جامعة الدول العربية لتسليم المجرمين 1953.

[3]- فهد عبد الله العبيد العازمي ، مرجع552.

النظر عن المكان الذي ارتكبت فيه الجريمة الالكترونية أو جنسية من ارتكابها أو نوع الجريمة [1] ويؤسس هذا المبدأ على فكرة التضامن بين الدول في مكافحة الجرائم فالتدخل الدولي وفقا لهذا المبدأ يهدف إلىتجنب إفلات المجرمين من العقاب وضمان محاكمة الجناة بغض النظر عن جنسياتهم أو جنسية المجني عليهم أو مكان أو نوع الجريمة ولقد نظر الفقه الجنائي إلى مبدأ العالمية يوصفه مكملا لغيره من المبادئ التي تحكم نطاق تطبيق العقوبات لسد ما يتسرب عليها من نقص [2].

بما أن جرائم التوقيع الالكتروني ذات يعد دولي عابر للحدود لارتكابها عبر شبكة الانترنت باستخدام التقنية العالية وكذا امتيازها سيمات الكترونية مما جعلها عن أيدي العدالة الجنائية وتنفيذ القوانين، لذا كان من الضروري إسنادهاإلى قانون دولي يمكن أن يستوعب الأحكام الخاصة بتلك النوعية من الجرائم المستحدثة وليس القانون الوطني وعلى ذلك فمبدأ عالمية العقاب يهدف إلى التصدي للجرائم العابرة للحدود أي الدولية ويتميز إفرادها بانتمائهم لفئة معتادي ومحترفي الإجرام[3].

ثانيا:تطبيقات عملية للتعاون الدولي لتسليم المجرمين في جرائم التوقيع الالكتروني:

و من التطبيقات العملية لتسليم المجرمين في جرائم الاعتداء على التوقيع الالكتروني في هنا المجال عملية أوديسوسodysseus التي تمت في فيفري 2004 بمبادرة من يوروبول حيث قامت قوات الشرطة خلالها بعمليات شملت 10 دول وهي: استراليا، بلجيكا، كندا، ألمانيا، هولندا النرويج، بيرو، اسبانيا، السويد وبريطانيا وقد تم تسليم المتهمين إلى سلطات التحقيق في بريطانيا حيث قمن بإدانتهم ولذلك يجب أن يكون هناك تنسيق بين مختلف التشريعات لتعريف جرائم الاعتداء على التوقيع الالكتروني أو على الأقل عدم اشتراط ازدواج التجريم وتوجد بالفعل بعض الاتفاقيات الدولية الثنائية التي تحدد الجرائم التي لا تتطلب فيها شرط ازدواج التجريم ومنها الجرائم المعلوماتية ومثال ذلك الاتفاقية الثنائية المتعلقة بالمساعدة القانونية المتبادلة واليت تم توقيعها بين أمريكا وكندا والتي لم تتطلب ازدواج التجريم كشرط للتعاون القضائي الدولي فيما بينهما وتدخل الجرائم المعلوماتية في إطار هذه الاتفاقية [4].

و نجد أيضا عملية محطم الجليد التي قام بها يوروبولeuropol في 14 يونيو 2005، ثم خلالها مداهمة وتفتيش أماكن في ثلاث عشرة دول أوروبية النمسا بلجيكا، فرنسا، المانيا، المجر، ايسلندا،

[1]- سليمان أحمد فضل،مرجع سابق ، ص411.

[2] - يعترف القضاء الفرنسي بمبدأ العالمية الدولة الطالبة إذا ارتكبت الجريمة محل طلب التسليم على إقليم الدولة الطالبة من قبل أحد رعاياها أو اجنبي، وذلك وفقا لقانون التسليم الفرنسي الصادر في 10 مارس 1927 في مادته الثالثة نبذ (3) فقرة (3)

[3]-سامي عبد الحميد، أصول القانون الدولي العام، الإسكندرية، دار الجامعية، طبقة الخامسة، الإسكندرية، مصر، 1998، ص32.

[4]- أيمن رمضان محمد أحمد، مرجع سابق.ص412.

ايطاليا، هولندا،بولونيا، برتغال،سلوفاكيا، السويد وبريطانيا، كما تم توقيف أفراد في كل من فرنسا، بلجيكا، المجر، ثم تم سليم المتهمين إلى بريطانيا التي قامت بتقديمهم للمحاكمة الجنائية وحكم القضاء بإدانتهم [1].

و في هذا الإطار أبرمت العديد من الاتفاقيات الدولية على اتفاقية الأوروبية للإجرام المعلوماتي حيث نصت المادة 29 على سرية حفظ البيانات المعلوماتية المخزنة وأجازت لكل طرف أن يطالب من الطرف الآخر الحفظ السريع للمعلومات المخزنة وعن طريق إحدى الوسائل الالكترونية الموجودة داخل النطاق المكاني لذلك الطرف الآخر والتي ينوي الطرف طالب المساعدة أن يقدم طالبا للمساعدة بشأنها بفرض القيام بالتفتيش أو الدخول بأي طريقة مماثلة وضبط أو الحصول أو الكشف عن البيانات المشار إليها.

كما أشارت المادة 31 من هذه الاتفاقية إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش، وأن يدخل بأي طريقة مشابهة وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني [2].

و من ناحية أخرى قامت اللجنة الأوروبية بشأن مشاكل الجريمة ولجنة الخبراء في مجال جرائم الحاسب الآلي بإعداد مشروع اتفاقية دولية تتعلق بجرائم الحاسب الآلي، وقد أعلن المجلس الأوروبي مشروع هذه الاتفاقية في افريل 2000م وأكد المجلس أن الاعتداءات الحديثة على مواقع الانترنت التجارية هي التي لفتت نظر المجتمع الدولي إلى المخاطر الآلي، وأن الجرائم المعلوماتية تهدد التجارة والمصالح الحكومية وبعد سنة ونصف تقريبا من المناقشات والتعديلات على هذا المشروع تم التوقيع على اتفاقية بودابست سنة 2001 بشأن الإجرام المعلوماتي [3].

و من الوقائع العملية التي طرحت على القضاء المغربي نجد قضية zotob هي من النهر القضايا نظرا لحجم الخسائر الناجمة من الأفعال المجرمة وكذا يكون المواقع المعتدى عليها خاصة بالكونجرس من الأمريكي وكذا مواقع مؤسسات إعلامية ضخمة بالولايات المتحدة الأمريكية، بإضافة إلى موقع مطار سان فرانسيسكو الأمريكي ومواقع عديدة لمستعملي windows2000وقد اتهم في هذه القصة الشاب المغربي 18 سنة كمتهم رئيس ومتهم آخر، وقد وجهت لهما تهمة تكوين عصابة إجرامية وتهمة السرقة واستعمال

[1]- إيهاب محمد يوسف، مرجع سابق ، ص220.

[2]- فهد عبد الله العبيد العازمي، مرجع سابق ، ص567.

[3]- هلالي عبد الله أحمد، مرجع سابق ، ص214.

بطاقات ائتمان مزورة وتهمة الولوج غير المشروع لنظم المعالجة الآلية للمعطيات وتزوير وثائق الكترونية [1].

[1]- فهد عبد الله العبيد العازمي، مرجع سابق ، ص572.

المبحث الثاني: التعاون القضائي الدولي لمكافحة جرائم التوقيع الإلكتروني

لا سبيل لملاحقة الجناة في جرائم الاعتداء على التوقيع الإلكتروني إلا من خلال التعاون الشرطي الدولي على الصعيد الإجرائي الجنائي وعلى نحو يتيح الاتصال مباشرة بين أجهزة الشرطة في مختلف الدول، وإنشاء مكاتب متخصصة عن مرتكبي تلك الجرائم [1] فيتعذر على الدولة بمفردها مكافحة هذه الجرائم كونها ترتكب في الغالب عبر إقليم أكثر من دولة حيث لا يتحقق التعاون الدولي في مجال مكافحة جرائم التوقيع الإلكتروني إلا من خلال عدة محاور أهمها تفعيل دور المنظمة الدولية لشرطة الجنائية وتعجيل الاتفاقات الشرطية الدولية[2] وكذا تفعيل أسلوب التدريب على التحقيق في جرائم التوقيع الإلكتروني لكل من رجال الضبط القضائي ونيابة عامة والاستفادة من خبرات المتخصصين في هذا المجال لمواجهة تلك الجرائم ومن ثم لا سبيل لتحقيق الأمن خلال المساعدة القضائية بين الدول وتسهيل مهمته المحاكمة من تبادل معلومات ونقل إجراءات وإنابات قضائية.

المطلب الأول: التعاون الدولي الشرطي لمكافحة جرائم التوقيع الإلكتروني في مرحلة جمع الاستدلالات.

تمثل المساعدة البوليسية بين أجهزة الشرطة الجنائية المخصصة لمكافحة الجرائم المعلوماتية بصفة عامة وجرائم التوقيع الإلكتروني بصفة خاصة أحد أهم الوسائل الهامة التي يمكن من خلالها مكافحة هذه الجرائم حيث سيستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة لحدود، لان جهاز الشرطة في هذه الدولة أو تلك لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابع لها فملاحقة مرتكبي هذه الجرائم وتقديمهم للعدالة لتوقيع العقاب عليهم يستلزم تعاون دولي شرطي وتأكيد على ذلك أنشأت العديد من منظمات الشرطة على الصعيد الدولي وأبرمت العديد من الاتفاقيات الدولية وأنشأت مكاتب شرطة انترنت لمكافحة جرائم الاعتداء على التوقيع الإلكتروني وسوف نتناول ذلك على النحو التالي:

الفرع الأول:المنظمات الدولية للشرطة الجنائية.

يعتبر التعاون الدولي على الصعيد الشرطي من أهم السبل لمواجهة جرائم الاعتداء على التوقيع الإلكتروني نظرا لخصوصيتها من جهة وتعديها لحدود الدولة من جهة أخرى، وتأكيدا لذلك تم

[1] - ايمن رمضان محمد أحمد، مرجع سابق. ص 416.

[2] - يوسف، بن سعيد الكلباني، مرجع سابق، ص 292.

إنشاءمنظمات دولية شرطية في المجال الجنائي لتعزيز التعاون بين أنظمة الدول المختلفة وهذا ما سنبينه على النحو التالي:

أولا: دور الانتربول في الكشف عن جرائم الاعتداء على التوقيع الالكتروني

لا مقام لنظام دولي أمني دون تعاون دولي فعال وإيجابي في الشرطي والقضائي الدوليين ويشكل هذا التزاما قانونيا دوليا لتأمين الحياة البشرية من المخاطر التي تهدد استقرارها وأمنها وهذا ما جعل بالمجتمع الدولي إلى الاعتماد على منهج جديد يتمثل في إنشاء أجهزة تعاونية على مستوى حكومي فني يتمثل في المنظمة الدولية لشرطة الجنائية حيث تعتبر أكبر منظمة شرطية في العالم أنشئت بغرض تيسير التعاون الشرطي العابر للحدود ودعم ومساعدة جميع المنظمات والسلطات والأجهزة التي تمثل مهمتها في الوقاية من الإجرام ومكافحة والبحث عن المجرمين وإيقافهم وتسليمهم ويستلزم الأمر هنا التعرض لدراسة النقاط الآتية:

أ- أهداف ومهام المنظمة الدولية لشرطة الجنائية في مجال مكافحة جرائم توقيع الالكتروني:

يعتبر التعاون الدولي سواء على الصعيد الشرطي أو القضائي أحد أهم السبل لمواجهة الاعتداء على التوقيع الالكتروني فيستحيل على الدولة منفردة مكافحة تلك الجرائم نظرا لطبيعتها الخاصة وتعديها حدود الدولة لارتكابها في غالب الأحيان خارج إقليمها[1]وتأكيد لذلك ثم إنشاء منظمة الشرطة الجنائية الدولية الانتربول والذي تهدف إلى تعزيز التعاون بين الأنظمة الداخلة لتلك الدول، وكذلك المساهمة في إقامة وتنمية نظم مكافحة ومنع الجرائم العادية جرائم القانون العام وتتبع مرتكبيها كانوا أفراد أو منظمات إجرامية عابرة للحدود.

حيث تتمثل مهام الانتربول الأساسية في تجميع البيانات والمعلومات لكشف عن الجريمة وتحديد الجاني والتعاون بين الدول في تتبع المجرمين الفارين والقبض عليهم ولا ينحصر اختصاص المنظمة في إطار الجرائم التي ترتكب داخل حدود إقليم الدولة يتعداه إلى الجرائم العابرة للحدود سواء من حيث العقل المادي المكون للجريمة أو النتيجة الإجرامية [2] ونلخص في ذلك أن نهدف الانتربول باختصار هو الوصول إلى بلد عالمي مأمون ومن أجل ذلك عمل الانتربول جاهدا للوصول إلى أربع وظائف أساسية يرتكز عليها وهي:

1- خدمات اتصال شرطي عالمي مأمون

[1]- عمر الفاروق الحسين، المشكلات الهامة في الجرائم المتصلة بالحاسب الألي وأبعادها الدولية، دراسة تحليلية لنصوص التشريع المصري مقارنا بالتشريع الفرنسي، دار النهضة العربية، القاهرة، طبيعة 2، مصر، 1995، ص 133.

[2]- حسين فتحي الحامولي، التعاون الدولي والأمني في تنفيذ أحكام جنائية، دار نهضة عربية ، مصر، 2014، ص 520.

2- خدمات بيانات ميدانية وقواعد بيانات للشرطة: أسماء، صور، بصمات جوازات سفر... إلخ.

3- خدمات إسناد شرطي ميداني وخاصة في مجال جرائم التوقيع الإلكتروني.

4- التدريب والإنماء الشرطي: تدريب شرطي مركز لأجهزة الشرطة الوطنية من دعم وتوجيهات بهدف تعزيز قدرة البلدان الأعضاء في مكافحة الجرائم الإلكترونية [1].

ب- اختصاصات المنظمة الدولية للشرطة الجنائية:

بمقتضي ميثاق منظمة الانتربول ونظامها الداخلي تتمتع هذه المنظمة بحملة من الاختصاصات العامة والخاصة التي تخولها القيام بنشاطات متعددة خاصة نصالمادة 2 الفقر بين أ- ب لذلك فإن خطورة جرائم التوقيع الالكتروني تفرض على الدول البحث عن وسائل متطورة وملائمة للحد منها، وذلك بالتضييق على التغيرات القانونية التي ستسمح لمرتكبي الإجرام بالهروب من العقاب أو بإقرار مجموعة من الآليات ذات الطبيعة التقنية والإدارية مستفيدين من التقدم التكنولوجي في مجال الاتصالات المعلوماتية ومن بين الاختصاصات التي تقوم بها المنظمة ما يلي:

1- الاختصاصات العامة:

-تجميع وتبادل المعلومات والبيانات:

ويشمل هذا المحور المعلومات بالمعنى الواسع حيث يدخل فيها البلاغات أو المرسلات أو الاتصالات التي يقوم بها رجال الشرطة في دولة عضو مع دولة أخرى عضو في الأمانة العامة بصدد الأنظمة الإجرامية ومرتكبيها ويشمل ذلك أوصاف المجرمين وبصماتهم وصورهم الفتوغرافية وأوصاف الأشياء محل الجرائم وصورها.

وفي هذا الإطار نحت المادة الأولى من اتفاقية الرياضي العربية للتعاون القضائي التي وافق عليها مجلس وزراء العدل العرب في المؤتمر العربي الأول بالقرار رقم 01 بتاريخ 5 أفريل 1983 بشأن ضرورة تبادل المعلومات بين دول الأطراف فيما يتعلق بالنصوص التشريعية النافذة والبحوث القانونية والقضائية، كما ألزمت المادة الخامسة من نفس الاتفاقية دول الأطراف فيها أن ترسل إلى وزارة العدل في كل دولة آخر البيانات عن الأحكام القضائية النهائية الصادرة ضد المواطنين أو الأشخاص المقيمين أو المولودين في إقليمها، كما تطرف مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين إلى ضرورة تطوير التبادل المنهجي للمعلومات، باعتبارها عنصرا مهما في خطة العمل الدولي لمنع الجريمة ومكافحتها،

[1]- فنور حاسين، لمنظمة الدولية لشرطة الجنائية والجريمة المنظمة، رسالة ماجستير في القانون الدولي وعلاقات الدولية، جامعة جزائر بن عكنون، 2012- 2013، ص 7، 8.

وأوصي كذلك بالتزام منظمة الأمم المتحدة بإنشاء قاعدة معلوماتية لا علام الدول الأطراف باتجاهات العالمية في مجال الجريمة [1].

هذا وقد تطرق شنغن للاتحاد الأوروبي المبرم في 24 جوان 1985 في مادته 39 إلى صياغة نظاما متكاملا لتبادل المعلومات، حيث ألزمت الدول الأطراف تبادل المعلومات فيما بين المراكز والهيئات والإدارات الوطنية المختصة ودعت إلى الحد من القيود المقررة بالخصوص. بين هذه المعلومات عناوين الأفراد سواء أولئك المطلوب تسليمهم من قبل دول أخرى، أو الممنوعين من دخول أراضي دولة ما أو المعلن اختفاؤهم أو المطلوب تقدمهم للعدالة بأمر قضائي لأي سبب كان[2].

- **تبادل الخبرات والمساعدة التقنية**:وفي هذا الإطار اتفقت الدول على ضرورة تبادل العناصر الإدارية الفنية وتعزيز القدرات التقنية لأجهزة العدالة، وكذا تحليل ونشر البيانات والمعلومات المتاحة حول الجرائم اعتداء على التوقيع الإلكتروني والسبل والآليات المبتكرة لمكافحة هذه الجرائم وفي هذا تطرق إعلان الأمم المتحدة بشأن الجريمة والأمن العام في مادته الرابعة [3]إلى ضرورة تقديم المساعدة التقنية الثنائية والمتقدمة الأطراف إلى دول الأعضاء، باستخدام التدريب وبرامج التبادل في الأكاديميات الدولية للتدريب على إنفاذ القوانين والمعاملات المعنية بالعدالة الجنائية على الصعيد الدولي أما المادة 21 من نفس مشروع الاتفاقية السالفة الذكر فإنها تنص في فقرتها الأولى والثنائية في إطار سياستها المقررة لدعم أشكال المساعدة التقنية على أنه " على الدول الأطراف أن تتعاون على صوغ برامج خاصة بشأن تبادل الخبرات والتدريب بين المسؤولين المختصين،وأن تمد بعضها البعض بالمساعدة الكفيلة بتسيير حصولها على المعدات أو تكنولوجيا تثبت فعاليتها في الجهود الساعية إلى تنفيذ هذا البرتوكول هذا وعلى الدول الأطراف أن تساعد بعضها البعض في تخطيط وتنفيذ برامج البحث الرامية إلى تقاسم الخبرة في مجال جرائم التوقيع الإلكتروني وتطبيق هذه الغاية لها أن تستخدم أيضا عن الاقتصاد المؤتمرات والحلقات الدراسية الإقليمية والدولية لتعزيز التعاون وتنشيط النقاش حول المشكلات ذات الأهمية المشتركة [4].

[1] - راجع: مؤتمر الأمم المتحدة السادس لمنع الجريمة، ومعاملة المجرمين، مجلة العدالة: السنة 8 العدد 27، تصدر عن وزارة العدل أبوظبي، أفريل 1981، ص 146.

[2] - أيمن عبد الحفيظ، مرجع سابق، ص 226 227.

[3] - الوثائق الرسمية الجمعية العامة للأمم المتحدة، دورة 51 – إعلان الأمم المتحدة بشأن الجريمة والأمن العام الوثيقة رقم (22/A/51) الأمم المتحدة نيويورك 1996 – ص 03.

[4] - شريف سي كامل، الجريمة المنظمة في القانون، طبعة الأولى، دار النهضة العربية ، القاهرة، مصر، 2001، ص 37.ب

2- الاختصاصات الخاصة:

-تعامله مع جهاز الشرطة والادعاء العام والقضاء في بلد معين

يرتكز عمل المركز الوطني للإنتربول في علاقاته مع جهاز الشرطة والادعاء العام والقضاء في بلد معين بناءا على نص المادة 32 من أحكام التنظيمية المسيرة لمنظمة الانتربول ولعل في الإشارة إلى المكتب المركزي الوطني – انتربول الجزائر"centre national Interpol Algérie".

ففي شهر أوت من سنة 1963 تقدمت الدولة الجزائرية بواسطة وزارة الخارجية بطلب الانخراط ضمن المنظمة الدولية للشرطة الجنائية / انتربول وقد حظي طلبها بموافقة أغلبية الدول الأعضاء، البالغ عددهم حينها واحد وخمسين51 ويقع المكتب المركزي الوطني للإنتربول الجزائر، تحت السلطة المباشرة لمديرية الشرطة القضائية التابعة إداريا لتصرف المديرية للأمن الوطني ويمارس مهامه وفقا اللأطر القانونية التالية:

- التشريعات والقوانين الوطنية، التشريعات الإقليمية والدولية.
- الأحكام التنظيمية المسيرة لمنظمة الانتربول، الأعراف الدولية، ومبدآ المعاملة بالمثل.

حيث يعتبر المكتب المركزي الوطني، القناة الرسمية الوحيدة في مجال التعاون الدولي ما بين المصالح الوطنية المكلفة بتنفيذ القانون في مجال الشرطة القضائية والمنظمة الدولية للشرطة الجنائية وكذا مجمل المكاتب المركزية الوطنية البالغ عددها حاليا 188.

في مجال النشاط الشرطي: حيث يقوم بما يلي:

- مباشرة التحقيقات الدولية من وإلى الخارج الوطن بالتنسيق مع المصالح الوطنية ونظيراتها الأجنبية.
- التبادل الآني والسريع للمعلومات الشرطية والجنائية ما بين المكاتب المركزية الوطنية لبلدان الأعضاء، بالتنسيق مع الأمانة العامة لمنظمة الانتربول.
- ملاحقة المجرمين المبحوث عنهم دوليا.
- تجميع المعلومات المعلوماتية، تحليلها وتبليغها للتحري والاستغلال إلى المصالح الوطنية.
- تقديم الدعم الفني التقني على كافة الأجهزة والمصالح الوطنية المكلفة بتنفيذ القانون.

في مجال التعاون القضائي الدولي: حيث يقوم بما يلي:

تنفيذ أوامر بالقبض الدولية الصادرة عن السلطات الأجنبية وأيضا تلك الصادرة عن السلطات القضائية الوطنية.

- المساهمة في تنفيذ الانابات القضائية الدولية، وطلبات المساعدة القضائية أو البحث الجزائي الدولي.
- تنفيذ إجراءات تسليم المجرمين [1]،خدمات اتصال شرطي عالمي مأمون:

وتعتبر من أهم الخدمات التي يقدمها الأنتربول لمختلف دول الأعضاء، فيه حيث يقوم الأنتربول بإتاحة منظمة اتصالات شرطية عالمية تعرف بمنظومة

24/7-اتسمح لموظفي إنفاذ القانون المرخص لهم في جميع البلدان أعضاء طلب معلومات شرطية عامة وإحالتها والوصول إليها بشكل أني ومأمون، إذ تؤكد الإحصائيات الصادرة عن منظمة الانتربول أن هناك أكثر من ثلاثة ملايين معلومة خاصة بالمجرمين قد تم تقديمها إلى الدول الأعضاء في المنظمة.

ب- أجهزة المنتظمة الدولية للشرطة الجنائية

يتشكل بيان المنظمة من الأجهزة الآتية[2]

الجمعية العامة: وهي الهيئة السياسية العليا الجهاز العام للمنظمة، ويمثل فيها كافة الدول الأعضاء ويتكون وفي الدولة عادة من أعضاء من جهاز الشرطة إلى جانب خبراء في المسائل ذات العلاقة بعمل الشرطة وتختص الجمعية بالنظر والبحث والدراسة والتقرير في كل ما يتصل بالتعاون الشرطي الدولي وهي المختصة بتحديد السياسة العامة للمنظمة وإصدار التوصيات والقرارات لأعضائها في المسائل التي تختص بنظرها ومعالجتها ودراسة وإقرار الاتفاقيات التي تفقدها المنظمة مع الهيئات الأخرى وكذا وضع السياسة المالية للمنظمة وبصفة عامة العمل على تقرير المبادئ والإجراءات العامة الملائمة لبلوغ الأهداف والمتمثلة في تشجيع المعونة المتبادلة في أوسع على نحو فعال في منع مكافحة الجريمة ونعقد الجمعية دوراتها العادية مرة واحدة في السنة وكل مرة في إقليم دولة مختلفة من دول الأعضاء ولها أن تعقد اجتماعات غير حين تتطلب الظروف وبناء على طلب اللجنة التنفيذية أو من غالبية الأعضاء وتعقد الدورة غير العادية في مقر المنظمة كمبدأ عام وتنتخب الجمعية رئيسها وثلاث نواب للرئيس وتسعة مندوبين ومنهم جميعا تتألف اللجنة التنفيذية [3].

[1]- شريف سي كامل، مرجع سابق، ص 45

[2]- أيمن عبد الحفيظ، مرجع سابق، ص 220.

[3]- جميل عبد الباقي صغير، مرجع سابق، ص 88

- اللجنة التنفيذية:

تتألف من ثلاث عشرا عضوا رئيس الجمعية العامة ونوابه الثلاثة والمندوبين التسعة تختارهم الجمعية العامة على أساس توزيع جغرافي منصف لا يجوز أن ينتهي اثنين منهم للدولة واحدة وهذه الولاية للرئيس أربع سنوات وباقي الأعضاء ثلاث سنوات غير قابلة للتجديد وتتمثل مهمة اللجنة التنفيذية في الإشراف على عمل السكرتارية العامة للمنظمة ومتابعة تنفيذ قرارات الجمعية العامة ومباشرة ما قد تعهد به إليها الجمعية من اختصاصات واتخاذ قرارات حرمان الدولة العضو من خدمات المنظمة أو من حق التصويت إذا تخلفت الدولة عن أداء التزاماتها المالية ويمكن القول بأن اللجنة التنفيذية تقوم في الغالب بدور الجهاز التنفيذي للمنظمة وتجتمع اللجنة التنفيذية عادة ثلاث مرات في السنة [1].

- السكرتارية العامة الأمانة العامة للإنتربول

تعتبر الأمانة العامة الجهاز التنفيذي الدائم لمنظمة الانتربول وهي جهاز الإداري للمنظمة العامة واللجنة التنفيذية وتتضمن القسم المعني بإدارة السجلات الجنائية وهو حلقة اتصال بين المكاتب المركزية الوطنية للشرطة الجنائية ويرأسها سكرتير عام تختاره اللجنة التنفيذية وقرار تعينه لمدة خمسة سنوات.

الأقسام المتخصصة:

قسم الإدارة العامة: وتتلخص مهامه في ما يلي:

- المحاسبة المالية، وإدارة وتسيير الموظفين، العتاد، والمصالح العامة.
- تحظر وتنظم الجمعيات العامة، والاجتماعات الأخرى التي تنظمها المنظمة الدولية لشرطة الجنائية.
- كل أعمال الترجمة والكتابة والطبع والإرسالات الخاصة بوثائق المنظمة وينقسم قسم الإدارة العامة إلى ستة مصالح تتمثل في:

مصلحة إصدار الوثائق، مصلحة المحاسبة المالية، مصلحة الأمن، المصالح العامة، مصلحة الموظفين والشؤون الاجتماعية، مصلحة الاجتماعات والمهام [2].

[1]- ايمن رمضان محمد أحمد، مرجع سابق، ص 320.

[2]- فهد عبد الله العبيد العازمي، مرجع سابق، ص 460

- قسم الاتصال والإعلام الجنائي الخاص بالتعاون الشرطي

يختص هذا القسم بنشر المعلومات الشرطية ودراسة الملفات الجنائية ذات الاهتمام الدولي ويقوم بمعالجة القضايا الدولية وبرمجة المعلومات الشرطية ومنظومة المحفوظات الإلكترونية كما يحتوي هذا القسم على مكتب الاتصال الأوروبي ومكتب التنسيق الجهوي وأربع فروع مكلفة كل واحدة منها بقطاع واسع من الإجرام الدولي وتتمثل في:

- الإجرام بصفة عامة مخالفات ضد الأشخاص، مخلفات ضد ممتلكات الإجرام المنظم

- الجرائم الاقتصادية والمالية جرائم الاحتيال – تزوير...الخ .

- مكافحة الإيجار غير المشروع في مخدرات.

- مكلف بمعالجة المعلومات الموجهة إلى المكاتب المركزية الوطنية بوسائل تكنولوجية متقدمة منها والمتعلقة بالانترنت.

قسم خاص بالمحلية الدولية لشرطة الجنائية

ويعمل هذا القسم علىإصدار المحلية الدولية للشرطة الجنائية، مع حرصه على أن تتضمن كل المسائل المتعلقة بالشرطة في إطار مكافحة الجريمة الدولية كما تقوم هذه المنظمة مكن خلال هذه المحلية بتوضيح خطورة الجريمة المنظمة.

كما تبرز كذلك أهمية التعاون الدولي الشرطي من خلال المنظمة الدولية لشرطة الجنائية في مكافحة هذه الجريمة وكذا الطرق الحديثة التي تقوم بها أثناء المكافحة [1].

- الأقسام الثانوية:

- المكاتب المركزية الوطنية:

وهي شبكة من المكاتب الوطنية للشرطة الجنائية حيث يوجد لكل دولة عضو مكتب يقوم بدور قسم التنسيق الشرطي ولكن على مستوى إقليم الدولة وتعمل هذه المكاتب وفق الدستور المؤسس للمنظمة وبرغم أن تشكيل هذه المكاتب من اختصاص الدولة المعنية فإنها تضم عادة ضباط شرطة وخبراء في مجال الجريمة والمهمة الأساسية لهذه المكاتب أعمال الاتصال المستمر مع أجهزة وإدارات الشرطة في مختلف المناطق داخل الدولة أو المكاتب المناظرة لها لدى دول الأعضاء وتقوم بتجميع ما تتحصل عليه من

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص 47

مختلف الجهات من معلومات وبيانات تفيد في مكافحة الجريمة وتتبع المجرمين وهي شبكة واسعة للخدمات الشرطة على مستوى الدول الأعضاء في الانتربول.

- المستشارون:

تستعين المنظمة بعدد من المستشريين تتولى تعينهم اللجنة التنفيذية لدراسة مسائل خاصة ومدة ولايتهم ثلاث سنوات، ويتم اختيارهم من بين الأشخاص الذين يتمتعون سمعة عالمية في أحد المجالات التي تهم المنظمة وتقتصر وظيفتهم على بدء المشورة فقط ويجوز تنحية أيامنهم بقرار من الجمعية العامة لمنظمة [1].

ومن خلال ما سبق بيانه لتحقيق التعاون بين أجهزة الشرطة المتخصصة في ضبط ومكافحة جرائم التوقيع الالكتروني التي تتجاوز حدود الدولة لا بد من تفصيل دور الاتفاقيات الشرطية الدولية وتفعيل دور المنظمات الدولية للشرطة الجنائية وتفعيل دور الشرطة الانترنت في جرائم التوقيع الالكتروني وهذا ما ستتناوله على النحو التالي:

ثانيا: دور الاتفاقات الشرطية في ضبط جرائم الاعتداء على التوقيع الإلكتروني:

حيث يمكن دعم التعاون الشرطي بين الدول من خلال الاتفاقيات الدولية، بحيث إذا ما اكتشفت الشرطة الوطنية لدولة وقوع جريمة الاعتداء على التوقيع الالكتروني من خلال موقع موجود في الخارج، فإنها تقوم بالإبلاغ عن هذه الجريمة إلى السلطات البوليس بالدولة التي يقع فعل الاعتداء على إقليمها للقيام بإجراءات اللازمة لوقف هذا الاعتداء على الفور فضلا عن الاستفادة من تبادل الخبرات الأمنيةبين الدول المتقدمة وباقي الدول في مجال العمليات الشرطية والتدريب ووسائل الاتصال [2]

فمن الضروريفي التحقيقات الجارية بشان جرائم الاعتداء على التوقيع الإلكتروني أن تسارع الانتربول إلى ضبط المعلومات عن هذه الجرائم وحفظها وتحليلها وتبادلها مع جميع بلدانه الأعضاء عبر منظومة الإنتربول العالمية للاتصالات ويتم ذلك التعاون من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنظمة [3] وذلك عن طريق:

- تيسير التعاون الميداني بين البلدان أعضاء من خلال أعداء لائحة بأسماء ضباط اتصال متيسرين للمساعدة في التحقيقات بشان جرائم الاعتداء على التوقيع الإلكتروني.

[1]- يزيد بوحليط، مرجع سابق. ص 526.

[2]- أيمن رمضان محمد أحمد، مرجع سابق. ص 420.

[3]- جميل عبد الباقي الصغير، مرجع سابق.ص 85.

- زيادة تبادل المعلومات بين بلدان الأعضاء بشان الأساليب الإجرامية المتعبة في جرائم الاعتداء على التوقيع الالكتروني عن طريق الطرق العاملة الإقليمية وحلقات العمال التدريبية، وقد تم إنشاء نقاط اتصال مستمرة ويمكنها من تلقي أو تقديم المعلومات وطلبات المساعدة.

- مساعدة بلدان الأعضاء في التحقيق في الجرائم الإلكترونية عبر تسيير خدمات في مجال التحقيق وقواعد البيانات.

- إنماء شركات إستراتيجية مع منظمات دولية أخرى وهيئات القطاع الخاص وتسير لتعاون الدولي ينظم الانتربول مرة كل عامين مؤتمر دوليا بشأن الإجرام الالكتروني ومن بينها جرائم الاعتداء على التوقيع الالكتروني[1].

ومن التطبيقات العملية لتعاون الدولي في هذا المجال نجدعملية فالكون falcom في أفريل 2005 والتي تمت بين كل من الشرطة الفيدرالية الأمريكيةfBIوالانتربوبل والشرطة الفرنسية والتي سمحت بتفكيك شبكة تنشط في العديد من الدول الأوروبية.

وكذا عملية أوديسوسadysseus التي تمت في فيفري 2004 بمبادرة من يوروبول وقامت قوات الشرطة من خلالها بعمليات شملت 10 دول وهي استراليا، بلجيكا كندا، ألمانيا هولندا النرويج، بيرو، إسبانيا، السويد، بريطانيا وفي هذا الإطار حرصت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمةعبر الوطنية 106 والتي تم التوقيع عليها في باليرمو عام 2000 على حث الدول التي تطويرا التعاون فيما بينها لمكافحة جرائم الانترنت ومنها الاعتداء على التوقيع الإلكتروني، وتحتوي الاتفاقية على أشكال مختلفة من التعاون الدولي في مجال المساعدة القانونية المتبادلة والمصادرة، كما تدعو الاتفاقية أيضا جميع الدول إلى عقد اتفاقيات آخري بهدف تعزيز التعاون [2]

ثالثا: دور الانتربول في الكشف عن الجرائم الاعتداء على التوقيع الإلكتروني

اليوروبول هو أحد أجهزة مكافحة جرائم الحاسب الآلي والانترنت الأوروبية وهو المكلف بمكافحة جرائم الاعتداء على التوقيع الإلكتروني عن طريق معالجة المعلومات المرتبطة بالأنشطة الإجرامية على مستوى الاتحاد الأوربي وكذا بتسهيل تبادل تلك المعلومات عن طريق تزويد المحققين ومدهم بمساعدة التقنية وتعتبر ملف التحليل المبلغة من قبل سلطات التحقيق التابعة لدول الأطراف في الاتحاد الأوروبي في جرائم الاعتداء على التوقيع الإلكتروني، أحد أهم الوسائل التي يعتمد عليها المحققين في مكافحتهم

[1]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 343.

[2]- جميل عبد الباقي الصغير، مرجع سابق. ص 88.

للشبكات الإجراميةكما أن من التطبيقات العملية للتعاون الدولي في هذا النوع من الجرائم ما اوالتي عليه عملية محطم الجليد والتي قامت بها يوربول في 2005 حيث تم من خلالها مواهمة وتفتيش شبكات الحاسب الآلي في ثلاث عشرة دولة أوروبية هي النمسا، بلجيكا، فرنسا ألمانيا، المجر اسلندا، إيطاليا هولندا، بولونيا، البرتغال، سلوفاكيا، السويد، بريطانيا العظمي كما تم توفيق أفراد في كل من فرنسا بلجيكا، المجر واسلندا، والسويد[1].

رابعا: دور الأورجيست في الكشف عن جرائم الاعتداء على التوقيع الإلكتروني [2]

يساعد جهاز الأورجيست على التعاون القضائي والشرطي في مواجهة ومكافحة جرائم الاعتداء على التوقيع الالكتروني، وتنعقد اختصاصه عندما يمس ذلك الإجرام الاعتداء على التوقيع الإلكتروني، وتنعقد اختصاصاته عندمايمس ذلك الإجرام دولتين على الأقل من أعضاء الإتحاد الأوربي أو دولة عضو مع دولة من دول العالم الثالث أو دولة عضو من الرابطة الأوروبية وهي في ذلك غير مقتصرة على الأشخاص فقط إنما تشمل كذلك المؤسسات وتؤدي مؤسسة الأورجيست عملها بالتنسيق مع اليوروبول، حيث يزودها بالتحليلات اللازمة للقيام بالتحقيقات في الجزائر المنظمة وتتلخص نشاطاته في التنسيق والتعاون بين السلطات القضائية المختصة لدول الأطراف في جرائم الحاسب الآلي، كما يمكنه أن يطلب من الوكلاء العامين ذوي الاختصاص الوطني إجراء تحقيقات أو إجراء ملاحقات أو التبليغ عن الجرائم إلى السلطات المختصة للدول الأطراف.

خامسا: دور شرطة الانترنت في جرائم الاعتداء على التوقيع الإلكتروني

تعتمد شرطة الانترنت في عملها على قاعدة بيانات مركزية عملاقة يتم من خلالها بتسجيل كافة الحوادث والأنشطة الإجرامية التي تم الإبلاغ عنها [3] وهذا أمر طبيعي لأن استخدام الانترنت على نطاق واسع بمقتضي إنشاء شرطة الانترنت تكون مهمتها ملاحقة الانتهاكات والجرائم التي يستخدم فيها الانترنت ومنها جرائم الاعتداء على التوقيع الإلكتروني [4].

---

[1]- د ايمن رمضان محمد أحمد، مرجع سابق ص 426.

[2]- تم إنشاء الأورجيست في 28/ 2002/02 من قبل مجلس الإتحاد الأوربي، ولقد تم إنشاؤها بهدف تقوية مكافحة جميع أنواع الإجرام الخطير، وهي منظمة عن طريق الاتفاقية الأوروبية الموقعة في 1990/07/26 والتي تحدد ومهامها والمسماة باتفاقية ما سرحت، راجع في ذلك شريف سيكامل، الجريمة المنظمة في القانون، حلقة الأولى دار النهضة العربية 2001 ص 72.

[3]- ايمن عبد الحفيظ، مرجع سابق، ص 226.

[4]- محمود وهيب السيد، شبكة الانترنت ومزيد من التقدم الأمني، مجلة مركز البحوث الشرطة العدد 21- 1999 ص 291.

وتأتي الولايات المتحدة الأمريكية في مقدمة الدول التي واجهت الجرائم المعلوماتية بإنشاء إدارة متخصصة.

الفرع الثاني: مظاهر التعاون الدولي في مجال التدريب لمكافحة جرائم التوقيع الإلكتروني.

فرض التطورات العلمية والتكنولوجية المتلاحقة في مجال الحاسب الآلي والجرائم التي ترتكب في عالمه الافتراضي على أجهزة الأمن ضرورة تطوير برامجها التدريبية لمواجهة هذا التطور المذهل في تكنولوجيا المعلومات والذي ترتب عليه تطور كبير في نوع الجريمة ووسيلة ارتكابها، حيث تحولت الجريمة من جرائم ترتكب في الواقع المادي إلى جرائم ترتكب عبر شبكات ونظم المعلومات وباستخدام وسائل وأساليب أخرى مختلفة تماما عن تلك التي تستخدم في الجرائم التقليدية ومن ثم أصبحت الحاجة ملحة للتطوير وسائل وآليات المواجهة لهذه الجرائم وتطوير العنصر البشري المتدرب من خلال آليات وبرامج مدروسة.

بعناية وفق منهج محدد حيث يمكن تحقيق الهدف المرجو من العملية التدريبية في هذا المجال، وعلى ذلك يمكن تقسيم الدراسة في هذا الفرع إلى العناصر التالية:

أولا: أهمية التدريب في جرائم التوقيع الإلكتروني ومتطلباته

يقصد بتدريب رجال العدالة تلك العملية التي يخطف لها ونصمم لها البرامج ويبذل الجهد والمال لتغيير سلوك العاملين في أجهزة العدالة سواء أكانوا من القضاء أومن رجال التحقيق والدعاء العام إلى النيابة العامة أو من رجال الضبط القضائي أومن رجال السلطة العامة القائمين على تنفيذ القانون أو من الموظفين المعاونين لهذه الأجهزة كالخبراء وغيرهم أو من المهنيين الذين يشاركون في تحقيق العدالة كالمحامين، حيث تهدف هذه العملية التي تغيير سلوكهم ورفع مستوى مهاراتهم واتجاهاتهم، بما يكفل حسن إنجاز العمل القانوني والقضائي والتنفيذي مما ينعكس إيجابا على الارتقاء بكيفية أداء العدالة وتقديمها للمتقاضين بشكل يكفل إقامة التوازن بين المصلحة العامة من جهة والمصلحة الخاصة للأفرادمن ناحية أخرى، مما يجعل الناس يطمئنون إلى جدية وفاعلية سير العدالة فينبعث ذلك على الثقة وتحقيق الأمن للجميع [1].

ولو أمعنا النظر في بعض الاتفاقيات الدولية والإقليمية لوجدنا أنها دعت وبصريح النص إلى ضرورة وجود تعاون بين الدول في مجال التدريب ونقل الخبرات فيما بينها كما هو الحال في المادة 29 من اتفاقية

[1]- هلالي عبد الله أحمد، مرجع سابق، ص 371.

الأمم المتحدة الجريمة المنظمة عبر الوطنية 2000 م والمادة 9 من مشروع الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود، والتعاون الدولي في مجال تدريب رجال العدالة على مواجهة الجرائم المتعلقة بشبكة الانترنت قد يكون بين الدول وأجهزة العدالة الجزائية لديها فعلى الصعيد العربي نجد مثلا انه هناك اجتماعات ثم عقدها في إطار التنسيق بين المعاهد القضائية العربية لتوفير التدريب والتأهيل المناسبين لأعضاء الهيئات القضائية العربية [1].

أما عن متطلبات التدريب في مكافحة جرائم التوقيع الالكتروني فإنهايتطلبالتحقيق في جرائم التوقيع الإلكتروني توافر مهارات خاصة لا تتحقق دول تلقي لتدريب متخصص وتتضمن عملية التدريب عدة عناصر [2]

أ-المتدرب:

يستلزم تحقيق التدريب لأثاره ونتائجه آن يتوافر لدى المتدرب الصلاحية العلمية والقدرات الذهنية لتلقي التدريب، ويفضل في مجال التدريب على تحقيق جرائم التوقيع الإلكتروني تدريب المتخصصين في معالجة البيانات على تدريب القائمين على تنفيذ القانون مع رجال الشرطة: كما يستلزم أن تتوافر لدى المتخصص المتلقي للتدريب خبرة لا تقل عن خمس سنوات في مجال عمليات الحاسب والبرمجة وتصميم النظم وتحليلها، وإدارة المشروعات، أما بالنسبة للخبرة في معظم نظم الحاسبات فهي غير متطلبة وان كان توافرها لدى المتدرب مفصلا.

1- منهج الدورة التدريبية:

وهو من العناصر الأساسية في التدريب على تحقيق في جرائم التوقيع الإلكتروني ويلزم أن تتضمن الدورة المجالات الأساسية للمعرفة بعلوم الحاسب الآلي، ونقل الخبرات من المتخصصين في هذا المجال إلى المتدربين عن طريق المحاضرات والتطبيقات العملية في مختلف مجالات عمليات الحاسب الآلي [3] ففي جمهورية مصر العربية نجد أن وزارة الداخلية تعقد الكثير من الندوات والمؤتمرات وحلقات النقاش وتشارك فيها سواء عقدت داخل مصر أو خارجها، بإضافة أنه يتم إرسال ضباط الشرطة من مختلف الدرجات في برامج خارجية وذلك بالتعاون مع أجهزة الشرطة في الدول الأخرى والهيئات الدولية بهدف الإطلاع على أحداث النظم المقارنة وقد يتم من خلال عقد ندوات ومؤتمرات وورشات عمل جماعي

[1]- فهد عبد الله العبيد العازمي، مرجع سابق، ص 209

[2]- حسام محمد نبيل الشرافي، مرجع سابق.ص 766.

[3]- حسام محمد نبيل الشرافي، مرجع سابق. ص 766.

متخصصة في مواجهة تلك الجرائم تعقد على المستوى الدولي، وعلى المستوى الإقليمي، حيث تقدم هذه الفعاليات العلمية من أبحاثها ودراساتها وموضوعات محاورها الضوء على المستجدات المتعلقة بالجرائم المستحدثة من خلال تحليل ومناقشة أبعادها بعقلية ناجحة مما يمكن المعنيين بالوقاية والمكافحة بأساليب تتناسب وتفوق أساليب ووسائل مرتكبيها وعلى ضوء هذه المؤتمرات أو الندوات أو ورش العمل الجماعي تعقد اللقاءات وتتبادل الآراء والخبرات، وتعد هذه الصورة أكثر تطورا للتعاون الدولي الذي يستهدف تقريب وجهات النظر وتوحيد المفاهيم بين المشاركين في مكافحة الجريمة في الدول المختلفة من خلال تبادل الخبرة وطرح موضوعات ومشكلات والتعرف على أحداث التطورات في مجال الجريمة سيما جرائم التوقيع الإلكتروني وأساليب مكافحتها.[1]

يمكن إيجاز الموضوعات التي يلزم أن تتضمنها الدورات في الأتي:

المخاطر والتهديدات ونقاط الضعف التي قد يكون الحاسب معرضا لها

مفاهيم معالجة البيانات المتعلقة بالبرمجة والأجهزة.

أنواع الجرائم الناشئة عن الاعتداء على التوقيع الإلكتروني.

المنهج التحقيقي ويشمل إجراءات التحقيق، والتخطيط، تجميع المعلومات وتحقيقها، أساليب المواجهة والاستجواب، مراجعة النظم الفنية للبيانات أساليب العمل الجنائي وأساليب عرض ودراسة الحالات.

2- التدريب الرسمي وغير الرسمي :

إن التدريب على مكافحة جرائم التوقيع الإلكتروني يمكن أن يكون رسميا أو غير ذلك وبعد التدريب أثناء الوظيفة هو الوسيلة الرئيسة للتدريب غير الرسمي ويمكن أن يتلقى المحقق هذا النوع من التدريب بالعمل مع من له خبرة في التحقيق غير رسمي في جرائم التوقيع الالكتروني، أما الوسيلة الأخرى فهي تناوب العمل والتي يقوم المحقق فيها بقضاء بعض الوقت في كل قسم من أقسام معالجة البيانات والعمل مع المتخصصين في أمن شبكات معلوماتية لتوقيع الالكتروني أما التدريب الرسمي فيتم من خلال الحلقات الدراسية أي ما يسمى بورش العمل التي تنعقد حول جرائم التوقيع الإلكتروني، وهي الوسيلة يمكن أن تحقق أفضل نتائج في التدريب الرسمي [2] ويكفل تفاعل المشاركين وتتضمن تحليلا لحالات دراسية واكتساب خبرة عملية في علوم الحاسب والتحقيق في جرائم التوقيع الالكتروني وتفعيل التدريب والوصول

[1]- فهد عبد الله العبيد العازمي، مرجع سابق، ص 437.

[2]- حسام محمد نبيل الشراقي، مرجع سابق، ص 767.

للمستهدف هذه يجب أن يكون مستمرا وان يتضمن دورات في المحاسبة ومعالجة البيانات والمراجعة المحاسبة في نظم المعالجة الآلية للبيانات والتحقيق وأمن المعلومات [1]

3- أساليب التدريب:

يعد أسلوب الفريق هو أفضل أساليب التدريب على تحقيق جرائم التوقيع الإلكتروني ويقوم هذا الأسلوب على فلسفة إدارة المشروعات المتمثلة في الاستخدام الفعال لمجموعة من المتخصصين في مهمة واحدة، أو استخدام فريق متكامل بدلا من عدد المحققين ذوي المهارات المتماثلة ووفقا لهذا يتم التدريب مجموعة من المتخصصين مجالات متعددة فليلم كل منهم بتخصص آخر، ويزداد فهمه لتخصصه الأصلي مع تعميق هذا الفهم باكتساب مهارات التحقيق ويمكن تقسيمهم إلى ثلاثة أقسام هم: القائمون على تنفيذ القانون والمتخصصون في التدقيق والمراجعةالمحاسبية والمتخصصون في المراجعة الإلكترونية للبيانات وتتضمن وسائل تدريب المحققين موضوعين أساسيين:

تعليم متخصصين في العديد من فروع العلم للوصول إلى درجة من الاحتراف ومن الناحية العملية فإن المحاسب في فريق التحقيق بتعليم المزيد من المحاسبة والرياضيات.

1- عند بلوغ مستوى الاحتراف والبراعة في التحقيق نبدأ المرحلة الثانية من التعليم وتتضمن استخدام دراسات حالة متزايدة من التعقيد، وتنمكن هذه المرحلة أعضاء الفريق من التعرف على كيفية معالجة الأعضاء الآخرين في الفريق للمشكلة المشتركة كل من زاوية خلفيته وتخصصه، ومع التناوب الملائم للأعضاء في الفرق المختلفة سيتأقلم كل متخصص على العمل مع مجموعة من المتخصصين الآخرين بأسلوب الفريق.

4- جهة التدريب:

يلزم نجاح التدريب لمحققي جرائم التوقيع الالكتروني أن يتم إسناد مهمة إعداد وتنفيذ البرامج التدريبية إلى جهاز متخصص يعني باختيار المدربين الذين تتوافر لديهم الإمكانية الفنية والعلمية والخصائص والصفات الشخصية لتوالي التدريب في هذا المجال وإعدادهم إعدادا خاصا يؤهلهم للقيام بهذه المهمة.[2]

[1]- جميل عبد الباقي الصغير، مرجع سابق ص 126.

[2]- حسام محمد نبيل الشراقي، مرجع سابق ص 769.

ثانيا: أهمية التدريب في جرائم الاعتداء وكل التوقيع الإلكتروني

يعد التدريب جزءا هاما من منظومة مكافحة جرائم التوقيع الالكتروني ويستهدف في المقام الأول تحقيق الكفاءة في إنجاز العمل، لذا فقدت حصرت الأجهزة الألمانية المختلفة على الاهتمام به وذلك لكونه من أهم الوسائل التي تؤدي لرفع مستوى الإلمام بكيفية التعامل مع الأدلة ومعطيات مسرح الجريمة في جرائم التوقيع الالكتروني، كما أنه يعد الوسيلة الناجحة والفعالة والتطبيقية الناجحة التي تحقق الاستفادة من تجارب الآخرين باستخدام أفراد أمن مؤهلين وقادرين على نقل تلك الخبرات والمهارات بطريقة بسيطة وقابلة للفهم من المتلقين، كما أنه يعد الوسيلة الفعالةفي وضع الخبرات والعلوم النظرية موضع التطبيق العملي وهو ما يؤدي للتعرف على السلبيات والأخطاء في مجال التحقيق والتحري عن الجناة في جرائم التوقيع الالكتروني [1] ويجب أن يراعي في هذا التدريب العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب وتأهيل القائمين على جمع الاستدلالات والتحقيق الابتدائي سواء فيما يتعلق بالأساليب الفنية المستخدمة في ارتكاب الجريمة وكيفية معاينتها والتحفظ عليها وتدريب القضاة على معالجة هذا النوع من القضايا التي تحتاج إلى خبرات عالية حتى يتمكنوا من النهاية من الفصل في هذه القضايا وقد اتجهت بعض الدول مثل كندا سنة 1980 وفرنسا 1980 وفرنسا 1983 وانجلترا سنة 1987 وفنلندا سنة 1990 إلى إعطاء دورات تدريبية لجهات الضبط القضائي عن كيفية تحقيق في جرائم الإلكترونية.

كما ينظم البوليس الدولي Interpol دورات تدريبية في مجال الجرائم التوقيع الالكتروني من أجل تحسين أداء الأعضاء من رجال الشرطة في مجال الكشف عن الجريمة وجمع المعلومات ومتابعة الجناة وإقامة الدليل في هذه الجرائم إلا أن التدريب لا يقتصر على رجال الشرطة بل يجب أن يمتد أيضا ليشمل الخبراء القضائيين حيث تتوقف قدراتهم في البحث عن الدليل على تكوينهم الفني بهذه التقنيات [2] كما أن التقارير هم أهمية بالنسبة لقضاة الحكم الذي غالبا ما يعول عليها في المسائل الفنية البحتة وفد اتجهت في ذلك كل من إيطاليا وهولندا وفرنسا منذ 1986 إلى عقد دورات تدريبية لأعضاء النيابة وقضاة التحقيق والحكم والخبرات حول التحقيق في الجرائم المرتبطة بتكنولوجيا المعلومات [3].

[1]- المرجع نفسه، ص 765.

[2]Alan Davidson, the Law of électronic commerce, USA, 2009, p197.

[3]- جميل عبد الباقي الصغير، مرجع سابق، ص 127.

ثالثا: الاستفادة من أسلوب محاكاة الحاسب الآلي في مجال التدريب

يعد محاكاة الحاسب الآلي من أحدث الوسائل التي بدأ استخدامها في كشف الجرائم فيما يعرف بإعادة تمثيل مسرح الجريمة فهو يعرف بأنه عبارة التقليد المحكم الذي يطابق ويماثل الأصل تماما بحيث يتم التعايش مع ظروف وملابسات واحتمالات الواقع العقلي للمواقف والأحداث بصورة تزيد من القدرة على التعامل مع مثل هذه المواقف في الحياة العملية [1] كما عرفها باحث آخر بأنها قيام المحلل نموذج لما يريد دراسته يكون تمثيلا صادقا للواقع الموجود في النظام وتجريد لما فيه من مكونات وتفاصيل ثم يقوم بعدها بالتعامل مع النموذج بدلا من النظام [2]

أ- مميزات محاكاة الحاسب الآلي:

1- إمكانية نقل الظروف والملابسات الخاصة بالجرائم المختلفة التي تقع على التوقيع الإلكتروني لأجهزة الحاسب ما يفيد في دراستها والتوصل لأفضل الوسائل لتحقيقها خاصة مع صعوبة الإبقاء على العوامل والمتغيرات التي حدثت في الواقع لفترة حتى يمكن دراستها.

2- خلق بيئة الكترونية تحاكي الظروف الواقعية وملابساتها من شأنه إيجاد إمكانية لمعالجة الأخطاء واكتساب الخبرات والمهارات وإيجاد الأساليب للتعامل مع الجريمة وإيجاد الفرصة للمبتدئين من المحققين لتدريب على تحقيق ذلك الجرائم دون إتلاف الأدلة أو ضياع معالمها.

3- يعطي الفرصة لإعداد سيناريوهات متعددة لمواقف وأحداث يتم التنبؤ بها وفق المتغيرات وفي ضوء المستجدات بما يسير الوصول لأساليب معالجتها دون انتظار وقوعها بالعقل بما يحقق لمتخذي القرار القدرة على المبادرة وعدم الاعتماد على أسلوب رد الفعل.

4- قياس ردود الفعل لدى المتدربين على نماذج المحاكاة على نماذج المحاكاة وكذا متخذي القرار[3].

5- الاستعانة بالمحاكاة في تصوير أشكال الجرائم التي يمكن أن تقع على التوقيع الإلكتروني ونظم معلوماته وكيفية قيام الأجهزة الأمنية بالتعامل معا في ضوء الإمكانيات المتاحة والقدرة على اتخاذ القرار فيها والانتقال لمسرح الحادث.

---

[1]- محمد محمود درويش، التطلعات المستقبلية نحو استخدام أسلوب المحاكاة في مجال التدريب الأمني بأكاديمية الشرطة، مجلة الأمن العام المصرية عدد 46ص 51.

[2]-حسام محمد رمضان، تطبيقات المحاكاة الحاسوبية في التخطيط والتدريب على إدارة الكوارث، مجلة البحوث الأمينة، أكاديمية الملك فهد الأمينة، مجلد 11 عدد 22 أكتوبر 2002.

[3]- حسام محمد رمضان، مرجع سابق، ص 204.

ب-الاستفادة من أسلوب المحاكاة الحاسب الآلي في مجال جرائم التوقيع الإلكتروني:

يفيد استخدام محاكاة الحاسب الآلي أجهزة الأمن في إعداد برامج لتدريب أفراد على استخدام الحاسب الآلي والذكاء الاصطناعي والنصوص المبرمجة والتدريب عن طريق الانترنت لتوصل للجناة وتحديد عناصر الجرائم في حالات الاعتداء على التوقيع الالكتروني.

يتم الاستفادة من محاكاة الحاسب الآلي في تصميم نماذج للبيئات والمواقف الأمنية المتعددة في مجال البحث الجنائي من جرائم الاعتداء على التوقيع الإلكتروني بحيث يتم إعداد هذه النماذج بصورة تصاعدية لتنمية مهارات المختصين من رجال الضبط القضائي[1]، إعداد نماذج لأساليب ارتكاب جرائم الاعتداء على التوقيع الالكتروني ذات سيناريوهات زمانية ومكانية مع محاكاتها باستخدام الحاسب الآلي بهدف التعليم والتدريب الأمني واكتساب الخبرات في مواجهة والبحث والتحقيق الجنائي لوقاية من أخطار هذه الجرائم ومواجهتها.

يفيد استخدام أسلوب محاكاة الحاسب الآلي في توفير نماذج مشابهة لجرائم الاعتداء على التوقيع الالكتروني وهو ما يوفر لرجال الضبط القضائي الظروف المماثلة لمسرح الجريمة ويساعده على التدريب على التعامل مع هذه الجرائم في الواقع العقلي.

ضخامة التحديات الأمنية التي تواجه رجال الضبط القضائي تستلزم مواكبة التطور الحادث في جرائم التوقيع الالكتروني. وضرورة مواكبة المستجدات باستخدام وسائل أكثر تطور في التحقيق والبحث عن تلك الجرائم [2]

المطلب الثاني: التعاون القضائي الدولي لمكافحة في جرائم الاعتداء على التوقيع الالكتروني في مرحلتي التحقيق والمحاكمة

إن تعقب مرتكبي الاعتداء وعلى التوقيع الالكتروني للوصول لأدلة كافية لتقديمهم للمحاكمة الجنائية، يوجب أن تتعاون الدول فيما بينها ليس فقط على الصعيد الشرطي بل على الصعيد القضائي أيضا ولا سبيل لتحقيق هذا إلا بتفعيل وتعزيز المساعدة القضائية التي تأخذ شكل تفتيش الحاسب وتقديم البيانات فدول القائمة بالمحاكمة تحتاج إلى مساعدة السلطات الأجنبية المختصة [3] وتحتوي

[1]- محمد مدحت المراسي، أوجه الاستفادة من المعطيات العلمية والتكنولوجية المعاصرة في مجال تطوير برامج تأهيل رجال الشرطة، مجلة مركز بحوث الشرطة، أكاديمية الشرطة عدد 22 سنة 2002 ص 127.

[2]- حسام محمد نبيل الشراقي، مرجع سابق، ص 781.

[3]- ايمن رمضان محمد أحمد، مرجع سابق ، ص432.

العديد من الاتفاقيات الدولية والقوانين الجنائية الداخلية نصوص تشجع عل المساعدة القضائية بين الدول وتتخذ المساعدة القضائية في جرائم الاعتداء على التوقيع الالكتروني صور متعددة تتعلق يحفظ البيانات والقدرة على النفاذ إلى البيانات المخزنة واعتراض البيانات وفي ضوء ذلك سنتناول المساعدة القضائية الدولي في مجال الكشف عن جرائم التوقيع الالكتروني من خلال الفروع التالية.

الفرع الأول: المساعدة القضائية الدولية في مجال الكشف عن جرائم الاعتداء على التوقيع الالكتروني

الانترنت ماهي الشبكة عالمية تمتاز بأنها دولية وإنها عابرة للحدود وبالتالي فان جرائم التوقيع الالكتروني المتصلة بها تعتبر هي الأخرى عالمية ذات طابع دولي وأثرها يمتد لأكثر من دولة مما دفع الدول إلى التعاون فيما بينها للقضاء على هذه الظاهرة الإجرامية.

أولا: مفهوم المساعدة القضائية الدولية في مجال الكشف عن جرائم الاعتداء على التوقيع الالكتروني

يمكن تعريف المساعدة القضائية الدولية بأنها كل إجراء قضائي تقوم به دولة من شانه تسهيل مهمة المحاكمة في دولة أخرى يصدد جريمة من الجرائم [1]، حيث تعتبر المساعدة القضائية الدولية فعالة في مكافحة جرائم التوقيع الالكتروني على اعتبار أنها عابرة للحدود لا تستطيع دولة مكافحتها لوحدها.

وترتيبا لذلك نصت العديد من الاتفاقية على المساعدة القضائية حيث ركزت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود والوطنية المعتمدة من طرف الجمعية العامية الجمعية العامة المنظمة للأمم المتحدة بتاريخ 2000/11/15 في المادة 18 على المساعدة القانونية المتبادلة وفي المادة 19 على التحقيقات المشتركة بين الدول وفي المادة 20 على أساليب التحري الخاصة لهذا النوع من الجرائم [2]

-كما نصت المادة 27 من اتفاقية بودابيست شان جرائم الحاسب الآلي على أهمية المساعدة القضائية في بعض الإجراءات دون حاجة أن تكون الدولة طرفا في تلك المعاهدة أو اتفاق بشأن هذه المساعدة وترتيبا على ذلك، يحق للدولة التقدم بطلبات طارئة للتعاون من خلال وسائل سريعة للتوصل عوضا عن اللجوء إلى الوسائل التقليدية والبطيئة القائمة على نقل الوثائق الخطية والمختومة، عن طريق القنوات الدبلوماسية، أو أنظمة إرسال البريد ومتى ارتكبت جرائم الاعتداء على التوقيع الالكتروني من خلال أكثر من دولة فانه يلزم عملا ينهى المادة 18 من اتفاقية باليرمو للجريمة المنظمة عبر الوطنية 2000

[1]- خالد ممدوح إبراهيم، مرجع سابق ، ص407.

[2]- يزيد بوحليط، مرجع سابق ، ص509.

على دول الأطراف أن تقدم كل منها للأخرى المساعدة القانونية المتبادلة في التحقيقات والملاحقات والإجراءات القضائية فيما يتصل بالجرائم المشمولة بهذه الاتفاقية حسبما تنص المادة 3 ويتعين عليها أنتمد كل منها الأخرى تبادليا المساعدة القضائية المطلوبة سيما إذا كان لدى الدولة الطالبة دوافع معقولة للاشتباه في أن الجرم المشار إليه في الفقرة أ أو ب من المادة 2 ذو طابع دولي [1]

كما حرصت المادة 26 من اتفاقية بودابيست على التأكيد على واجب الدولة التي تمتلك الدعاوى الجنائية في الحالات التي لا يدرك فيها الفريق الذي يجري التحقيقات والملاحقة وجود هذه المعلومات في هذه الحالة، لا يقدم أي طلب بالمساعدة المتبادلة وذات الصورة نجدها في المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي الصادر مجلس التعاون الخليجي [2]

ثانيا: بيانات طلب المساعدة القضائية

يتضمن طلب المساعدة القضائية السلطة مقدمة الطلب وكذا موضوع وطبيعة التحقيق أو الملاحقة أوالإجراء القضائي الذي يتعلق به الطلب، واسم وظائف السلطة التي تتولى التحقيق أو الملاحقة أوالإجراء القضائي وملخصها للوقائع ذات الصلة بالموضوع باستثناء ما يتعلق بطلبات المقدمة لغرض تبليغ مستندات قضائية وصف للمساعدة الملتمسة وتفاصيل أي إجراءات معينة تود الدولة الطرف الطالبة إتباعها وهوية أي شخص معني ومكانه وجنسية حيثما أمكن ذلك والغرض الذي تلتمس من اجله الأدلة أو المعلومات أو التدابير، تعدم الطلبات كتابة أو حيث ما أمكن، بأي وسيلة كفيلة بان تنتج سجلا مكتوبا، بلغة مقبولة لدى الدولة الطرف متلقيه الطلب وفي ظروف تتيح لتلك الدولة الطرف أن تتحقق من صحته، ويتعين إبلاغ الأمين العام للأمم المتحدة باللغة المقبولة لدى الدولة الطرف وقت قيام كل دولة طرف بإيداع صك تصديقها على هذه الاتفاقية أو قبولها أو إقرارها أو الانضمام إليها[3]أما في الحالات العادلة وحيثما تتفق الدولتان الطرفان على ذلك، فيجوز أن تقدم الطلبات شفويا، على أن تؤكد الكتابة على الفور [4]

وفي هذا الصدد نجد أن المشرع الجزائري قد وفق كثير في تسهيل قبول طلبات المساعدة القضائية باعتماد الطلب حتى وان جاء عبر وسائل تكنولوجيات الإعلام والاتصال الحديثة يشترط التأكد من

[1]- فهد عبد الله العبيد العازمي، مرجع سابق ، ص489.

[2]- اعتمد هذا النموذج من المجلس الأعلى لمجلس التعاون الخليجي في دورته الرابعة والتي انعقدت بدولة الكويت في الفترة من 2003/12/22/21 م، وكذا أصدرت اتفاقية الرياض، مملكة العربية السعودية في 1933/3/6.

[3]- هلالي عبد الله أحمد، مرجع سابق ص253

[4]- راجع في ذلك، نص اتفاقية الأمم المتحدة المكافحة الفساد (un) لتعاون الدولي، مادة 46 فقرة 21.

صحته وهذا بسبب السرعة المتطلبة لبحث والتحري الإلكترونية ذات الطبيعة الخاصة وملاحظة المجرم الإلكتروني ضمان إفلاته من العقاب [1]

وهذا ما يمكن سلطات البحث والتحري الجزائرية بالتعاون مع السلطات الألمانية ويتعاون الولايات المتحدة الأمريكية بالجزائر ومكتب الانتربول،Interpol، فرع بالجزائر من القبض على الرأس الشبكة الإجرامية المختصة في القرصنة الالكترونية، حيث قام هذا الشخص وهو من مدينة عناية باختراق قاعدة بيانات متواجدة بمدينة ميونيخ بألمانيا وقام بتحميل البيانات الرقمية الخاصة ب1500 بطاقة ائتمان باستعمال عنوان الكتروني Adressip مما مكنه من تحويل ما قيمته 100.000 دولار منذ 2005 من حسابات زبائن البنك الكندي، حيث أدانت محكمته عناية قسم الجنحالجاني بجنحة تصميم وإدخال عن طريق الغش لمعطيات المنظومة المعلوماتية وكذا جنحة التقليد ومعاقبة عام حسيا نافذا وغرامة قدرها 500.000 دج طبقا لنصوص المواد 394مكرر 1-394 مكرر2 من ق-ع-ج والمواد 151-152 و153 من القانون رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة [2]

ثالثا: القيود الواردة على طلبات المساعدة القضائية الدولية:

إن اللجوء إلى المساعدة القضائية الدولية ليست مطلقة وفق المشرع الجزائري،حيث نصت المادة 18 من القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على يرفض تنفيذ طلبات المساعدة إذا كان من شانها المساس بالسيادة الوطنية أو النظام العام، يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب

وعليه يتم رف طلبات المساعدة القضائية في الحالات الآتية:

- إذا كان فيها مساس بالسيادة الوطنية
- إذا كانت ماسه بالنظام العام.
- كما يمكن الاستجابة لطلبات المساعدة القضائية وذلك بشروط:
- المحافظة على سرية المعلومات المبلغة لتلك الدولة.

[1]- المادة 36 من الأمر رقم 05-06 المؤرخ في 23 /2005/8 يتعلق بمكافحة التهريب تحت عنوان " التعاون العملياتي " على مع مراعاة مبدأ المعاملة بالمثل وفي إطار الاتفاقيات الثنائية ذات الصلة، توجه طلبات المساعدة في مجال محاربة التهريب الصادرة عن السلطات الأجنبية كتابيا، أو بالطريقة الالكترونية إلى الجهات المختصة وتكون مصحوبة بكل المعلومات الضرورية، إذا كان وجه الطلب الكترونيا يمكن تأكيده بواسطة أي وسيلة تترك أثرا مكتوبا.

[2]- انظر الحكم رقم 10/077357 الصادر عن محكمته عناية قسم الجنح بتاريخ 2010/6/28

- عدم استعمال المعلومات في غير الحالة الموضحة في طلب المساعدة القضائية

وهذا يسبب حساسية وامن المعطيات والبيانات التي قد تحتويها منظومة معلوماتية سواء ما تعلق بأمن الدولة لو الأشخاص، تجنب المشكلات التي تثار بين الدول في هذا مثل التجسس بكافة أشكاله.... الخ لذا ألزمت الاتفاقية الدولية الموضوعية للتوقيع الأمم المتحدة في نيويورك في 2005/09/14 والخاصة.يقمع أعمال الإرهاب النووي للأطراف وفق نص المادة 2/07 منها باتخاذ التدابير لحماية سرية المعلومات التي يحصل عليها سرا بموجب هذه الاتفاقية من دولة أخرى [1] كما نجد أناتفاقية الأمم المتحدة لمكافحة un التعاون الدولي في المادة 46 الفقرة 21 نصت كذلك على الحالات التي يجوز فيها رفض تقديم المساعدة القضائية المتبادلة وهي كالآتي:

- إذارأت الدولة الطرف متلقية الطلب أن تنفيذ الطلب قد يمس بسيادتها وأمنها ونظامها العام أو معالجها الأساسية الأخرى
- إذا كان القانون الداخلي للدولة الطرف متلقية الطلب يحظر على سلطاتها تنفيذ الإجراء المطلوب بشأن أي جرم مماثل
- لو كان ذلك الجرم خاضعا لتحقيق أو ملاحقة أو إجراءات قضائية في إطار ولايتها القضائية
- إذا كانت تلبية الطلب تتعارض مع النظام القانوني للدولة الطرق متلقية الطلب فيما يتعلق بالمساعدة القانونية المتبادلة
- كما لا يجوز للدول الأطراف أن ترفض طلب مساعدة قانونية متبادلة لمجرد أن الجرم يعتبر أيضا متصلا بأمور مالية ويتعين إبداء الباب الرفض [2] كما يجوز لدولة الطرف متلقية الطلب أن ترجئ المساعدة القانونية المتبادلة بسبب تعارضها مع تحقيقاتأو ملاحقات أو إجراءات قضائية جارية [3]

كما نصت المادة 26 من ذات الاتفاقية على أن قبل رفض أي طلب بمقتضى الفقرة 21 من هذه المادة أوإجراء تنفيذه بمقتضى الفقرة 25 من هذه المادة، نتشاور الدولة الطرف متلقية الطلب مع الدولة الطرف الطالبة للنظر في إمكانية تقديم المساعدة رهنا بما تراه ضروريا من شروطوأحكام، فإذا قبلت الدولة الطرف الطالبة تلك المساعدة مرهونة بتلك الشروط وجب عليها الامتثال لتلك الشروط [4]

[1] - المرسوم الرئاسي رقم 10-270 المؤرخ في 2010/11/10 يتضمن التصديق يتحفظ على الاتفاقية الدولة لقمع أعمال الإرهاب المقترحة للتوقيع في مقر الأمم المتحدة في نيويورك في 14 /2005/9 ج رقم 68 المؤرخة في 2010/11/10 ، ص6

[2] - راجع في ذلك نص اتفاقية الأمم المتحدة لمكافحة لفساد (un) التعاون الدولي المادة 46 الفقرة 23.

[3] - راجع في ذلك نص اتفاقية الأمم المتحدة لمكافحة الفساد (un) التعاون الدولي مادة 46 الفقرة 26.

[4] - نص الاتفاقية الأمم المتحدة لمكافحة فساد (un) مادة 26.

الفرع الثاني: صور المساعدة القضائية الدولية في جرائم الاعتداء على التوقيع الالكتروني

تتخذ المساعدة القضائية في جرائم الاعتداء على التوقيع الالكتروني صورا متعددة تتعلق بتبادل المعلومات وكذا نقل الإجراءات وإنابته القضائية كما هناك صور أخرى تتعلق بمساعدة القضائية في مجال حفظ البيانات وقدرة على النفاذ إلى البيانات المخزنة ومساعدة في مجال اعتراض البيانات الخاصة بمحتوى التوقيع الالكتروني.

أولا:تبادل المعلومات في جرائم الاعتداء على التوقيع الالكتروني

عرف العصر الحالي ثورة في مجال المعلومات مما حتم على المجتمع الدولي أن يولي لتبادل المعلومات أهمية قصوي باعتباره من انجح الوسائل لمكافحة الإجرام عموما، والجريمة الالكترونية خصوصا لما توفره المعلومات الصحيحة والموثوقة من تسهيل ومساندة الأجهزة في مجال متابعة النشاطات الإجرامية وكشف عن المجرمين

فتبادل المعلومات يشمل [1] تقديم المعلومات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية بصدد جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، وهناك مظهر آخر لتبادل المعلومات يتعلق بالسوابق القضائية للاجئناه[2] من خلالها تتعرف الجهات القضائية بدقة على الماضي الجنائي passé pénalللفرد المحال إليها والتي تساعد في تشديد العقوبة في حالة العود، أو في وقف تنفيذها، إلاأن تدوين الصحيفة الجنائية casien judicaireمازال في مرحلة الأولى، ففرنسا مثلا لا تسمح بإعطاء صور ضوئية من صحف الحالة الجنائية إلا عن رعايا الدول التي تربط بها اتفاقيات تبادل المعلومات كل ذلك يتم [3] من خلال تعزيز الاتصال بين سلطات الدول وأجهزتها ودوائرها المختصة بمكافحة الجرائم الالكترونية، ويعتبر إنشاء مثل تلك القنوات ضرورة وذلك من اجل تسيير تبادل المعلومات بصورة مأمونة وسريعة بشان كل ما يتعلق بتلك الجرائم مثل

-هوية الأشخاص المشتبه فيهم في تلك الجرائم وأماكن وجودهم وأنشطتهمأوأماكن الأشخاص الآخرين المعنيين

-حركة عائدات الجرائم أو الممتلكات المتأتية من ارتكاب تلك الجرائم

[1]- جميل عبيد الباقي صغير،مرجع سابق.ص 91.

[2] - المادة 5 من اتفاقية الرياض العربية للتعاون القضائي 1983.

[3]- محمد كمال محمود الدوسقي، مرجع سابق ، ص148.

-تبادل المعلومات عبر الوسائل والأساليب المحددة التي تستخدمها الجماعات الإجرامية لارتكاب جرائمها ووسائل وأساليب إخفاء أنشطتها.

-كما يمكن أن تقوم الجهة المختصة في دولة ما بإرسال إلى الجهة المختصة لدى دولة أخرى وهي يصدد النظر في الجريمة ما بيانات عن الأحكام القضائية النهائية الصادرة ضد مواطني الأخيرة أوالأشخاص المولودين أو المقيمين في إقليمها والإجراءات التي اتخذت ضدهم والمفيدة في محق الحالة الجنائية لدولة المرسلة ووفقا للمبادئ العامة للتعاون الدولي القسم من فصل 3 من اتفاقيته مجلس أوروبا حول الجريمة الالكترونية " يتعين على دول الأطراف التعاون بشكل موسع وتذليل العقبات التي تعترض التدفق السريع للمعلومات والأدلة [1]

كما حرصت المادة 26من اتفاقية بودابست على التأكيد على واجب الدولة التي تمتلك معلومات هامة مساعدة دولة أخرى في معرض التحقيقاتأو تداول الدعاوى الجنائية أو الملاحقة وجود هذه المعلومات، في هذه الحالة، لا يقدم أي طلب بالمساعدة المتبادلة [2]

ولهذه الصورة من صور المساعدة القضائية الدولية صدى كبيرا في كثيرا من الاتفاقيات كالبند و" والبند ز" من الفقرة الثانية من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية [3]

كما وتنص المادة 66 من قانون رومانيا رقم 2004/203 على حق السلطات الرومانية المختصة في أن ترسل تلقائيا إلى السلطات الأجنبية المختصة المعلومات والبيانات الضرورية التي تسمح لهذه الأخيرة باكتشاف الجرائم المرتبكة بواسطته جهاز الحاسوب أو يحل القضايا المتعلقة بتلك الجرائم [4]، فيجب التنسيق بين الدول المختلفة والمعينة بشأن إجراءات التحقيق في الجرائم الدولية الخاصة بتكنولوجيا الحديثة ومنها جرائم الاعتداء علىالتوقيع الالكتروني بغض النظر عن مكان وقوع الضرر وذلك عن طريق وسائل المعونة المتبادلة السابق ذكرها [5]

[1]- إيهاب محمد يوسف، مرجع سابق ص 23.

[2]- فهد عبد الله العبيد العازمي، مرجع سابق ، ص490.

[3]- صدرت هذه المعاهدة في 1990/12/14 في الجلسة 28 للجمعية العامة للأمم المتحدة وتقتضي باتفاق أطرافها على ان يقدم كل منهم للآخر كبير قدر ممكن من المساعدة المتبادلة في التحقيقات أو الإجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخل في اختصاص السلطة القضائية في الدولة الطالبة للمساعدة

[4]- ART66OF ROMAINIA LAW NO 161.2003.

[5] -Lamy AlainBensausan, Intervention au colloque de la CREDA, organisé le 13 mai 1998 sur le thème commerce électroniques avenir des circuits : de l'expérience des USA aux perspectives français, 1998. P532.

ونظرا لما تثيره مسالة المساعدة القضائية بين الدول من حساسيته متعلقة بسيادة الدولة من جهة ومن جهة أخرى بطبيعة جرائم الحاسوب والانترنت التي يمكن من خلالها الحصول على معلومات تتعلق بأمن الأفراد والدولة على حد سواء وضع المشرع الجزائري شروطا لمساعدة القضائية ترد منه نص المادة 17 من قانون رقم 09 -04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلامأو الاتصال ومكافحتها التي تنص على تتم الاستجابة إلى طلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظيه وفقا للاتفاقيات لدولته ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل هذا وما جاءت به أيضا المادة 4 من نفس القانون على تلتزم كل دولة طرف وقفا لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى فقد وضع المشرع الجزائر هذه الشروط طبقا لمبدأ المعاملة بالمثل واحتراما للسيادة الوطنية وأيضا حمايته الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي نظرا لما تمثله هذه المعلومات من خطورة على سلامة الشخص ولا وعلى من الدولة ثانيا [1] ومن التطبيقات العملية لإمكانية الاستعانة شهود من دولة أخرى أو الاستعانة بخبرائها في التحقيقات التعاون في قضية "exe" حيث كان ضابط من بريطانيا هو الشاهد الرئيسي، وتم الاستعانة بآخر الخبراء من بريطانيا الذي انتقل للإقامة في روسا لمدة شهور.

ثانيا: نقل الإجراءات في جرائم الاعتداء على التوقيع الالكتروني

ويقصد به قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توافرت شروط معنية [2] من أهمها التجريم المزدوج يقصد به أن يكون العقل المنسوب إلى الشخص بشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة.

وقد نصت الاتفاقية الأوروبية للمساعدة المتبادلة في القضايا الجنائية على أن الدولة المطلوب إلي يجب أنتنقط وفقا للنمط المنصوص عليه في قانونها الداخلي أية رسائل تتعلق بالقضايا الجنائية والموجهة إليهامن السلطات القضائية للدول الطالبة لأغراض الحصول على شهادة أوإرسال أشياء أو مواد

---

[1]- يزيدبوحليط، مرجع سابق، ص 516- 517

[2]- سالم محمد سليمان الاوحلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية دراسة مقارنة، رسالة دكتورة – جامعة عين شمس، مصر، 1998 ص428.

لتقديمها كدليل أو محاضر رسمية أو وثائق قضائية [1] ويتعين أن تتسم إجراءات المساعدة بالسرية والأمان وذلك لتأكد من إن الاستعمال قاصر فقط على الجريمة محل المساعدة وحتى لا يتم نقل المعلومات إلىأشخاص غير القائمين على إنفاذ القانون لدى سلطات التحقيق التي قدمت الطلب[2]

غير أن الاعتماد على الآليات التقليدية للتعاون عند تقديم الطلب بطريق الدبلوماسي تجعلها لتتسم بالبطيء وهو ما يتعارض مع طبيعة جرائم الاعتداء على التوقيع الالكتروني، وتطبيقا لذلك، أبرمت اتفاقيات جديدة لتقصير الوقت واختصار الإجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق مثل الاتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفويا في حالة الاستعجال، على أن يتم تأكيد هذا التبادل كتابة بعد ذلك كما حث المجلس الأوروبي لدول الأعضاء على تسيير اتخاذ الإجراءات وإنشاء نظام الربط بين السلطة القضائية والسلطات الأجنبية بهدف الحصول على الأدلة على وجه السرعة، الأمر الذي يقتضي الترخيص لسلطات الدول المطلوب إليهاأن تقدم المساعدة من خلال التفتيش في النظام المعلوماتي وتضبط البيانات المواد إرسالهاإلى الدولة الطالبة فقد تعاونت المباحث الفيدرالية الأمريكية والبوليس الإنجليزي في الكشف عن أول حادث اختراق في مقاطعة ويلز في بريطانيا في مارس 2000 والقبض على المحترف[3]

ثالثا:الإنابة القضائية الدولية في جرائم الاعتداء على التوقيع الالكتروني

يقصد بالإنابة القضائية "طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها للقيام من إقليمها نيابة عنها بأيإجراء قضائي متعلق بدعوى ناشئة عن جريمة دولية معلوماتية، للفصل في مسالة معروضة على السلطة القضائية في الدولة الطالبة ويقذر عليها القيام به بنفسها"[4] كما يمكن تعريف الإنابة القضائية الدولية بأنها كل إجراء قضائي تقوم به دولة من شانها تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم [5].

فالإنابة القضائية تسهل إذن الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارستها بعض الإعمال القضائية داخل أقاليم الدول الأخرى، كسماع الشهود أوإجراء تفتيش والمعاينات وتبليغ

[1]- فهد عبد الله العبيد العازمي، مرجع سابق 492.

[2]- هلالي عبد الله محمد، مرجع سابق ، ص287.

[3]- أيمن رمضان محمد أحمد، مرجع سابق.ص446.

[4]- حازم الحارون " الإنابة القضائية الدولية المجلة الجنائية القومية، القاهرة، دورة ثالثة، ص 20 وعبد الرءوف مهدي " شرح القواعد العامة الإجراءات جنائية، دار النهضة العربية 2000، ص 102.

[5]- جميل عبد الباقي الصغير، مرجع سابق ، ص 83.

الوثائق القضائية وتنفيذ عمليات التفتيش والحجز، وغيرها [1] وتستلزم أيضا إرسال الملفات الخاصة بالدعوى الجنائية بمرفقاته محاضر جمع الاستدلالات والتحقيق والمستندات التي أجريت بمعرفة السلطة القضائية في الدولة الطالبة الإنابةإلى السلطة القضائية في الدولة المطلوب منها اتخاذ بعض إجراءات التحقيق.

وتجد الإنابة القضائية، أساسها في القوانين الوطنية وفي الاتفاقات الدولية فقد حرصت الأمم المتحدة لمكافحة الجريمة الالكترونية المنظمة عبر الوطنية على نقل الإجراءات الجنائية الإنابة القضائية فنصت المادة 21 على انه " يتعين على دول الأطراف أن تنظر في إمكانية أن تنقل أحداهاإلى الأخرى إجراءات الملاحقة المتعلقة يجرم مشمول بهذه الاتفاقية في الحالات التي يعتبر فيها ذلك النقل في صالح التيسير السليم للعدالة وخصوصا عندما يتعلق الأمر بعدة ولايات قضائية وذلك بهدف تركيز الملاحقة ومن بين الاتفاقيات التي أبرمت في مجال الإنابة القضائية، تلك التي أبرمت بين فرنسا والجزائر سنة 1962 ومع ألمانيا فسنة 1984 ومع مصر سنة 1982 والاتفاقية الأوروبية للتعاون القضائي في المواد الجنائية لسنة 1962 [2]

ففي فرنسا تسلم الإنابة القضائية بالطريق الدبلوماسي par la voie diplomatiqueويتم توجيهها إلى وزارة العدل، حسب الإجراءات المنصوص عليها بالنسبة لطلبات تسليم المجرمين، فبالسنة للاتفاقية الأوروبية للتعاون القضائي يتم تبادل الإنابة القضائية بين وزارات العدل مباشرة، وفي حالة الاستعجال " urgent" يمكن إرسالها مباشرة من الدولة الطالبة "requise"، وقد يتم التسليم بواسطة الانتربول وفضلا عن ذلك فان وزير العدل منوط به تقدير ما إذا كانت المهمة يجب تنفيذها من عدمه بالنظر إلىأحكام القانون الداخلي [3]

وتجد الإشارة كذلك إلى الجهود المبذولة من قبل جمهورية مصر العربية حيث أبرمت عدة اتفاقيات منها الاتفاقية المبرمة مع الكويت 1988 " التي قضت المادة الثانية منها " يكون الإجراء القضائي الذي يتم بطريق الإنابة القضائية وفقا لأحكام الأثر القانوني ذاته الذي يكون له فيما له تم أمام الجهة المختصة في الدولة الطالبة وعادة يتم إرسال طلب الإنابة القضائية عبر الطرق الدبلوماسية [4]

[1]- فهد عبد الله العبيد العازمي، مرجع سابق، ص494.

[2]- فهد عبد الله العبيد العازمي،المرجع السابق ، ص497 ، 498.

[3]- جميل عبد الباقي الصغير، مرجع سابق ، ص 98.

[4]- فهد عبد الله العبيد العازمي، مرجع سابق، ص496

وكذلك الاتفاقية المبرمة بين دول الجامعة العربية سنة 1953 ووافقت عليها مصر بالقانون رقم 30 لفنية 1954 والاتفاقية الخاصة بالتعاون القضائي في المواد الجنائية مع المملكة المغربية سنة 1989 واتفاقية التعاون القضائي مع البحرين 1989[1]

أن إجراءات التعاون القضائي الجنائي بالطريق الدبلوماسي يجعلها تتم بالبطيء وكثرة الشكليات وهو ما يتنافى والطبيعة الخاصة المتعلقة بالتوقيع الالكتروني نظرا لان عمل السرعة يعتبر من العوامل الرئيسية والهامة في مكافحة الجرائم المتعلقة بالتوقيع الالكتروني نظرا لان عامل السرعة يعتبر من العوامل الرئيسية والهامة في مكافحة الجرائم المتعلقة بالتوقيع الالكتروني لكون غالبية هذه الاتفاقيات صدرت في وقت لم تكن شبكة الانترنت فقد ظهرت أو كانت موجودة ولكنها محدودة.

ان تعديل هذه الاتفاقيات التقليدية للتعاون القضائي الدولي أصبح ضرورة ملحة خاصة مع التطور الكبير في تكنولوجيا المعلومات والاتصالات، ولأجل ذلك أبرمت العديد من الاتفاقيات الجديدة التي ساهمت في تقصير الوقت واختصار الإجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق، مثال ذلك الاتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفويا في حالة الاستعجال ونفس الشيء نجده في البند الثاني من المادة 30 من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999 والمادة 15 من اتفاقية الرياض العربية للتعاون القضائي 1983م والمادة 53 من اتفاقية شنجن 1990 والخاصة باستخدام الاتصالات المباشرة بين السلطات القضائية في دول الأطراف، والفقرة 13 من المادة 46 من اتفاقية الأمم المتحدة لمكافحة

رابعا:حفظ البيانات المخزنة في نطاق المساعدة القضائية

تتخذ المساعدة القضائية في جرائم الاعتداء على التوقيع الالكتروني صورا متعددة تتعلق يحفظ البيانات والقدرة على النفاذ إلى البيانات المخزنة وإمكانية الوصول العابر للحدود لتلك البيانات وهو ما سنتناوله على النحو التالي:

أ- حفظ البيانات المخزنة في أجهزة الحاسب الآلي

يعتبر الحفظ العاجل لبيانات المخزنة في أجهزة الحاسب الآلي آلية تقنية بالغة الأهمية على المستوى الدولي، حيث لحق لأي دولة المطالبة بحفظ البيانات المخزنة في أجهزة الحاسب الآلي الموجودة في أراضي

[1]- سليمان أحمد فضل، مرجع سابق، ص426.

الدولة المطلوب إليها على وجه السرعة للدول دون تغيير أو إزالة أو محو، بيانات المستند الالكتروني، خلال الفترة الضرورية لتنفيذ طلب المساعدة المتبادلة من اجل الحصول على البيانات [1]

وقد تناولت هذا الإجراء المادة 29 من اتفاقية بودابست المتعلقة بالجريمة الالكترونية والتي تنص على انه، يجوز لأي طرف أن يطالب طرف آخر أن يأمر أو بالأحرى ليحفظعلى بيانات مخزنة، بواسطة نظام كمبيوتر يقع داخل إقليم ذلك الطرف الآخر والتي ستأخذها ينوي الطرف الطالب تقديم طلب بالمساعدة المتبادلة من اجل البحث أو الدخول على أو مصادرة أو تامين أو كشف هذه البيانات [2]

كما وقد حددت هذه الاتفاقية الفترة اللازمة للتحفظ على البيانات " على انه يجب على كل دولية التأكد من إن البيانات المحفوظة ستحجز لمدة 60 يوما على الأقل وإذا يتبين لسلطات الدولية المطلوب إليهاأن حفظ البيانات قد يتخذ إجراءات من شانها تهديد السرية آو عرقلة التحقيق الذي تجريه الدولة الطالبة فعليها أن تبلغها بذلك، على وجه ومن مميزات هذا الإجراء انه سريع ويكفل حماية سرية البيانات التي تهم الشخص المعني [3]

والمساعدة المتبادلة في التحفظ العاجل على البيانات المخزنة في النظام المعلوماتي المنصوص عليه في المادة السابقة هو أمر ضروري تستلزمه طبيعة الأدلة في الجرائم الالكترونية وذلك لتفادي أي تغيير في هذه الأدلة أو نقلها أوإتلافها ومحو أثار الجريمة وهو إجراء ذو طبيعة وقتية لتدخل بطريقة سريعة .

بمجرد تنفيذ التماس أو طلب المساعدة المتبادلة كما يتسم هذا الإجراءبأنه ليس فيه مساس بسرية المعلومات والبيانات محل الإجراء لوقتي موضوع الطلب غير أن اللجوء إلى هذا الإجراء ليس مطلقا وإنما يتقيد هام نصت عليه المادة 31 من اتفاقية بودابست وهو أن يوجد سبب للاعتقاد بان البيانات ذات الصلة قد تتعرض للعقد أو التعديل حتى تلتزم الدولة بحفظ تلك البيانات أو الإفصاح عنها، ولذلك حثت الاتفاقية الأوروبية في شان جرائم الانترنت، الدول أطرافأن تطلب من بعضها المساعدة القضائية في مجال التحقيقات باستعمال وسائل سرعته في حالات الاستعجال مثل الفاكس بشرط ضمان سلامة المعلومات المتبادلة من الطرفين بما فيها استعمال وسائل التشفير عند الضرورة ذلك يطلب رسمي لاحق [4]

[1]- فهد عبد الله عبيد العازمي، مرجع سابق، ص 430.

[2]- يقابل هذه المادة، المادة السابعة وثلاثون من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010

[3]- ايمن رمضان محمد أحمد، مرجع سابق، ص 437.

[4]- المرجع نفسه، ص 438.

ب: المساعدة المتبادلة فيما يتعلق بجمع البيانات المارة في القوت الحقيقي

في الكثير من الحالات، يتعذر على المحققين في جرائم الاعتداء على التوقع الالكتروني تعقب اتصال ما، وصولا إلى مصدره عبر متابعة سجلات عمليات البث السابقة، إذ لا يستعبد إقدام مورد الخدمات على محو البيانات المارة الأساسية تلقائيا ضمن سلسلة البث قبل التمكن من حفظها [1] وبالتالي لابد أن يتمتع المحققون التابعون لكل دولة بالقدرة على الحصول على البيانات المارة في القوت الحقيقي فيما يتعلق بالاتصالات المارة عمر احد أجهزة الحاسوب لدى الدول الأخرى.

لذلك فقد نصت المادة 33 من اتفاقية بودابست " يجب على الأطراف أن تقدم المساعدة المتبادلة إلى بعضها البعض بالنسبة لجمع بيانات المرور في القوت العقلي والتي تكون مرتبطة باتصالات معينة على أرضهم ومرسلة عن طريق نظام معلوماتي على أن يجري هذا التعاون بموجب المعاهدات والاتفاقيات والقوانين باعتبار انه الطريقة الوحيدة لتحديد هوية مرتكب الجريمة ولما كان هذا الإجراء ذو طبيعة اقل مساس بالخصوصية فان الفقرة 2 استخدمت مصطلح " على الأقل لتشجيع الأطراف على السماح بأوسع نطاق ممكن للمساعدة المتبادلة بهذا الخصوص حتى في ظل غياب مبدأ التجريم المزدوج [2]

لذلك حصرت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والتي تم التوقيع عليها باليرمو عام 2000 على حث الدول إلى تطوير التعاون فيما بينها وتحتوي الاتفاقية على إشكال مختلفة من التعاون الدولي في مجال المساعدة القانونية المتبادلة كما تدعوا الاتفاقية جميع الدول إلى عهد اتفاقيات أخرى بهدف تعزيز التعاون فيما بينها [3]

ج: المساعدة المتبادلة فيما يتعلق باعتراض البيانات الخاصة بالمحتوى الالكتروني

نظرا لما تنطوي عليه اعتراض بيانات المستند الالكتروني من اختراق للخصوصية والسرية، فن تقديم المساعدة المتبادلة على مستوى اعتراض البيانات الخاصة بالمحتوى يجب أن تتقيد ببعض القيود.حيث تنص المادة 34 من اتفاقية بودابست على " يجب على الأطراف تقديم المساعدة المتبادلة لبعضها البعض، إلى المدى المسموح به في معاهداتهم وقوانينهم الداخلية المطبقة، فيما يتصل بجمع أو تسجيل بيانات المحتوى في الوقت الفعلي للاتصالات الجارية عبر نظام معلوماتي "إذ يجب أن يكون تقديم المساعدة المتبادلة في الحدود التي تسمح بها المعاهدات والقوانين الداخلية المطبقة للأطراف وبما أن التطبيق العملي

[1]- ياسر محمد الكومي، مرجع سابق، ص 341.

[2]- هلالي عبد الله أحمد، مرجع سابق ص 292.

[3]- ايمن رمضان محمد أحمد، مرجع سابق، ص 439.

للمساعدة المتبادلة المتعلقة باعتراض بيانات بان يتم تنظيمه وفقا للقوانين الداخلية المعمول بها من حيث مدى الالتزام بتقديم هذا النوع من المساعدة والقيود التي ترد عليه [1].

كما نصت المادة 35 من نفس الاتفاقية على انه يجب على كل دولة إن تقوم بتعيين نقطة اتصال عامة على مدار الساعة من اجل ضمان مساعدة فورية على مستوى التحقيقات والدعاوى انسجاما مع أحكام الفصل 3 من الاتفاقية ولا بد أن يتم هذا الإجراء سرعة وفعالية وفي حالة تبين أن احد موردي الخدمات في دولة أخرى يمتلك معلومات متعلقة بالبيانات العابرة، ويتعين على قسم محاربة الجريمة الالكترونية إبلاغ السلطة الأجنبية التي قدمت الطلب على الفور بهذا الأمر وتزويدها بالمعلومات الضرورية من اجل تحديد هوية مورد الخدمات المذكورة [2].

كما ونلاحظ أن هذا الإجراء مماثل لمراقبة المحادثات والمرسلات السلكية واللاسلكية أو تسجيل الأحاديث لمصلحة التحقيق والمنصوص عليها في المادة 93 من قانون الإجراءات الجنائية البحرية لسنة 2002 والتي أحاط هذا الإجراء لعدة شروط أهمها أن يتم هذا الإجراءإذا كان له فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس، وان يتخذ هذا الإجراء بإذن من قاضي المحكمة وان يكون قرار ضبط المراسلات أو المراقبة أو التسجيل مسببا ولمدة فصلا عن أن المادة 26 من دستور مملكة البحرين المعدل عام 2003 قد نصت على أن حرية المراسلة البريدية وأنها تقنية الالكترونية مصونة، وسريتها مكفولة، فلا يجوز مراقبة المراسلات أوإفشاء سريتها إلا في الضروريات التي يبينها القانون ووفقا للإجراءات والضمانات المنصوص عليها فيه[3]

ومؤدي ذلك انه إذا تبين لسلطات الدولة المطلوب منها أن الافضاح عن بيانات المستند الالكتروني قد يتخذ إجراءات من شانها تمديد السرية أو عرقلة التحقيق الذي تجريه الدولة التي قدمت الطلب فان لها أن تتحفظ على البيانات غير المادة أوجبت على تلك السلطات ضرورة إبلاغ سلطات التحقيق في الدولة الطالبة بذلك على وجه السرعة والعلة من ذلك بطبيعة الحال إتاحة الفرصة للدولة الطالبة اتخاذ تدابير آخري توصلا لأدلة قبل مرتكبي أي جريمة تتعلق باعتداء على التوقيع الالكتروني[4] ويثور التساؤل حول مدى أحقيته الدولة في اللجوء للتحفظ على بيانات المستند الالكتروني أوضبطها دون الحاجة لموافقة الدولة الأخرى ؟

[1]- هلالي عبد الله أحمد، مرجع سابق، ص 293.

[2]- لخالد ممدوح إبراهيم، مرجع سابق ص 341.

[3]- محمد كمال محمود الدوسقي، مرجع سابق، 165.

[4]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 338.

وقد أجابت المادة 32 من اتفاقية بودابست على ذلك التساؤل عندما نصت صراحته على انه يحق لسلطات الدولة الوصول بشكل أحاديإلى بيانات المستند الالكتروني المخزنة في أجهزة الحاسب الآلي الموجودة لدى دولة أخرى من دون الحصول على مساعدة متبادلة في حالتين هما

- أن تكون البيانات التي يتم الوصول إليها متوفرة للجمهور
- أن يصل فريق البحث إلى بيانات موجودة خارج أراضيه أو تلقاها من خلال جهاز حاسب آلي موجود ضمن أراضيه أو يحصل على الموافقة القانونية والطوعية للشخص الذي يتمتع بالسلطة القانونية ليفضح له عن هذه البيانات عبر هذا النظام [1]

د: الإفصاح السريع عن البيانات المارة المحفوظة

ومن الإجراءات الهامة لتيسير المساعدة القضائية في جرائم الاعتداء على التوقيع الالكتروني الإفصاح السريع عن البيانات المارة المحفوظة بناء على طالب المقدم من سلطات التحقيق حيث تتولى سلطات التحقيق في الدولة المطلوب إليها، حفظ بيانات المستند الالكتروني لتعقبها وصولا إلى مصدرة والكشف عن هوية المحرم أو ضبط الأدلة الحاسمة وهذا ما نصت عليه المادة 30 من تفتيش الاتفاقية والتي تنص على انه " في حالة إذا ما اكتشف الطرف المطلوب منه، أثناء تنفيذ الطلب المقدم إليه وفقا للمادة 29 من اجل التحفظ على خط سر بيانات تتعلق باتصال محدد، أن احد مقدمي الخدمة في دولة أخرى مشترك في نقل الاتصال يقوم الطرف المطلوب منه على الفور بالكشف عن القدر الكافي من خط سير البيانات للتعرف على مقدم الخدمة هذا والمسار والذي سلطه الاتصال [2].

وما يحدث في هذه الحالة انه عندما يقوم الطرف المقدم إليه الطلب بتنفيذ ما طلب منه بالتحفظ على بيانات المرور المتعلقة بنقل الاتصال بواسطة مزودي الخدمة بغرض من خلال تتبع مصدر الاتصال لتحديد هوية مرتكب الجريمة أو تجميع الأدلة على ذلك، انه قد يكتشف أثناء ذلك أن بيانات المرور التي وجدت في إقليمه تشير إلى

أن الاتصال قد تم إرساله من خلال مزود خدمات موجود في إقليم دولة ثالثة أو حتى في إقليم الدولة مقدمة الطلب، فانه في هذه الحالة يجب على الدولة المقدم إليها الطلب أن بالكشف لدولة الطالب عن القدر الكافي من البيانات من خط سر البيانات الذي يمكنه من التعرف على مزود الخدمة هذا والمسار الذي سلكه الاتصال، وفي ذلك فائدة للدولة مقدمة الطلب حيث تتمكن من خلال هذه المساعدة من

[1]- هلالي عبد الله أحمد، مرجع سابق، ص 293.

[2]- هلالي عبد الله أحمد، مرجع سابق ، ص 288-289.

معرفة الدولة التي تقدم إليها طلب المساعدة العاجلة بشأن البيانات والمعلومات المخزنة في النظام المعلومات وهكذا حتى يتم الوصول إلى المصدر الحقيقي للاتصال [1].

وترتيبا على ذلك يحق للدولة التقدم بطلبات طارئة للتعاون من خلال وسائل سريعة للتواصل عوضا عن اللجوء إلى الوسائل التقليدية والبطيئة القائمة على نقل الوثائق الخطية والمختومة عن طريق القنوات الدبلوماسية، أو أنظمة إرسال البريد ومتى ارتكبت جرائم الاعتداء على التوقيع الالكتروني من أكثر من ثلاثة أشخاص من خلال إقليم أكثر من دولة، فانه يلزم عملا حسب نص المادة 18 من اتفاقية باليرمو لعام 2000 " على دول الأطراف أن يقدم كل منها للأخرى، اكبر قدر ممكن من المساعدة القانونية المتبادلة في التحقيقات والملاحقات والإجراءات القضائية ونفس ما نصت عليه اتفاقية بودابست بشأن جرائم الحاسب الآلي [2]

خامسا: التنسيق القضائي في جرائم التوقيع الالكتروني

تتبين ضرورة التنسيق القضائي على المستوى الدولي في مسائل الإجراءات العقابية المتعلقة بتنسيق تكنولوجيا الأنظمة الفعالية لتجنب نشوء ما يطلق عليه " الملاذ الرقمي " أي اتخاذ الانترنت ملانا لممارسة الجريمة مما يعني العمل على تنسيق السياسات الوقائية التي تهدف إلى الحد من فرص ارتكاب الجرائم الالكترونية [3]

خامسا التنسيق التقني: لإقامة تعاون دولي لأنه من إقامة تنسيق تقني وهذا ما نصت عليه اتفاقية الأمم المتحدة لمكافحة الفساد UN التعاون الدولي حسب مادة 48 فقرة3تسعى دول الأطراف إلى التعاون، فمن حدود إمكانياتها على التصدي للجرائم المشمولة بهذه الاتفاقية، التي ترتكب باستخدام التكنولوجيات الحديثة ولتحقيق التكامل مع الاتجاه العام لحوسبة عمليات العدالة الجنائية وتطوير المعلومات وتحليلها على الوجه الذي تخدم أهداف السياسة الجنائية الحديثة لمكافحة الإجرام الالكتروني ينبغي تبادل " العناصر الإدارية، والتقنيات الفنية وتعزيز القدرات لأجهزة العدالة وتحليل ونشر البيانات والمعلومات المتاحة حول الجريمة والسيل والآليات المبتكرة لمكافحة ما هو تقليدي وغير تقليدي [4].

[1] - محمد كمال الدسوقي، مرجع سابق، ص 160.

[2] - فهد عبد الله العبيد العازمي، مرجع سابق، ص336.

[3] -فهد عبد الله العبيد العازمي، مرجع سابق ، ص 502.

[4] - محمد كمال محمود الدوسقي، مرجع سابق ، ص153.

خـــاتمـــة

خاتمة:

بعد تناولنا لموضوع الحماية الجنائية لتوقيع الالكتروني سواء في جانبيه الموضوعي أو الإجرائي، وبينا موقف التشريع الجزائري والمقارن من ذلك، ثم تناولنا مدى ملائمة القواعد الإجرائية التقليدية لضبط الجاني في تلك الجرائم ومحاكمته، وصلة ذلك بالتعاون الدولي سواء على الصعيد البحث وتحقيق الأولي "مصالح الأمن والشرطة" أو في مرحلة التحقيق"المحاكمة".

وفي ضوء هذه الدراسة، فإننا نلخص النتائج نوجزها فيما يلي:

بخصوص تعريف التوقيع الالكتروني لاحظنا أن هذا التوقيع نشأ باستخدام التقنيات الحديثة من خلال الحاسوب الالكتروني، وأن معظم التشريعات الدولية والعربية وغير العربية متفقة إلى حد ما على أن التوقيع الالكتروني يتخذ شكل معلومات الكترونية يتم إجراؤه من خلال التقنية الالكترونية، ويتخذ أشكالا وصورا لا تنحصر في صورة أو نوع واحد، ويأتي ذلك التعدد من تعدد أطراف إصداره، والتي قد تكون على شكل حروف أو أرقام أو رموز موثوقة على تقنيات التشفير ليتمتع بالمصداقية والأمان.

ويعتبر التوقيع الالكتروني بديلا عن التوقيع التقليدي فيما يتعلق بالتعاملات الالكترونية ومؤديا لكامل وظائفه لكونه يثبت عدم حصول تغيير بالمستند الإلكتروني أو الرسالة الالكترونية، كما يثبت هوية الموقع بشكل أكثر دقة من التوقيع التقليدي بسبب التقنيات المستخدمة فيه.

كما تبين لنا التوقيع الالكتروني يحق وظيفتين أساسيتين، الأولى هي تحديد الموقع والثانية هي صحة المعلومات الصادرة عنه، لكن تبين لنا أن المشرع الجزائري قد أحاطه بشروط قانونية أخرى، وهي ضرورة الاعتراف به حتى يرتب الآثار القانونية التي يرتبها التوقيع اليدوي، أولهما استعمال منظومة موثوق بها وثانيهما أن تتضمن تلك المنظومة الصلة بين التوقيع الالكتروني والموقع.

إن أحد سبل الحماية الوقائية للتوقيع الالكتروني هو أن يسبع عليه وأن الحجية المقررة للتوقيع التقليدي وهذا ما أخذ به المشرع المصري والأردني الذين اعترفا للتوقيع الالكتروني بالحجية القانونية في الإثبات وساووه بينه وبين التوقيع التقليدي، كما وقد منح المشرع الجزائري لتوقيع الالكتروني المؤمن الحجية الكاملة في الإثبات مثله مثل التوقيع التقليدي كورقة عرفية يرتب جميع الآثار القانونية عندما تتوافر فيه الشروط القانونية المطلوبة، أما باقي صور التوقيعات الالكترونية الأخرى التي لا تستجيب لمتطلبات الآلية المؤهلة لإحداث التوقيع الالكتروني الموثوق بها يتقرر لها حجية ناقصة.

ومن شروط صحة التوقيع الالكتروني هو الرجوع إليه عند الحاجة، لكن ما يلاحظ أن المشرع الجزائري لم ينص على ذلك، كما يجب أن يكون هذا الاطلاع مضمونا طوال المدة صلاحية محتوى التوقيع الالكتروني ولضمان توفر كل هذه الشروط يجب اعتماد آليات تحقق هذا الحفاظ الذي يكون في الغالب محفوظا على حامل الكتروني، وعبارة الحامل الالكتروني هي الأخرى لم يعرفها المشرع الجزائري ويستحسن أن يقوم بذلك.

هذا ويعتبر التشفير أحد أهم سبل الحماية التقنية للتوقيع الالكتروني، يتم بصور متعددة منها التوقيع بالرقم الكودي، واعتماد على المفتاحين العام والخاص وكذا استخدام أدوات القياس الحيوي مثل بصمة الإبهام وحدقة العين وبصمة الصوت.

لقد اختلفت القوانين المنظمة للتوقيع الالكتروني بهذا الشأن،حيث أن بعضها عرف التوقيع الالكتروني وربط الاعتراف القانوني به بمدى توفر شروط التوثيق والأمان التي تقوم على هيئات التوثيق الالكترونية، وذلك بمدى قوة التوقيع للاعتراف به، ولكن معظم التشريعات الالكترونية ركزت على ضرورة وجود جهة ثالثة لتصديق التوقيعات الالكترونية وتوفير الثقة والأمان الكاملين في استعمال التوقيع الالكتروني، ولاسيما أن طبيعة استعمال التوقيع الالكتروني يتطلب استخدامها ما بين أطراف بعيدين عن بعضهم.

وفي هذا الصدد اشترط المشرع الجزائري كباقي تشريعات العالم، استعمال منظومة توثيق التوقيع الالكتروني تضمن بصفة حقيقية وقوية الصلة بين الوثيقة الالكترونية والتوقيع الالكتروني من خلال تدخل الغير كطرف ثالث ومحايد وموثوق به، وهو جهة التصديق الالكتروني التي تسمح بضمان الصلة بين منظومة توثيق توقيع الكتروني يتعلق بشخص معين دون غيره.

وتأكيدا لحرص مشرعي الدول المختلفة على وضع ضمانات الكفيلة بحرية المعاملات الالكترونية وإصباغ الحماية الجنائية على المستند الالكتروني تم تجريم أفعال الاعتداء على التوقيع الالكتروني، سيما وقد بدا الدخول على الانترنت وسيلة سهلة في ارتكابها.

لذلك استهدف المشرع عند وضع قانون التوقيع الالكتروني في الجزائر تنظيم التوقيع والتصديق الالكترونيين بنصوص خاصة مستقلة وهذا استجابة لمتطلبات التطور التكنولوجي الحاصل في جميع مجالات الحياة، إذ حدد المقصود بالتوقيع الالكتروني وشروطه وكذا الجهات المختصة بالتصديق الالكتروني وفي الأخير نص على مجموعة من الجرائم محاولا من خلالها إقرار حماية جزائية في مواجهة مؤدي خدمات التصديق الالكتروني وكذا طالبي خدمة التوقيع الالكتروني.

وقد تعددت أنماط التجريم وفقا لمصلحة محل الاعتداء، فقد يرتبط السلوك المادي لجرائم الاعتداء على التوقيع الالكتروني بتداول بيانات المحرر الالكتروني كما هو الحال بالنسبة لجريمة التعامل غير المشروع في نشاط التصديق أو انتهاك سرية وخصوصية البيانات، كما أنه من المتصور أن يكون محل الجريمة هو المساس بحجية التوقيع الالكتروني في الإثبات كما هو الحال في جريمة تزوير التوقيع الالكتروني أو إتلافه، لذلك كان ضروريا ملاحقة ذلك الاعتداء بالتجريم بالتوازي مع الحماية التقنية سالفة البيان.

فعلى صعيد التجريم والعقاب، قام المشرع الجزائري بخطوة أولى تمثلت في النص على تجريم الاعتداءات على شرف واعتبار الأشخاص وعلى حياتهم الخاصة باستعمال تكنولوجيا الإعلام والاتصال مثل جرائم الإهانة أو السب أو القذف باستعمال الوسائل الالكترونية أو المعلوماتية وعموما بأي وسيلة الكترونية توفرها التقنية الحديثة بموجب المواد 144 مكرر و144 مكرر 2 و146 من قانون العقوبات وفي الاتجاه نفسه نصت المواد 303 مكرر 303 مكرر 3 من نفس القانون.

وفي الشأن ذاته ونظرا لخطورة الجرائم الالكترونية، قام المشرع بخطوة ثانية مهمة في سياسته الجنائية الرامية لمواجهتها، تمثلت في تعديل قانون العقوبات مرة أخرى بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 بإضافة قسم سابع مكرر عنوانه "جرائم المساس بأنظمة المعالجة الآلية للمعطيات" من المواد 394 مكرر إلى 394 مكرر 7 مثل جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات وجريمة التلاعب في معطيات نظام المعالجة الآلية للمعطيات وغيرها، كما اتجه المشرع إلى تجريم بعض أشكال الجرائم الالكترونية بموجب بعض القوانين الخاصة كقانون البريد والمواصلات السلكية واللاسلكية، وفي خطوة ثالثة إصدار قانون رقم 15-04 المؤرخ في 2015/02/01 المتعلق بالتوقيع والتصديق الالكترونيين الذي جرم كافة الاعتداءات التي قد تلحق بهما خاصة المتعلقة بالإتلاف والتزوير والدخول والبقاء الغير مصرح بهما مما يلزم الرجوع إلى القواعد العامة المدرجة في قانون العقوبات والتي يعاب عليها أنها لم تتناول التزوير المعلوماتي وفقا للقانون 23/06 بالرغم من أهميته بالنسبة لتوقيع الالكتروني.

كما يعاب أيضا على المشرع الجزائري أنه اقتصر على الحماية المقررة في مواجهة مؤدي خدمات التصديق في حالة الإخلال بالتزاماتهم وكذا طالبي الخدمة في حين أن التحايل الالكتروني قد يقع من عدة أطراف كالقراصنة مثلا مما يتعين على المشرع الجنائي مواجهة جميع صور التحايل لأجل حماية كافة

المصالح المعتدى عليها، ضف إلى ذلك أن صور التجريم المستحدثة لحماية التوقيع الالكتروني من المؤكد تزايدها في المتقبل.

وفي مقابل تتجلى الأهمية البالغة التي وقف عليها المشرع الجزائري في محاولة تبني قانون خاص بالتوقيع الالكتروني وهو القانون 15-04 متفاديا مختلف الانتقادات التي وجهت له خاصة بعد أن أصبح التعامل بالوسائل الالكترونية واقعا مفروضا على المشرع والمجتمع معا، حيث حاول من خلال قانون التوقيع الالكتروني الحفاظ على الحق في الخصوصية وضمان سرية المعلومات وجرم العديد من الأفعال وقرر لها عقوبات رادعة.

ومن خلال ما تم عرضه توصلنا إلى أنه بالرغم من صدور قانون 04/15 المتعلق بالتصديق والتوقيع الالكترونيين وبالرغم من مصادقة الجزائر على الاتفاقية العربية لمكافحة جرائم الانترنت أو اعتراف المشرع في القانون المدني المعدل سنة 2005 لإمكانية الإثبات بواسطة مستندات موقعة الكترونيا فإن المشرع لم ينص على جريمة التزوير التوقيع الالكتروني ومن ثم لا يمكن تطبيق النصوص المتعلقة بجرائم الماسة بأنظمة المعالجة الآلية للمعطيات لاختلاف المصلحة المحمية بينها وبين جريمة تزوير التوقيع الالكتروني، ناهيك عن حظر القياس في القانون الجنائي.

إن صعوبات التي تعترض إثبات جرائم الاعتداء على التوقيع الالكتروني متعددة يتعلق البعض منها بالعنصر البشري حيث تتم أفعال الاعتداء على التوقيع الالكتروني عادة عن بعد وقد تمتد إلى النطاق الإقليمي لدولة أخرى مما يضاعف صعوبة كشفها أو ملاحقتها، فضلا عن نقص خبرة القائمين بالتحقيق في جرائم الاعتداء على التوقيع الالكتروني كما أن الجناة كثيرا ما يستخدمون أسماء مستعارة أو يدخلون إلى الشبكة من خلال مقاهي الانترنت ويتعلق البعض الآخر بطبيعة أدلة الإثبات مثل سهولة محو الدليل أو تدميره، وتعذر الوصول إلى الدليل الالكتروني في تلك الجرائم، فضلا عن فخامة كم البيانات المتداولة وصعوبة التعاون الدولي وصولا لدليل الكتروني فيها.

كما وأن التحقيق والبحث في جرائم الاعتداء على التوقيع الالكتروني 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.

اما فيما يتعلق بالجانب الاجرائي و بالضبط في الجانب المتعلق باجراءات التقليدية للبحث و التحري كالتفتيش و المعاينة تبين لنا انها غيؤر كافية و لا تتلائم مع الطبيعة الخاصة بجرائم التوقيع الالكتروني

مما دفع بالمشرع الجزائري الى تعديل قانون الاجراءات الجزائية اين استحدث اساليب خاصة لبحث و التحري كاعتراض بيانات مستند التوقيع الالكتروني و التقاط الصور و تسجيل الاصوات

وبعد دراستنا لاعتراض المراسلات وتسجيل الأموات والتقاط وما تمثله هذه الإجراءات الجديدة في مكافحة الجرائم المستحدثة ومنها جرائم التوقيع الالكتروني إلا انه يمكن ملاحظة بعض الإشكاليات العملية الآتي يجب مراعاتها وإيجاد حلول سنخلصها كما يأتي:

- مدى توافر الوسائل التقنية لاعتراض المراسلات وتثبيتها وهي عادة ما تكون وسائل تقنية ذات كفائة عالية.

- مدى توفر االعنصر البشر بالكافي والمؤهل

- إمكانية، التلاعب المراسلات والأصوات المثبتة على دعامات الكترونية أو مغناطيسية، لذا لابد من إيجاد احتياطات خاصة لتخزينها

إن تخطي جرائم التوقيع الالكتروني حدود الدول أفرزتجملة من التحديات القانونية على الصعيد الإجرائي تجسدت في المقام الأول في صعوبات إثبات هذه الجرائم وقبول الدليل بشأنها باعتبارها لا تترك أثر مادي ملموس، كما هو الحال في الجرائم التقليدية فضلا عما يثيره ذلك من عقبات تواجه الأجهزة القضائية والأمنية في سبيل مباشرة الإجراءات عبر الحدود كالمعاينة والتفتيش في نطاق البيئة الافتراضية، يضاف إلى هذا مشكل تنازع الاختصاص بصدد هذه الجرائم باعتبار أن أثارها تتجاوز حدود الدول، الأمر الذي أدى إلى أن الحلول الوطنية غير مجدية، وتظل مشوبة بالقصور وعدم النجاعة، وعليه يحتاج الأمر إلى تعاون وتنسيق في الدول لتجاوز هذه العقبات الإجرائية.

كما لا يجوز امتداد التفتيش في الوسط الافتراضي خارج حدود الدولة احتراما لمبدأ السيادة ومع ذلك يجوز الحصول على الأدلة الموجودة في وسط افتراضي خارج حدود الدولة تطبيقا لاتفاقيات الإنابة القضائية، أو وفقا لنظام تبادل المساعدات، وبالتالي لا بدى من التعاون الدولي في هذا المجال بمقتضى اتفاقية ثنائية أو متعددة الأطراف أو على الأقل الحصول على إذن الدولة يتم التفتيش في مجالها الإقليمي.

التوصيات:

وفي ضوء نتائج الدراسة سالفة البيان فإنني اخلص لبعض التوصيات التي تقتضيها الضرورة التشريعية الجنائية في سبيل مكافحة الجرائم الناشئة عن التوقيع الالكتروني وتتمثل تلك التوصيات فيما يلي:

-بالرغم من الايجابيات التي أتى بها القانون 04/15 المتعلق بالتوقيع والتصديق الالكتروني إلا أنه لم يخلو من السلبيات أهمها:

-لم يتناول كافة الاعتداءات التي قد تلحق بهما خاصة المتعلقة بالإتلاف والتزوير والدخول والبقاء غير المصرح بهما.

- يتعين على المشرع الجنائي مواجهة جميع صور التحايل لأجل حماية كافة المصالح المعتدى عليها.

-ضف إلى ذلك ضرورة النص على تجريم صنع أو حيازة أو الحصول على برنامج أو نظام معلوماتي لإعداد توقيع الكتروني كما هو الحال في التشريعات المقارنة ذلك أن العبث بالتوقيع الالكتروني لابد أن يتم من خلال تقنية فنية وهو ما يعكس صورة من الحماية الجنائية الوقائية التي تستهدف منع الجريمة قبل وقوعها تبررها خطورة تلك الأفعال.

تجريم محاولة الحصول على توقيع أو محرر الكتروني بنص خاص.

بخصوص التحايل الإلكتروني من الأفضل إضافة المشرع الجزائري عبارة أي طرف أخر كون أن التحايل قيد يقع أيضا من طرف القراصنة

من شروط صحة التوقيع الالكتروني هو الرجوع إليه عند الحاجة لكن ما يلاحظ أن المشرع الجزائري لم ينص على ذلك، ويجب أن يكون هذا الاطلاع مضمونا طوال مدة صلاحية محتوى التوقيع الالكتروني ولضمان توفر كل هذه الشروط يجب اعتماد آليات تحق هذا الحفظ الذي يكون في الغالب محفوظا على حامل الكتروني وعبارة الحامل الالكتروني هي الأخرى لم يعرفها المشرع الجزائري ويستحسن أن يقوم بذلك.

وجوب تنظيم المشرع الجزائري للتصديق الالكتروني سواء كان جهة وطنية أو أجنبية وتحديد هيكل قانوني يحدد القواعد الملائمة فيما يخص المعايير التي ينبغي أن يستوفيها أو القواعد التي تحكمه لضمان أمن وسلامة المعاملات الالكترونية.

ومن جانب آخر اتضح لنا أن نشاط مزود لخدمات التصديق الالكتروني يجمع معلومات شخصية خاصة بأصحابها، وهو أمر أثار ولازال يثير إشكال حماية المعطيات الشخصية للمتعاملين عبر الشبكة وقد شغل هذا الإشكال بالمشرعين في العالم لكن الجزائر هي مرة أخرى متأخرة في هذا المجال لهذا سيكون من الضروري تنظيم هذه المسألة الحساسة.

بالنسبة لإثبات العقد الالكتروني كان لازما الاعتراف بالوثيقة الالكترونية الممضاة الكترونيا في شكل التوقيع الالكتروني على أنها وثيقة تمكن صاحبها من إثبات قيام علاقة تعاقدية بين طرفين، لكن يشترط فيها السلامة والحفظ حتى تتحقق حجيتها أما فيما يخص مسألة حفظ الوثيقة فكان من مفروض على المشرع الجزائري بتعريف مفهوم الحفظ، لتحديد أدوات إنشاء الوثيقة الالكترونية والجهة التي أنشأتها والوسائل التقنية التي تضمن عدم التحريف والتغيير والتلف والزوال حتى تكتسي نفس قيمة الوثيقة الورقية.

- أهمية تدعيم الحماية الفنية للتوقيع الالكتروني باستعمال الطرق الحديثة للتشفير الالكتروني وتحويل بياناته إلى رموز أو إشارات لحماية وسريته.

إن التوقيع الالكتروني يحقق وظيفتين أساسيتين الأولى هي تحديد الموقع والثانية هي صحة المعلومات الصادرة عنه لكن تبين لنا أن المشرع الجزائري قد أحاطه بشروط قانونية وهي ضرورة الاعتراف به واستعمال منظومة موثوق بها وأن تتضمن تلك المنظومة الصلة بين التوقيع الالكتروني والموقع لكن حبذا من المشرع الجزائري النص على تحديد تلك المنظومة.

لم يحدد المرسوم التنفيذي 01-123 المؤرخ في 2001/5/9 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، القواعد التي تحكم المواصفات التقنية لمنظومة إنشاء التوقيع الالكتروني المتبناة من قبل معظم التشريعات العالم ألا وهي منظومة التشفير اللاتماثلي والتي تعد من أبرز بروتوكولات العالمية في هذا المجال وأكثرها استخداما فيكون بذلك قد غاب عن تعريف التشفير ولابد أن يحدد نظمه وضوابطه في إطار التجارة الالكترونية.

-ضرورة إصدار النظام اللازم المتعلق بتنظيم كيفية حفظ الوثيقة الموقعة الكترونيا، فبدونه ينبغي التعامل عبر الوسائط الالكترونية حبرا على ورق.

-وضع نص قانوني يتضمن قرينة قانونية تفيد موثوقية التوقيع الالكتروني الموصوف على غرار ما فعل المشرع الفرنسي والأردني مما يساهم في عبئ إثبات صحة التوقيع الالكتروني.

-ضرورة العمل على تطوير الأنظمة والقوانين التقليدية بشكل دوري، ومحاولة احتوائها لكافة الجرائم المستحدثة، وإصدار تنظيمات وقوانين جديدة لما يعجز عن استيعابه النص التقليدي وذلك لمواكبة التطور السريع في أساليب وطرق ارتكاب الجريمة.

-ضرورة العمل على تحديث الإجراءات الكفيلة بكشف الأساليب المبتكرة الحديثة وتأهيل العاملين من أجهزة العدالة ليتمكنوا من الإلمام بهذه الأساليب وتطورها وفهمها.

-ضرورة أن تعمل الجزائر على استحداث أقسام متطورة داخل أجهزة العدالة تعنى بمكافحة جرائم التوقيع الالكتروني والتي من أهم سماتها صعوبة اكتشافها وكذلك ضبطها.

-ضرورة تأمين التوقيع الالكتروني بأدق وسائل الحماية حتى لا يتعرض لتزوير والإتلاف ويفضل أن تعتمد المؤسسات المالية على أكثر من وسيلة عند تصميمه كما يفضل أن تضمن لأكثر صورة التوقيع الالكتروني، كأن يوضع بإضافة إلى التوقيع بالرقم السري، توقيع بيومتري كبصمة العين واليد.

ضرورة ضمان القدر الكافي من المرونة من التشريعات المنظمة لتوقيع و التصديق الإلكترونيين من طرف المشرع ،بما يسمح بمواجهة المستجدات المتعلقة بجرائم الاعتداء على منظومة المعاملات الإلكترونية خاصة في ظل تطورها المستمر و الدائم.

-العمل على تأمين المؤسسات الخاصة بالتصديق الرقمي الحكومية منها والخاصة والعمل على وضع الاحتياطات الكفيلة بمنع تسرب المعلومات السرية لتواقيع الالكترونية والحيلولة دون استغلالها.

-التأكيد على أهمية الإجراءات الوقائية الدولية لمحاربة جرائم الاعتداء على التوقيع الالكتروني، مثل اعتراض وتسجيل بيانات المستند المتضمن التوقيع الالكتروني للمحافظة عليه من خطر الضياع أو التعديل.

-ضرورة إنشاء نيابة متخصصة بجرائم الحاسب الآلي ومن ضمنها جرائم الاعتداء على التوقيع الالكتروني والعمل على تعزيز قدرات أعضاء النيابة العامة في الموضوعات المرتبطة بتلك الجرائم وآليات مكافحتها، كيفية البحث والتحقيق فيها، خصوصا في الجانب المتعلق بجمع وسائل الإثبات وتقييم الأدلة والتأكيد على أهمية عقد دورات تكوينية حول تقنيات التحقيق في جرائم الاعتداء على التوقيع الالكتروني لما لهذا الموضوع من تأثير في مكافحة هذه الجرائم.

-لقد أصبح من الضروري على المشرع الجزائري إدراج نصوص إجرائية في قانون 04/15متعلق بالتوقيع والتصديق الالكترونيين من حيث إجراءات البحث والتحري إلى غاية المحاكمة .

-تعميق التفكير حول فكرة التخصص بالنسبة للمحاكم والمجالس المنوط بها النظر في جرائم الاعتداء على التوقيع الالكتروني، مع تأهيل قضاتها بكيفية التعامل مع هذا الدليل الالكتروني وفحصه أثناء المحاكمة، حتى يتسنى لمحاكم أو المجالس مراقبة عمل الخبير، وتفهم طبيعة تلك الجرائم، ما يستلزم الفصل فيها من سرعة ودقة.

ضرورة التعاون الإقليمي والدولي في مجال مكافحة جرائم الاعتداء على التوقيع الالكتروني عبر شبكة الانترنت والسعي نحو إيجاد إطار قانوني للتعاون بين أجهزة الشرطة والنيابات العامة العربية والأجنبية والأجهزة المساعدة لها للعمل على ضبط مرتكبي هذه الجرائم وملاحقتهم جنائيا من خلال إجراءات التسليم والمساعدة والإنابة القضائية.

ضرورة التنسيق بين دول المغرب العربي ودول الخليج فيما يتعلق بتبادل الخبرات في مجال مكافحة جرائم التوقيع الالكتروني حتى يتم تطويق الأساليب الإجرامية والقضاء عليها مبكرا قبل انتشارها في كافة الدول باستغلال الفراغ التشريعي.

تنظيم مؤتمرات عربية بهدف وضع قواعد موحدة لتنظيم التوقيع الالكتروني بذات التوجيه الذي أصدره الاتحاد الأوروبي.

قائمة المصادروالمراجع

قائمة المصادروالمراجع:

القرآن الكريم

الكتب العامة:

1- أحسنبوسقيعة، الوجيز في القانون العام، دار هومة للطباعة والنشر والتوزيع، الجزائر 2011.

2- أحسن صادق المرصفاوي، أصول الإجراءات الجنائية في القانون بمنشأة المعارف الإسكندرية 1982.

3- أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، الطبعة الثانية، دار النهضة العربية، القاهرة 2006 .

4- أحمد فتحي سرور، أصول الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1994 .

5- بن شيخ حسين، مبادئ القانون العام، دار هوهة لنشر والتوزيع، بوزريعة الجزائر سنة 2002.

6- جباري عبد المجيد، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة دار هومة الجزائر 2012.

7- حسين فتحي الحامولي، التعاون الدولي والأمني في تنفيذ أحكام جنائية، دار نهضة عربية، القاهرة، مصر، 2014.

8- رقيةعواشرية، نظام تسليم المجرمين ودوره في تحقيق التعاون الدولي لمكافحة الجريمة المنظمة، محلية المفكر، جامعة محمد خيثر، الجزائر، بسكرة العدد الرابع 2008 .

9- رمزي رياض عوض، حماية المتهم في النظام الانجلو أمريكي، دار النهضة العربية، القاهرة، 1998.

10- رؤوف عبيد، جرائم التزييف والتزوير في القانون المصري، مطابع دار الكتاب العربي، القاهرة، 2007.

11- سامي عبد الحميد، أصول القانون الدولي العام، الإسكندرية، دار الجامعية، طبقة الخامسة.1998.

12- سليم علي عبده، التفتيش في ضوء قانون أصول المحاكمات الجزائية الجديد، دراسة مقارنة منشورات تربي الحقوقية، بيروت، لبنان، ط1 2006 .

13- شريف سيكامل، الجريمة المنظمة في القانون، الطبعة الأولى دار النهضة العربية، القاهرة، 2001.

14- طارق سرور، جرائم النشر، الطبعة 01 دار النهضة عربية، القاهرة، 2001 .

15- عبد الرؤوف مهدي " شرح القواعد العامة الإجراءات جنائية، دار النهضة العربية، القاهرة، 2000.

16- عبد الفتاح محمد سراج، النظرية العامة لتسليم المجرمين، دار النهضة العربية، القاهرة، 2001.

17- عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري التحري والتحقيق، دار هومة، الجزائر، 2004.

18- قدري عبد الفتاح الشهاوي، أدلة مسرح الجريمة، الأساليب التقنية المتقدمة، علما وقانونا وتحليلا وفنا وعملا وتطبيقا، منشأة المعارف، الإسكندرية، مصر، 1998.

19- مأمون محمد سلامة، قانون الإجراءات الجنائية معلقا عليه بالفقه والقضاء، دار الفكر العربي، القاهرة، سنة 1981.

20- محمد علي سويلم، التعليق على قانون المحاكم الاقتصادية، دار المطبوعات الجامعية،الإسكندرية، الجزء الثاني، مصر، 2018.

21- محمود نجيب حسني، النظرية العامة لقصد الجنائي، دراسة تأصيلية مقارنة لركن المعنوي في الجرائم العمدية، دار النهضة العربية، القاهرة، 1988.

22- محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1988.

23- هدى قشقوش، شرح قانون العقوبات، دار النهضة العربية، القاهرة، مصر2007.

24- هلالي عبد الله أحمد، حجية المخرجات، دار النهضة العربية، الطبعة1، القاهرة،1997.

الكتب المتخصصة:

1- إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الالكترونية، مجلس البحث العلمي، جامعة الكويت، 2002.

2- أحمد حسام عجيله، الحماية الجنائية للمحررات الالكترونية، دار النهضة العربية، القاهرة، 2014.

3- أحمد خليفة المطلط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية 2000.

4- -أحمد محمد الهواري، عقود التجارة الالكترونية، مركز البحوث والدراسات أكاديمية شرطة دبي، الإمارات العربية المتحدة، 2003.

5- أحمد محمود موافى، شرح وتعليق على أحكام قانون التوقيع الالكتروني، دار الفكر القانوني، طبعة أولى، الاسكندرية، 2008.

6- أزاد دزه يي، النظام القانوني للمصادقة على التوقيع الالكتروني، دار الفكر الجامعي، الإسكندرية، الطبعة01، 2015.

7- أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دراسة مقارنة، ط2 دار النهضة العربية، القاهرة، 1998.

8- أشرف توفيق شمس الدين، الحماية الجنائية لمستند إلكتروني، دراسة مقارنة، دار النهضة العربية، القاهرة، الطبعة الأولى، مصر، 2006.

9- أيمن سعد سليم، التوقيع الالكتروني ، دراسة مقارنة، دار النهضة العربية، القاهرة، 2004.

10- أيمن عبد الله فكري، جرائم نظم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2007

11- ثروت عبد الحميد، التوقيع الإلكتروني ماهيته، مخاطره، وكيفية مواجهته، ومدى حجيته في الإثبات، دارالجامعة الجديدة، مصر، 2007.

12- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة 2001.

13- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الطبعة الثانية، دار النهضة العربية، القاهرة، 2011.

14- حسام محمد نبيل الشرقاوي، جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، مصر، سنة، 2013.

15- خالد ممدوح إبراهيم، إبرام العقد الالكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2008.

16- خالد ممدوح إبراهيم، التوقيع الالكتروني، الدار الجامعة الجديدة، الإسكندرية، ط أولى سنة 2000.

17- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى، عين مليلة، الجزائر، 2010.

18- داود سليمان على الحمادي، أحكام جريمة التزوير الالكترونية، دار النهضة العربية، القاهرة، مصر، 2008.

19- دلخار صلاح الدين بوتاني، الحماية الجنائية الموضوعية للمعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، سنة 2016.

20- راشد بن حمد البلوشي، التوقيع الالكتروني والحماية الجزائية المقررة له، دراسة في القانون العماني والقانون المقارن، منشورات الحلبي الحقوقية، طبعة أولى، 2018.

21- ربيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011.

22- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2007.

23- سمير حامد عبد العزيز جمال، التعاقد عبر تقنيات الاتصال الحديثة،دار النهضة العربية ,القاهرة ,مصر ,2006 .

24- سعيد سيد قنديل، التوقيع الالكتروني، دار الجامعة الجديدة، الإسكندرية، مصر، 2006.

25- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، دار النهضة العربية، الطبعة الأولى، القاهرة، مصر 1999.

26- سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت دار النهضة عربية 2008.

27- سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية " الانترنت، دار نهضة العربية، القاهرة، 2007.

28- شمسان ناجي صالح الخيلي، الجرائم المستحدثة بطرق غير مشروعة لشبكة الانترنت، دار النهضة العربية، القاهرة، سنة 2009.

29- شيماء عبد الغني عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2008.

30- صلاح الدين بوتاني، الحماية الجنائية الموضوعية للمعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، مصر، سنة 2016.

31- عادل ابو هشيمة محمود حوته، عقود خدمات المعلومات الالكترونية في القانون الدولي الخاص، دار النهضة العربية، مصر، 2004.

32- عادل رمضان الابيوكي: التوقيع إلكتروني في التشريعات الخليجية، المكتب الجامعي الحديث، القاهرة، 2009.

33- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية 2010.

34- عبد الحليم فؤاد الفقهي، جريمة تزوير التوقيع الالكتروني، دار النهضة العربية، القاهرة، 2016.

35- عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم المقارنة، دار الفكر الجامعي، الإسكندرية، طبعة 01، مصر، 2004.

36- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال تحقيق الابتدائي في الجرائم المعلوماتية، ط.1، دار الفكر العربي الإسكندرية، مصر، 2009 .

37- عبد القادر القهوجي، الحماية الجنائية لحاسب آلي، دار الجامع للطباعة والنشر، الإسكندرية،2004.

38- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، مصر 2001.

39- عمر الفاروق الحسني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دراسة تحليلة لنصوص التشريع المصري مقارنا بالتشريع الفرنسي، دار النهضة العربية، القاهرة، طبيعة 2، مصر، 1995.

40- عمر خالد الزرقيات، عقود تجارة الالكترونية، عقد البيع عبر الأنترنت، ط1، دار الجامعة للنشر والتوزيع، الأردن، 2007.

41- عيسى غسان عيسى، القواعد الخاصة بالتوقيع الالكتروني، دار الثقافة للنشر والتوزيع، عمان، طبعة اولى، سنة 2005.

42- فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2016.

43- ماجد راغب الحلو، العقد الإداري الإلكتروني، تأليف: رحيمة الصغير ساعد نمديلي، دار الجامعة الجديدة، 2007.

44- محمد أمين الرومي المحامي، النظام القانوني للتوقيع الالكتروني، دار الكتب القانونية، مصر، سنة 2008.

45- محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2003.

46- محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة الجديدة، مصر، 2003.

47- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.

48- محمد علي سويلم، الحماية الجنائية للمعاملات الالكترونية بين الجوانب الإجرائية والأحكام الموضوعية، دراسة مقارنة لقانون تنظيم التوقيع الالكتروني وتكنولوجيا المعلومات، دار المطبوعات الجامعية، الإسكندرية، طبعة أولى سنة 2018.

49- محمد فهمي طلبه، فيروسات الحاسب الآلي والبيانات،، مطابع الكتاب المصري الحديث، القاهرة، 1996.

50- محمد فواز المطالقة، الوجيز في عقود التجارة الالكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان 2008.

51- محمد فواز المطالقة، عقود التجارة الإلكترونية، أركانه، إثباته، حماية تشفير التوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، طبعة أولى، 2006.

52- محمد كمال محمود الدوسقي، الحماية الجنائية لسرية المعلومات الالكترونية، دار الفكر والقانون، المنصورة، 2018.

53- محمد محمود مصطفى، شرح قانون الإجراءات الجزائية، دار النهضة العربية، القاهرة، الطبعة 10، 1980.

54- محمود احمد طه، المواجهة التشريعية لجرائم الكمبيوتر وانترنت، طبعة1، دار الفكر، المنصورة 2013.

55- محي الدين عوض، مشكلات السياسية الجنائية المعاصرة في جرائم نظم المعلومات، دار النهضة العربية، القاهرة، 1994.

56- مدحت عبد الحليم رمضان، جرائم الاعتداء على أشخاص والانترنت –دار النهضة 2001.

57- المصطفى فارس، الإثبات الرقمي، الحجية القانونية للسندات الالكترونية، مكتبة رشاد للتوزيع والنشر، الطبعة 01، المغرب، 2005.

58- منير ممدوح محمد الجنمبهي، أمن المعلومات الالكترونية، دار الفكر الجامعي، الإسكندرية، 2005.

59- نايل نبيل عمر، الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2012.

60- نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقه، دار النهضة العربية، القاهرة، 2003.

61- نبيل عمر، الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2012.

62- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر، 2013.

63- نهلا عبد القادر الموسني، الجرائم المعلوماتية، طبعة1، دار الثقافة للنشر والتوزيع، عمان، 2008.

64- هدى حامد قشقوش الجرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، مصر، 2000.

65- هشام محمد فريد رستم الجوانب الإجرائية للجرائم المعلوماتية –دراسة مقارنة، مكتبة الآلات الحديثة، مصر 1994.

66- هلال بن محمد بن حارب البوسعيدي، الحماية القانونية الفنية لقواعد المعلومات المحسوبة، دراسة قانونية وفنية مقارنة، دار النهضة العربية، القاهرة، 2009.

67- -هلال عبد الله أحمد، تفتيش نضم الحاسب الآلي ونمانات المتهم المعلوماتي،، دراسته مقارنة، دار النهضة العربية. 2006.

68- هلالي عبد الله أحمد، جرائم المعلوماتية التقليدية والمستحدثة وتطبيقها في النظام البحريني، دار النهضة العربية، القاهرة، 2013.

69- هلالي عبد الله أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، دار النهضة العربية، مصر 2011 .

70- هلالي عبد الله، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة، مصر، الطبعة 01، 2003.

71- وائل أنور بندق، موسوعة القانون الإلكتروني وتكنولوجيا الاتصال، دار المطبوعات الجامعية، الإسكندرية، 2007.

72- يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في قانون العقوبات وقانون الإجراءات الجزائية والقوانين الخاصة، دار الجامعة الجديدة، الإسكندرية، مصر، 2019.

73- يمينة حوحو، عقد البيع الالكتروني في القانون الجزائري، دار بلقيس للنشر والتوزيع، دار البيضاء، طبعة أولى سنة 2016.

74- يوسف بن سعيد الكلياني، الحماية الجزائية للبيانات الالكترونية في التشريعين العماني والمصري، دار النهضة العربية، الطبعة الأولى سنة 2017.

75- يونس عرب، موسوعة القانون وتقنية المعلومات، دليل من المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، منشورات اتحاد المعارف العربية، طبعة الأولى.

76- وائل أنور بندق، موسوعة القانون الإلكتروني وتكنولوجيا الاتصال، دار المطبوعات الجامعية، الإسكندرية، 2007

الرسائل العلمية والمذكرات:

<u>رسائل الدكتوراه:</u>

1- إبراهيم الغماز الشهادة كدليل اثبات في المواد الجزائية رسالة دكتورة، كلية الحقوق جامعة القاهرة 1980 .

2- أحمد حسام طه، الجرائم الناشئة عن الحاسب الآلي، رسالة دكتوراه، جامعة 2000.

3- أمين عزان، الحماية الجنائية لتجارة الالكترونية، دراسة مقارنة، رسالة دكتوراه، حقوق عين شمس، 2005.

4- إيمان مأمون أحمد سليمان، الجوانب القانونية للتجارة الالكترونية، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، قسم القانون التجاري، 2006.

5- ايمن رمضان محمد أحمد، الحماية الجنائية لتوقيع الالكتروني، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، 2010.

6- أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2005.

7- ايهاب محمد يوسف، اتفاقيات تسليم المجرمين، رسالة دكتورة، كلية الدراسات العليا بأكادمية الشرطة ،دبي2003.

8- سالم محمد سليمان الأوحلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، رسالة دكتوراه، كلية الحقوق عين شمس، مصر، 1998.

9- سعد احمد محمود سلامة، التبليغ عن الجرائم، دراسة مقارنة، رسالة دكتورة اعادية الشرطة، القاهرة،.2003

10- صالح شنين، الحماية الجنائية لتجارة الالكترونية دراسة مقارنة، رسالة دكتورة جامعة أبوبكربلقايد تلمسان، 2013/2012.

11- صباح رمضان، ياسين صالح، السياسة الجنائية في مواجهة الجرائم المعلوماتية، دراسة تحليلية، رسالة دكتوراه، العراق، سنة 2013.

12- عايض راشد المري، مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود التجارية، رسالة دكتوراه، جامعة القاهرة، 1998.

13- عمار عبيد محمد الغول، نطاق تطبيق القانون الجنائي من حيث المكان وفق لمعطيات التكنولوجيا المعاصرة، رسالة دكتورة، كلية الحقوق، جامعة القاهرة، سنة 2006.

14- عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترنيا، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2009.

15- محمد احمد نور حسيبة، مدى حجية التوقيع الالكتروني في عقود التجارة الالكترونية، رسالة دكتوراه حقوق، القاهرة، 2005.

16- محمد سعيد اسماعيل، أساليب الحماية القانونية لمعاملات التجارة الالكترونية، رسالة دكتوراه حقوق، عين الشمس، 2005.

17- محمود عمر محمود، المسؤولية الجنائية الناشئة عن جرائم المحمول، دراسة مقارنة بين القانون الوضعي والشريعة الإسلامية، رسالة دكتوراه.

18- معندة سويدان، نظرية الاقتناع الذاتي للقاضي الجنائي، رسالة دكتورة كلية حقوق، جامعة قاهرة، 1985 .

19- مفيدة سويدان، نظرية الاقتناع الذاتي القاضي الجنائي، دراسة مقارنة، رسالة دكتورة، كلية الحقوق، جامعة القاهرة 1990.

20- ياسر محمد الكومي أبو حطب، الحماية الجنائية والأمنية لتوقيع الكتروني، رسالة دكتوراه في القانون الخاص، جامعة حلوان.

21-دمرين يونس، الجرائم عن استخدام الانترنت، رسالة دكتورة، جامعة عين شمس، القاهرة، 2004.

رسائل الماجستير:

1- أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة القاهرة،سنة 2010.

2-سويسر سفيان، جرائم المعلوماتية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، الجزائر، 2010.

3-صلاح عبد الحكيم المصري، متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية، رسالة ماجستير في إدارة الأعمال، كلية التجارة، الجامعة الإسلامية غزة، 2007.

4-فنور حاسين، لمنظمة الدولية لشرطة الجنائية والجريمة المنظمة، رسالة ماجيستير في القانون الدولي وعلاقات الدولية، جامعة جزائر بن عكنون، 2012-2013.

5-لالوش راضية، أمن التوقيع الالكتروني، رسالة ماجستير، في الحقوق، فرع القانون الدولي للأعمال، جامعة مولود معمري تيزي وزو، سنة 2012.

6-حنان محمد حسن علي، مبدأ الإقليمية الجنائي في القانون والشريعة الإسلامية رسالة ماجيستير، جامعة الخرطوم، 2008.

المجلات العلمية:

1- أيمن عبد الحفيظ، حدود مشروعية أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة، العدد 25، يناير 2004 .

2- حسام محمد رمضان، تطبيقات المحاكاة الحاسوبية في التخطيط والتدريب على إدارة الكوارث، مجلة البحوث الأمينة، أكاديمية الملك فهد الأمينة، مجلد 11 عدد 22 أكتوبر 2002.

3- خالد ممدوح إبراهيم، الحماية الجنائية لتوقيع الالكتروني، مجلة الفكر الشرطي، عدد 88 يناير 2019.

4- عزيزة لرقط، الحماية الجنائية للتوقيع والتصديق الالكترونيين في التشريع الجزائري، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي تمنراست، عدد 1 جانفي، 2017.

5- فريد لطفي، التعاون الدولي في مجال تسليم المجرمين، مجلة الشرطة الجزائرية العدد 92 أكتوبر 2009 .

6- فيصل سعيد الغريب، التوقيع الالكتروني وحجيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، مصر، 2005.

7- محمد زكي أبو عامر، القيود القضائية على حرية القاضي الجنائي في الاقتناع، مجلة القانون والاقتصاد، العدد 51، 1991 .

8- محمد محمود درويش، التطلعات المستقبلية نحو استخدام أسلوب المحاكاة في مجال التدريب الأمني بأكاديمية الشرطة، مجلة الأمن العام المصرية عدد 46.

9- محمد مدحت المراسي، أوجه الاستفادة من المعطيات العلمية والتكنولوجية المعاصرة في مجال تطوير برامج تأهيل رجال الشرطة، مجلة مركز بحوث الشرطة ، أكاديمية الشرطة عدد 22 سنة 2002 .

10- محمود وهيب السيد، شبكة الانترنت ومزيد من التقدم الأمني، مجلة مركز البحوث الشرطة العدد 21- 1999.

11- هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، دبي كلية الشرطة، العدد 2، 1999.

12- هشام محمد فريد رستم، جرائم الحاسب الآلي كصورة من صور الجرائم الاقتصادية المستحدثة مجلة الدراسات القانونية، جامعة أسيوط،العدد،1990،17.

المؤتمرات:

1- عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجل سرقة المعلومات، بحث مقدم لمؤتمر العلمي الأول، حول الجوانب القانونية والأمنية للعمليات الالكترونية، محور القانون الجنائي، دبي الإمارات العربية المتحدة 23 ابريل 2003 .

2- عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجل سرقة المعلومات، بحث مقدم لمؤتمر العلمي الأول، حول الجوانب القانونية والأمنية للعمليات الالكترونية، محور القانون الجنائي، دبي الإمارات العربية المتحدة 23 ابريل 2003 .

3- عبد الناصر محمد محمود فرغلي، الإثبات الجنائي بأدلة الرقمية من الناحيتين القانونية والفنية دراسة طبيعية مقارنة، المؤتمر العربي الأول لعلوم أدلة الجنائية والطب الشرعي من 12 إلى 14 نوفمبر 2007، رياض، السعودية

4- هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية المنعقد بـ 25 أكتوبر،القاهرة ،1993.

الاتفاقيات:

1- الإعلان العالمي لحقوق الإنسان الصادر في : 1948/12/10، انضمت اليه الجزائر غداة الاستقلال بموجب نص المادة 11 من دستور 1963 الصادر بتاريخ 1963/09/08.

2- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من طرف الجمعية العامة لمنظمة الأمم المتحدة يوم 2000/11/15 صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 04-165 المؤرخ في 2004/06/08.

3- اتفاقية بودابيست ودورها في تنسيق للقانون الدولي لمكافحة جرائم الانترنت 23/نوفمبر/2001.

4- النموذج الاسترشادي لاتفاقية التعاون القانوني القضائي الصادر عن جلس التعاون الخليجي أعتمد هذا النموذج من الجلس الأعلى لمجلس التعاون الخليجي في دورته الرابعة والتي انعقدت بدولة الكويت في الفترة من 21-2003/12/22

5- اتفاقية ثنائية بين الجزائر وفرنسا حول التعاون في مجال مكافحة الجرائم المنظمة، المرسوم الرئاسي رقم 07-375 المؤرخ في 2007/12/01 الجريدة الرسمية العدد 77، المؤرخة في 2007/12/09

6- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 2010/12/21 صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 2014/09/08 الجريدة الرسمية رقم 57 المؤرخة في 2014/09/28.

النصوص القانونية:

أولا-النصوص القانونية الوطنية:

1- القانون رقم 2000-03 المؤرخ في 2000/08/05، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية، ج.ر، رقم 48 المؤرخة في : 2000/08/06

2- القانون رقم 05-10 المؤرخ في 2005/6/20 يعدل ويتمم الأمر رقم 75-58 المؤرخ في 1975/09/26 والمتضمن القانون المدني، ج ر، رقم 44 المؤرخة في 2005/06/26.

3- القانون رقم 01/06 المؤرخ في 2006/02/20 المتعلق بالوقاية من الفساد ومكافحته، ج ر، رقم 14 المؤرخة في 2006/03/08.

4- القانون رقم: 09-04 المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، رقم: 47، المؤرخة في 2009/08/16.

5- القانون: رقم 15-04 المؤرخ في 2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج ر، رقم 06 المؤرخة في: 2015/02/10.

6- الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني المعدل والمتمم.

7- الأمر رقم 66-155 المؤرخ في 08 يونيو 1966 الذي يتضمن قانون الاجراءات الجزائية المعدل والمتمم.

8- الأمر رقم 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات المعدل والمتمم.

9- الأمر رقم 05-06 المؤرخ في 2005/08/23 المتعلق بمكافحة التهريب، ج ر، رقم 59 المؤرخة في 2005/08/28.

10- المرسوم الرئاسي رقم 89-67 المؤرخ في 1989/05/16، المتضمن انضمام الجزائر إلى العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية، والعهد الدولي الخاص بالحقوق المدنية والسياسية والبروتوكول الاختياري المتعلق بالعهد الدولي الخاص بالحقوق المدنية والسياسية الموافق عليها من طرف الجمعية العامة للأمم المتحدة بتاريخ 1966/125/16، ج.ر، رقم 20 المؤرخة في 1989/05/17.

11- المرسوم الرئاسي رقم 04-183 المؤرخ في 2004/06/16 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج.ر، رقم: 41 المؤرخة في 2004/06/27.

12- المرسوم الرئاسي رقم 04-432 المؤرخ في 2004/12/29 يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي

13- المرسوم الرئاسي رقم: 15-261 المؤرخ في 2015/10/08، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، رقم: 53 المؤرخة في 2005/10/08.

14- المرسوم التنفيذي رقم 98-257 المؤرخ في 1989/08/25، يضبط شروط وكيفيات إقامة خدمات الانترنت واستغلالها، ج.ر، رقم 63 المؤرخة في 1989/09/26.

15- المرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/05 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج.ر، رقم 63 المؤرخة في 2006.2/10/08

16- المرسوم التنفيذي رقم 07-162 المؤرخ في 2007/05/30 والمتعلق بـ نظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج.ر، رقم : 37 المؤرخة في 2007/07/07.

ثانيا-النصوص القانونية الأجنبية:

1- قانون العقوبات المصري الصادر في: 31 يوليو 1937 المعدل والمتمم.

2- القانون الفرنسي رقم 2001/272 الصادر بتاريخ 30 مارس 2000 المتعلق بالتوقيع الالكتروني المعدل والمتمم للمادة 13/6 من القانون المدني الفرنسي، الجريدة الرسمية عدد 77 الصادرة بتاريخ 31 مارس 2000.

3- القانون رقم: 2000-83 المؤرخ في 09 أوت 2000 المتعلق بالمبادلات والتجارة الالكترونية، الرائد الرسمي للجمهورية التونسية العدد 64، المؤرخ في 2000/08/11

4- القانون الأردني رقم 85 لسنة 2001الخاص بالتعاملات الالكترونية .

5- القانون رقم 02 لسنة 2002 المتضمن قانون التجارة الالكترونية لإمارة دبي.

6- القانون البحرين رقم 83 لسنة 2002 بشأن المعاملات الالكترونية

7- قانون دولة الإمارات العربية المتحدة لسنة 2003

8- القانون العربي النموذجي الموحد في شأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصال لسنة 2003.

9- القانون رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الالكتروني وإنشاء هيئة التنمية وصناعة التكنولوجية المعلومات بجمهورية مصر العربية، الجريدة الرسمية 218 الموافق لـ 22 أفريل 2004.

10- نظام مكافحة الجرائم المعلوماتية السعودي الصادر في: 2007/03/26

11- القانون العربي الاسترشادي للمعاملات والتجارة الالكترونية الذي اعتمد بقرار مجلس وزراء العدل العرب رقم : 25/812 بتاريخ 2009/11/19

المراجع باللغة الأجنبية:

LES OUVRAGES :

1- Huet J, vers une consécration de la preuve et la signature électronique, D. 2000، DALLOZ.

2- Ben-Halima(Sassi), les crimes informatiques et d'autres crime dans le domaine de la technologie informatique en Tunisie, 1993.

3- vidal G, cours de droit criminel et de science pénitentiaire, 2^{emme}, paris, 2010.

4- WILMS, Mélanges Jean Pardon, « De la signature au « notaire électronique ». La validation de la communication électronique », Bruxelles, Bruylant, 1996.

5- LéclercQ (jean), la signature électronique: lecture critique, technique et juridique, Le décret du 30 mars 2001 relatif à la signature.

6- Lamy alainbensausan, Intervention au colloque de la CREDA organisé le 13 mai 1998 sur le thème commerce électroniques avenir des circuits : de l'expérience des USA aux perspectives français. 1998.

7- Francillon (Jacques). Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France, Revue internationale de droit pénal, 1993.

8- Matthew R. *Zakaras*, Revue *internationale* de droit pénal, 2001.

9- adelbrahim, signature électronique et droit, édition Ms،Tunisie، 2004.

10- AlainBensoussan, internet aspect juridique, HERMES, paris,France, 2eme édition, 1998.

11- Alain Bensoussan, la signature électronique, premier réflexion après la publication de la directive du 13 décembre 1999 et la loi 13 mars 2000.

12- CAPRIOLI (ERIC), « Vote électronique, sécurité, technique et conformité juridique, Communication commerce électronique, revue mensuelle Lexis NexisJuris Classeur, Octobre 2012.

13- MARTIN H,La signature électronique : comment la technique répond elle aux exigences de la loi ? gazette du palais, 2000.

14- Mechaljaccard, problème juridique les transactions sur le réseaux, édition 2000.

15- Lionel (b), internet et commerce électronique, 2eme édition, Delmas 2001.

16- Christiane Féralschuhl،Cyberdroit, le droit à l'épreuve de l'Internet editiondalloz,، 2009

The books

1- alandavdson, the law of électronic commerce, ، USA, 2009.

2- *Jeff* C. Dodd and James A. Hernandez, contracting in cyberspace, avril 1998.

3- Edward h، j، d-، digital signature and électronic contacts, 2004.

4- vinezosins, digital Europe international lawer, decembre 2000.

5- Lornabrazel,Electronic Signatures and Identities Law and Regulation**,** 200**8.**

6- Nehadalhussban, admissibility of electronic signature in and It's Legal Effect ?A Comparative Study in the Jordanian Laws, ،university of Jordanian, December, 2005.

memory

1- willaimsdavid and john benamati,Technology foundations & e-*business applications, university new yourk,* 2003.

2- Jackblogna, Corporate Fraud: The Basics of Prevention and Detection, Butterworth-Heinemann, (July 1, 1984)

فهرس المحتويات

فهرس المحتويات

الملخص:

لقد كان لتطور مجال تكنولوجيا المعلومات وقطاع الاتصالات الذي يمر به العالم في الوقت الراهن، اثر بالغ واضح على المبادئ التي تحكم ابرام التصرفات والمعاملات القانونية، خاصة عناصر الدليل والإثبات الكتابة والتوقيع والمحرر فينما هذه التصرفات تنشأ بواسطة الكتابة التقليدية الخطية وتوقع بواسطة احد أشكال التوقيع التقليدي ورقي. أصبحت الآن تنشأ بواسطة تقنيات حديثة تتألف من كتابة إلكترونية وتوقيع إلكتروني. حيث ترتب عن الأهمية المتزايدة للتوقيع الإلكتروني عدة مشاكل قانونية أخطرها الاعتداء على منظومته القانونية على نحو يهدد التنمية الإقتصادية، مما أدى إلى ضرورة توفير حماية جنائية لتوقيع الإلكتروني، وعليه اتجهت العديد من الدول ومنها الجزائر إلى توفير حماية جنائية موضوعية وإجرائية سواء في إطار نصوص عامة أم نصوص خاصة بالتوقيع الإلكتروني.

الكلمات المفتاحية: التوقيع الإلكتروني، التجارة الإلكترونية، التوثيق الإلكتروني

Abstract

The development of the information and communication technological sector that the world is currently undergoing has had a significant and clear impact on the principles that govern the conclusion of legal acts and transactions, especially evidence and proof/corroboration components (writing, signature and edition), whereas, these behaviours originate through traditional handwriting and are signed by one of the traditional paper signature forms. It is now created by means of modern technologies, consisting of electronic writing and signature/signing. The increasing importance of the electronic signature has resulted in several legal issues, the most serious of which is the assault/offensive/infringement of its legal system in a manner that threatens economic development, which led to the necessity of providing criminal protection for the electronic signature. Accordingly, many countries, including Algeria, have tended to provide substantive and procedural criminal protection, whether in the framework of general texts or those relating to electronic signature.

Keywords: E-signature, e-commerce, e-authentication

Résumé

Le développement du secteur des technologies de l'information et de la communication que traverse/vit actuellement le monde a eu un impact significatif et clair sur les principes qui régissent la conclusion des actes et des transactions juridiques, en particulier les éléments d'évidence et de preuve (rédaction, signature et édition). Tandis que ces comportements proviennent de l'écriture manuscrite traditionnelle et sont signés par l'un des formulaires de signature papier traditionnels. Il est désormais créé au moyen de technologies modernes consistant en l'écriture électronique et la signature électronique. L'importance croissante de la signature électronique ayant entraîné plusieurs problèmes juridiques, dont le plus grave est l'attaque/infraction/agression contre/ violation de son système juridique d'une manière qui menace le développement économique, ce qui a conduit à la nécessité de fournir une protection pénale pour la signature électronique. En conséquence, de nombreux pays, dont l'Algérie, ont eu tendance à offrir une protection pénale matérielle et procédurale, que ce soit dans le cadre de textes généraux ou ceux relatifs à la signature électronique.

Mots clés: signature électronique, commerce électronique, authentification électronique